МВД России
Санкт-Петербургский университет

Т.В. Малкова

АНГЛИЙСКИЙ ЯЗЫК

ХРЕСТОМАТИЯ СПЕЦИАЛЬНЫХ ТЕКСТОВ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

Под редакцией
кандидата педагогических наук,
доцента Н.А. Беломытцевой

Санкт-Петербург
2017

План 2017, поз. 49

УДК 372.881.111.1
ББК 81.2Англ-93
М 18

Малкова Т.В.

М 18 **Английский язык. Хрестоматия специальных текстов «Информационные системы и технологии»** / под ред. Н.А. Беломытцевой. СПб.: Изд-во СПб ун-та МВД России, 2017. — 152 с.

Хрестоматия представляет собой сборник аутентичных, систематически подобранных текстов, снабженных англо-русским глоссарием, в которых затрагиваются вопросы обеспечения доступности, целостности и безопасности информации, уязвимости данных, классификации преступлений в сфере информационных технологий и борьбы с ними, компьютерной безопасности. Хрестоматия представляет теоретический и практический интерес в области применения информационных технологий в правоохранительной деятельности и их безопасности, а также деятельности сотрудников полиции по предупреждению, раскрытию и расследованию преступлений в сфере информационных систем и технологий в России и за рубежом.

Предназначена для обучающихся в образовательных организациях системы МВД России, а также может быть использована практическими работниками правоохранительных органов.

УДК 372.881.111.1
ББК 81.2Англ-93

Рецензенты:
Кравчук Л.С., заведующий кафедрой иностранных языков
(Белгородский юридический институт МВД России
им. И.Д. Путилина);
Анохина Л.И., кандидат филологических наук, доцент
(Орловский юридический институт МВД России
им. В.В. Лукьянова)

CONTENTS

UNIT 1

UNIT 2

UNIT 3

UNIT 4

UNIT 5

UNIT 6

UNIT 1
INFORMATION SYSTEMS AND TECHNOLOGIES. INFORMATION TECHNOLOGIES IN LAW ENFORCEMENT

1. INFORMATION SYSTEM (IS)

An information system (IS) refers to a collection of multiple pieces of equipment involved in the dissemination of information. Hardware, software, computer system connections and information, information system users, and the system's housing are all part of an IS. An information system commonly refers to a basic computer system but may also describe a telephone switching or environmental controlling system. The IS involves resources for shared or processed information, as well as the people who manage the system. People are considered part of the system because without them, systems would not operate correctly. There are several types of IS, including the following common types:

- Operations support systems, including transaction processing systems;
- Management information systems;
- Decision support systems;
- Executive information systems.

An operations support system, such as a transaction processing system, converts business data (financial transactions) into valuable information. Similarly, a management information system uses database information to output reports, helping users and businesses make decisions based on extracted data.

In a decision support system, data is pulled from various sources and then reviewed by managers, who make determinations based on the compiled data. An executive information system is useful for examining business trends, allowing users to quickly access custom strategic information in summary form, which can be reviewed in more detail.

2. INFORMATION TECHNOLOGY (IT)

Information Technology (IT) is a business sector that deals with computing, including hardware, software, telecommunications and generally anything involved in the transmittal of information or the systems that faciliate communication. IT involves many things. Take, for instance, an IT department in a company. There are many people with many jobs and varied responsibilities. These responsibilities range from keeping systems and data secure to keeping networks up and running. There are people who input data, people who manage databases and people who do programming. There are also the decision makers, such as Chief

Information Officers (CIOs), who decide how an IT department will operate and what components will be purchased.

IT also includes the management of data, whether it is in the form of text, voice, image, audio or some other form. It can also involve things related to the Internet. This gives IT a whole new meaning, since the Internet is its own realm. IT involves the transfer of data, so it makes sense that the Internet would be a part of IT. IT has become a part of our everyday lives and continues to proliferate into new realms.

3. IT JOBS

IT (information technology) is the broad subject concerned with all aspects of managing and processing information, especially within a large organization or company. IT is generally not used in reference to personal or home computing and networking. While IT is often used to describe computers and computer networks, it actually includes all layers of all systems within an organization — from the physical hardware to the operating systems, applications, databases, storage, servers and more. Telecommunication technologies, including Internet and business phones are also part of an organization's IT infrastructure.

An information technology specialist applies technical expertise to the implementation, monitoring, or maintenance of IT systems. Specialists typically focus on a specific computer network, database, or systems administration function. Specialty areas include network analysis, system administration, security and information assurance, IT audit, database administration, web administration, and more.

The information technology manager is responsible for implementing and maintaining an organization's technology infrastructure. Businesses rely on a central information processing system to support efficient data management and communications. The IT manager monitors the organization's operational requirements, researches strategies and technology solutions, and builds the most cost-effective and efficient system to achieve those goals.

The information technology architect applies IT resources to meet specific business requirements. The role requires a high degree of technical expertise as well as business understanding, as IT architects determine which information technology investments will yield the best return, both in terms of hard costs and productivity benefits. IT architects strive to bring operational efficiency to an organization through information integration and management. Achieving this ideal requires

technical skill in planning, implementing, and managing IT infrastructure and information software.

The IT supervisor works with other information technology management professionals to install, maintain, and upgrade an organization's technology systems. Supervisors generally oversee a team of IT administrators and support personnel responsible for the day-to-day operation of the IT network and system components.

4. INFORMATION AND COMMUNICATIONS TECHNOLOGY

Information and communications technology (ICT) refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions. Although ICT is often considered an extended synonym for information technology (IT), its scope is more broad.

ICT has more recently been used to describe the convergence of several technologies and the use of common transmission lines carrying very diverse data and communication types and formats. Converging technologies that exemplify ICT include the merging of audiovisual, telephone and computer networks through a common cabling system. Internet service providers (ISP) commonly provide Internet, phone and television services to homes and businesses through a single optical cable. The elimination of the telephone networks has provided huge economic incentives to implement this convergence, which eliminates many of the costs associated with cabling, signal distribution, user installation, servicing and maintenance costs.

5. COMPUTER TECHNOLOGY IN LAW ENFORCEMENT

The use of computers in law enforcement has changed and developed rapidly, especially in recent years. Computers are used to hold databases of information, to run sophisticated software that can recognize faces or identify fingerprints and to connect to the Web, an avenue for communication and a rich source of intelligence. As well as desktop computers, law enforcement personnel also use mobile devices, such as laptops and tablets, to do their job.

Databases

Computer technology allows law enforcement services to store and retrieve vast amounts of data. This information can include details of incident reports, criminals' descriptions, fingerprints and other identifying marks. It can also include descriptions and registrations of vehicles involved in criminal activity. Another crucial pool of information is DNA

data taken from suspects. DNA databases allow samples of DNA taken from suspects to be matched with samples taken from crime scenes.

Sharing Information

Computers are an invaluable tool for communication between individuals, departments and law enforcement agencies. Documents, photographs and other material can be sent almost instantaneously from one location to another, saving valuable time. Email is a good example: Encrypted emails can be used to send important data securely while mitigating the risk that the information they contain will fall into the wrong hands.

Crime Scene Computing

Mobile computing devices — laptops, notebook computers and tablet PCs — are very useful to law enforcement. Armed with a laptop, a police officer can take notes, access records or contact colleagues in other districts, all without leaving a vehicle. Mobile devices can be used to check the identity or other credentials of individuals at the scene of a crime, as well as recording and tracking vital data such as vehicle license plates. Computers can also be used to track the position of GPS devices, helping law enforcement officers to find vehicles.

The Internet

The Internet is used by law enforcement agencies in innumerable regards. Web sites can be used by law enforcement agencies to educate and inform the public, appeal for information or alert people to ongoing situations such as a missing child or a felon at large. Because criminals often use the Internet to share information, it can be very useful in crime prevention and detection. For instance, those responsible for a crime sometimes incriminate themselves by discussing it on social sites such as Facebook or Twitter — this information can be used to prosecute them.

Cyber Crime

Law enforcement agencies must also use the Internet when tackling online crime. This can include the sharing of illegal material, such as pirated commercial movies or music. «Phishing» and other forms of identity theft that use email or the Internet must also be addressed using computer technology, as must attacks using viruses and hacking attacks. Law enforcements from different countries must often work together to tackle cyber crime.

6. DIGITAL FORENSICS

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events. The context is most often for usage of data in a court of law, though digital forensics can be used in other instances. The evidentiary nature of digital forensic science requires rigorous standards to stand up to cross examination in court. As a result, there have been efforts by organizations like the National Institute of Standards and Technology, which published the «Guide to Integrating Forensic Techniques into Incident Responses». Despite this, there are several challenges facing digital forensic investigators:

- How does one duplicate or preserve evidence without knowing the duplication itself inherently changed the data?
- Time lines are critical for showing who did what, and when. But digital time stamps are notoriously absent, or can be spoofed, in digital data.
- In order to be able to state conclusively that Action A caused Result B, the concept of repeatability must be introduced. This is very difficult with digital forensics.

7. CYBERFORENSICS

Cyberforensics is an electronic discovery technique used to determine and reveal technical criminal evidence. It often involves electronic data storage extraction for legal purposes. Although still in its infancy, cyberforensics is gaining traction as a viable way of interpreting evidence. Cyberforensics is also known as computer forensics.

Cybercrimes cover a broad spectrum, from email scams to downloading copyrighted works for distribution, and are fueled by a desire to profit from another person's intellectual property or private information. Cyberforensics can readily display a digital audit trail for analysis by experts or law enforcement. Developers often build program applications to combat and capture online criminals; these applications are the crux of cyberforensics. Cyberforensic techniques include:

- Cross-driven analysis that correlates data from multiple hard drives;
- Live analysis, which obtains data acquisitions before a PC is shut down;
- Deleted file recovery.

Each of the above techniques is applied to cyberforensic investigations.

8. CRIMINAL JUSTICE INFORMATION SYSTEMS

Information systems are an essential part of today's criminal justice system. An information system is a process that uses information technology to capture, transmit, store, retrieve, manipulate, or display information used in one or more business processes. In today's environment, without information systems, the components of the criminal justice system would grind to a halt.

Criminal justice agencies depend on information technology to perform their daily functions. As the world moves deeper into the information age, the need to manage information becomes ever more critical. There is no greater reliance on information technology than that found in the criminal justice system. Information technology is what makes the management of information in these environments possible. These exciting new technologies have given way to improved information-sharing efforts that enhance the effectiveness of the justice system.

Since 9/11, law enforcement has recognized the need to share information on criminal activity between justice agencies. The importance of sharing information about crimes and criminals is a key factor in the fight against terrorism. This brought about the creation of new databases to assist in this task. A vital national database developed to promote this information sharing supported by the FBI is the Law Enforcement National Database Exchange (N-DEx). N-DEx is a repository of criminal justice records, available in a secure online environment, managed by the FBI's Criminal Justice Information Services (CJIS) Division. N-DEx brings together information such as incident and case reports, arrest reports, computer-aided dispatch (CAD) calls, traffic citations, narratives, photos, supplements, booking and incarceration data, and parole/probation information. In addition, N-DEx automatically correlates and resolves data from open and closed reports to determine relationship between people, vehicles/property, locations, and/or crime characteristics. It also supports multijurisdictional task forces — enhancing national information sharing, links between regional and state systems, and effective regional information sharing. Information-sharing technologies are the wave of the future in CJIS databases.

9. IT IN CRIMINAL INVESTIGATIONS

Investigative police work is mostly about the recovery, analysis and interpretation of information about criminal offenses. Timely and accurate information is critical to the success of policing. In order to increase the probability of generating quality information, the police employ information

technologies. Information technologies appear as important instruments of criminal investigations because they facilitate creation, storage, retrieval, transfer, and application of investigation-related information. Moreover, information technologies may help produce effective use of time devoted to criminal investigation by automating some routine investigative tasks.

Due to the important role information plays in the investigative process, criminal investigation can be defined as: “The identification, interpretation and ordering of information with the objective of ascertaining whether a crime has occurred, and if so, who was involved and how”. The information work approach emphasizes the importance of information for the success of criminal investigation and implies that technologies helping police to better process information may be an important factor for solving crimes.

Studies on criminal investigation have consistently found that the quality of preliminary investigation and information collected at this stage are crucial factors for the outcome of the investigation. Existing studies generally reveal positive contributions of information systems to the police work. Several studies examined the impact of crime analysis systems and found that modus operandi systems can be effective in identifying offenders. Researches examined the effects of computing on the performance of police detectives and found that more than 80 % of detectives experienced information benefits from computing, and nearly two thirds of detectives indicated that computers assisted them in some of their arrests and clearances. The researchers examined factors affecting homicide clearance rates and found that officers’ use of information systems in their daily job has relationship with homicide clearances. They also analyzed the impact of the Integrated Ballistic Identification System (IBIS) in the Boston Police Department and showed that the IBIS system significantly improved the productivity of the Boston Police Department’s Ballistic Unit, and it was associated with a six fold increase in the monthly number of ballistic matches.

10. LAW ENFORCEMENT’S USE OF TECHNOLOGY

Law enforcement’s use of technology has been challenged by civil and privacy rights concerns and objections and directly attacked by cybersecurity threats. There is an overarching need for greater development of standard policies and procedures related to civil rights, privacy, and security. Law enforcement’s use of surveillance technologies is facing a growing raft of legal challenges. This is especially true of systems that can generate large numbers of observations of the general public, with examples including LPR

(license plate reader) systems and surveillance cameras in public areas (especially combined with automatic facial recognition technology).

Key drivers for the challenges have been perceived as inadequate privacy and civil rights policies (e.g., surveillance data collected as widely as possible for indefinite lengths of time for uncertain purposes other than that it might be useful in the future). For the cybersecurity area, a major theme is both that the cybersecurity threat is increasing rapidly and that many departments lacked knowledge of what to do to protect their systems. Directly related to sharing and displaying information are needs for requesting assistance on what to do when given information about what, when, and where criminal activity is likely to be concentrated, and by whom. Practitioners have expressed a good bit of interest in IT for responding to major events and disasters. This theme includes calls for tracking systems for responders during major events, improved unified command training for large-scale responses, and reducing the cost of homeland security supplies in general.

11. IT SYSTEMS IN POLICE WORK

The major IT systems can be grouped into the following categories:

1. **A crime reporting system.** CRISP records all reports of suspected or actual crime. Entries are required only for indictable offences (e.g. homicide or assault) or simple offences of a serious nature (such as unlawful use of a motor vehicle, unlawful possession of property).

2. **Incident-based systems for command, control and dispatch.** CAD operates within the metropolitan area and some of the larger provincial areas, and the

Incident Management System (IMS) operates in some rural and suburban areas. When a call is received from the public, the information is recorded by the police communication centre on either the CAD or IMS systems and is radioed to an available patrol unit for action. The systems record information about the call such as the nature of the offence, the name of the informant, the location of the problem and the times that the patrol car acknowledges the call, arrives and leaves the scene.

3. **Internal communications services** such as email and the Bulletin Board (Phoenix). All legislation is now recorded on the Bulletin Board for ready access to up-to-date information by police.

4. Various **indexes** (such as domestic violence, weapons, tattoos), many of which relate to legislative requirements.

5. **Traffic systems** such as Traffic Incident Recording System (TIRS) and Transport Registration and Integrated Licensing System (TRAILS).

6. **Intelligence systems** such as Intelligence Database and ARI (Activity Report Index).

7. **Other systems**, including daily activity logs of operational police; databases of persons, vehicles and vessels of interest; various forms packages (such as court briefs); human resources, financial and library management systems, electronic warrants and mobile data — MINDA (Mobile Integrated Network Data Access); and a variety of national linkages, such as NEPI (National Exchange of Police Information).

12. IT IMPACT ON POLICE PRACTICES AND PERFORMANCE

The introduction of computer technology in the mid-1970s was modest and haphazard, being directed at responding to the information needs of a specific crime problem (vehicle theft). With the advance of information technology, the use of computer systems was expanded over the next two decades to include processing of data for crime recording and investigation, communication with other government agencies, and computer-aided dispatching. Successive attempts to upgrade the information systems were made to redress technical deficiencies found by various external inquiries — quality of data, accessibility, lack of integration and various inefficiencies.

Information technology has the potential to change and improve police practices and performance in various ways. For example, computer-aided dispatch systems can be used to better manage the deployment of police vehicles and make police patrol activities more information-driven. The capability of these systems can be further enhanced by the use of global positioning systems (now widely employed in the taxi industry, among others) that provide accurate, real-time information about the location of vehicles.

Well-designed information systems can also facilitate the apprehension and detection of offenders by increasing the range and timeliness of information that investigators can access, by providing analytical tools that can be used to profile suspects and identify offending patterns, and by making it easier to identify and track repeat offenders. In addition, information technology can substantially assist problem-oriented policing activities by aiding in the identification of problem areas and addresses, by highlighting trends and patterns that warrant attention by police and other agencies and by allowing information to be shared by agencies.

13. THE POTENTIAL OF TECHNOLOGY IN POLICING

New technologies are changing almost all aspects of our society, and the field of policing is no exception. Understanding the effects of technological change is a critical issue in contemporary policing. In recent decades, there have been many important developments with respect to information technologies (IT), analytic systems, video surveillance systems, license plate readers, DNA testing, and other technologies that have far reaching implications for policing. Technology acquisition and deployment decisions are high-priority topics for police, as law enforcement agencies at all levels of government spend vast sums on technology in the hopes of improving their efficiency and effectiveness.

For a decade or more, police departments have been using a growing array of technologies, including crime mapping systems, predictive analytics software, gunshot detection systems, DNA evidence, dash cameras, body-worn cameras, social media, data mining tools, cellphone tracking, and automated monitoring of security cameras.

Technological advancements have shaped modern policing in many important ways. One need only consider that the primary police strategy for much of the 20th century — motorized preventive patrol and rapid response to calls for service — was developed in response to the invention of the automobile, two-way radio communications, and computer-aided dispatch (911) systems. More recent technological developments have also had far-reaching effects on police agencies. Information technology (IT), video surveillance systems, DNA testing, and bullet-resistant vests, for instance, are now common and critical tools in law enforcement. Contemporary concerns over homeland security and counterterrorism have created new technological problems and demands for police, as has the growth of computer-related crime. Indeed, the late 20th and early 21st centuries have been periods of particularly rapid technological change in policing.

14. IMPACT OF TECHNOLOGY ON POLICING

Modern policing technologies extend the physical capacity of police officers to see, hear, recognize, record, remember, match, verify, analyze and communicate. These might include information technologies such as computer-aided dispatch or records management systems (RMS), forensic technologies such as DNA testing tools or fingerprint readers, or data processing systems such as crime analysis or computerized mapping.

Such technological advances have great potential for enhancing police work. For example, technology may strengthen crime control by

improving the ability of police to identify and monitor offenders (particularly repeat, high-rate offenders); facilitating the identification of places and conditions that contribute disproportionately to crime; speeding the detection of and response to crimes; enhancing evidence collection; improving police deployment and strategies; creating organizational efficiencies that put more officers in the field and for longer periods of time; enhancing communication between police and citizens; increasing perceptions of the certainty of punishment; and strengthening the ability of law enforcement to deal with technologically sophisticated forms of crime (e.g., identity theft and cybercrime) and terrorism.

Technological advancements in automobiles, protective gear, weapons, and surveillance capabilities can reduce injuries and deaths to officers, suspects, and bystanders. Pressing operational needs exist in numerous areas to which technology is central, including crime analysis and information-led policing, information technology and database integration, and managing dispatch and calls for service. And to the extent that technology improves police effectiveness, strengthens communication between police and citizens, reduces negative outcomes from police actions, and increases police accountability, it may also have the added, indirect benefit of enhancing police legitimacy.

15. IT BENEFITS FOR LAW ENFORCEMENT

IT is the technology that affects almost all aspects of police work and management. IT may enhance various dimensions of police efficiency and effectiveness, such as: the speed and accuracy of crime reporting; the amount of time officers spend in the field; the ability of officers to identify persons, vehicles, and places of interest (thus enhancing both reactive and proactive field work and improving officers' ability to identify potential safety threats); the ability of detectives and officers to identify and locate suspects in criminal investigations; the capacity of managers to identify and respond to crime patterns and trends, monitor organizational performance, and assess the work and conduct of individual officers; the problem-solving capabilities of officers and managers; information exchange with the public; and the speed of administrative processes.

These benefits might be offset to some degree, however, by technical difficulties and complexities in use of the IT systems, additional time and resources devoted to maintaining the systems and meeting reporting requirements, reduced interaction with citizens (i.e., officers may become more engrossed in working with technology and less engaged with

people), and (as alluded to previously) the inability or disinterest of officers and managers to capitalize on the strategic uses of IT.

16. KEY TECHNOLOGIES IN LAW ENFORCEMENT

Developments in IT have enhanced records management, data sharing, crime analysis, and performance management in police agencies in many ways over the last few decades. The following categories of police technologies are particularly central to everyday police work and successful practices:

- Information technologies for the collection, management, and sharing of data;
- Analytic technologies such as GIS (geographic information system) and crime analysis;
- Communications technologies including those related to dispatch (e.g., next generation 911 and computer-aided dispatch with GPS tracking of patrol cars) and those for disseminating information to personnel in the field (e.g., mobile computers and wireless access systems);
- Surveillance and sensory technologies (e.g., CCTV networks, LPRs, and patrol car cameras);
- Identification technologies (e.g., DNA testing and other forensics equipment).

From among these categories, the following specific technologies to aid us in understanding the impact of technology on law enforcement should then be selected:

- Information technologies (IT), defined broadly as intra- and interagency systems for managing, sharing, and analyzing data, including mobile computers and wireless access systems for sharing information with officers in the field;
- Crime analysis, defined to include analytic processes and products of crime analysis as well as the mechanisms for disseminating results throughout the agency;
- License plate readers (LPRs);
- Patrol car video cameras;
- DNA testing technology.

These five technologies — information technology systems, crime analysis, LPRs, in-car video, and DNA analysis — are major technologies in use by many police agencies today. They reflect common types of technology used in policing more generally (i.e., informational, analytic, communications, surveillance, and forensics technologies) and could potentially have a number of intended and unintended effects in policing.

17. INFORMATION TECHNOLOGIES WITHIN POLICE AGENCIES

Information technologies (IT) within police agencies include a wide array of databases and data systems (and their supporting hardware and software) for storing, managing, retrieving, sharing, and analyzing information both within and across agencies. Common IT components in police agencies include records management systems (RMS) that capture criminal incident records, computer-aided dispatch systems that record and assign calls for service, and various other databases that may contain information and/or intelligence on persons, groups, personnel, and other matters. Police agency websites used to exchange information with community members constitute another important part of police IT systems. Finally, IT also include mobile computers and data terminals that give officers wireless access to information in the field and that allow them to file reports remotely. (Mobile computers may also be viewed as communication technologies.)

Developments in IT have enhanced records management, data sharing, crime analysis, and performance management in police agencies in many ways over the last few decades. Police use computers for records management, crime investigation, personnel records, information sharing, and dispatch. Indeed, computers are now used for these functions in a majority of all but the smallest police agencies. Agencies also use computers to support functions like automated booking, fleet management, and resource allocation. The majority of police agencies maintain electronic data on incident reports, arrests, calls for service, stolen property, and traffic citations. Other data that agencies often maintain in electronic form include warrants, criminal histories, traffic accidents, and summons. The development of IT systems for sharing and analyzing data within and across agencies has been emphasized in recent years. In many agencies, various types of records maintained by different units are now integrated and are easily accessible and searchable for officers, often remotely.

18. TECHNOLOGY SYSTEMS IN LAW ENFORCEMENT: RISKS

Technology systems have contributed significantly to the operational effectiveness and efficiency of law enforcement agencies of all types. As the ability to collect, share, and use information continues to gain momentum in modern policing, technology tools that offer agencies the chance to develop this ability are ever more omnipresent. Yet, as much as we rely on technology for some of our most sensitive and necessary activities, securing

that technology is often an afterthought to system deployment rather than being an integrated part of the strategic implementation process.

Technology continues to proliferate throughout law enforcement. Indeed, information systems are indispensable tools for effective, expedient, and well-informed policing. Technology also poses an enormous security risk. Law enforcement agencies that operate mission-critical information technology (IT) systems without adequate security controls in place put the public, themselves, and our government at extreme risk. Data contained within these systems are extraordinarily sensitive and mission-critical.

Sensitive case reports, confidential investigative data, agency intelligence, suspect and personal data, and personnel information are just a few examples of data that may be subject to compromise via a malicious hack, an untrustworthy insider, an accidental misuse of the system, and/or a natural disaster.

Creating security policies and instituting a security process has traditionally been — at best — an afterthought in many IT implementations. Too often, only marginal consideration is given to the security of a system (such as requiring passwords) when it is being developed or implemented. What is missing is the adoption of an IT security policy development process, a conscious decision by senior management to establish a formal procedure to investigate and analyze the very real security risks to the agency's IT systems, and to develop mechanisms and policies designed to mitigate those risks. Securing an information system is much more involved than merely requiring a password, applying a digital signature, or using encryption. It is an organizational strategy that must be driven by the highest levels of the organization. Having effective information technology security policies is essential to protecting the information assets of an agency from accidental or malicious compromise.

19. CRIME ANALYSIS

Crime analysis is the main analytic technology used by police today. Crime analysis involves the use of large amounts of data and modern technology — along with a set of systematic methods and techniques that identify patterns and relationships between crime data and other relevant information sources — to assist police in criminal apprehension, crime and disorder reduction, crime prevention, and evaluation. Common duties for crime analysts involve assisting detectives, mapping crime, identifying crime patterns, conducting network analysis, and compiling data for crime reporting and managerial meetings. The development and adoption of crime analysis has been an important trend in policing over the last few

decades. It has been facilitated by the improvement of police data systems and the development of computer software for specialized applications such as geographical and intelligence analyses. Computerized crime mapping is an innovation that has spread widely in policing.

Crime analysis has great potential for improving the effectiveness of police. While it has perhaps been linked most prominently to hot spots (small areas of crime concentration) policing, crime analysis is also used heavily for investigative work and can be a valuable component of problem-oriented policing. Realizing the full potential of crime analysis requires more emphasis on long-term strategic planning, more attention to developing analytical products of value to officers, and proper training, coaching, support, and reinforcement at all levels in the agency.

20. INFORMATION SHARING LEADS TO INTERAGENCY COLLABORATION

Since 9/11, federal, state, local, and tribal law enforcement agencies have worked collaboratively to detect and prevent terrorism-related and other types of criminal activity. FBI-sponsored Joint Terrorism Task Forces (JTTFs) and fusion centers represent a change in culture and a willingness to share information among agencies and across all levels of government. Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, state, local, tribal, territorial (SLTT), and private sector partners. Both are partnerships that rely on new policies, business processes, architectures, standards, and systems that provide users the ability to collaborate and share information. In addition, both resulted in key agreements and partnerships to exchange operational data reports, case files, and similar information on both open and closed investigations.

A common, although not universal, implementation approach features distributed sharing methods, which allow each organization to retain its own information and, at the same time, make it available for others to search and retrieve. Since this information may be maintained in different formats by each organization, the Law Enforcement Information Sharing Program Exchange Specification (LEXS) — a subset of the National Information Exchange Model (NIEM) — was developed to translate information shared among different law enforcement systems into a common format, enabling participants on one system to receive and use information from multiple sources.

21. NATIONAL CRIME INFORMATION CENTER

It’s been called the lifeline of law enforcement — an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year.

The National Crime Information Center, or NCIC, was launched on January 27, 1967 with five files and 356,784 records. By the end of 2015, NCIC contained 12 million active records in 21 files. During 2015, NCIC averaged 12.6 million transactions per day.

NCIC helps criminal justice professionals apprehend fugitives, locate missing persons, recover stolen property, and identify terrorists. It also assists law enforcement officers in performing their official duties more safely and provides them with information necessary to aid in protecting the general public.

About the records: The NCIC database currently consists of 21 files. There are seven property files containing records of stolen articles, boats, guns, license plates, parts, securities, and vehicles. There are 14 persons files, including: Supervised Release; National Sex Offender Registry; Foreign Fugitive; Immigration Violator; Missing Person; Protection Order; Unidentified Person; Protective Interest; Gang; Known or Appropriately Suspected Terrorist; Wanted Person; Identity Theft; Violent Person; and National Instant Criminal Background Check System (NICS) Denied Transaction. The system also contains images that can be associated with NCIC records to help agencies identify people and property items. The Interstate Identification Index, which contains automated criminal history record information, is accessible through the same network as NCIC.

How NCIC is used: Criminal justice agencies enter records into NCIC that are accessible to law enforcement agencies nationwide. For example, a law enforcement officer can search NCIC during a traffic stop to determine if the vehicle in question is stolen or if the driver is wanted by law enforcement. The system responds instantly. However, a positive response from NCIC is not probable cause for an officer to take action. NCIC policy requires the inquiring agency to make contact with the entering agency to verify the information is accurate and up-to-date. Once the record is confirmed, the inquiring agency may take action to arrest a fugitive, return a missing person, charge a subject with violation of a protection order, or recover stolen property.

22. THE INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

The Integrated Automated Fingerprint Identification System, or IAFIS, is a national fingerprint and criminal history system that responds to requests 24 hours a day, 365 days a year to help our local, state, and federal partners — and our own investigators — solve and prevent crime and catch criminals and terrorists. IAFIS provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses.

What is included in IAFIS: not only fingerprints, but corresponding criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color; and aliases. The system also includes civil fingerprints, mostly of individuals who have served or are serving in the U.S. military or have been or are employed by the federal government. The fingerprints and criminal history information are submitted voluntarily by state, local, and federal law enforcement agencies.

How big it is: AFIS is the largest criminal fingerprint database in the world, housing the fingerprints and criminal histories for more than 70 million subjects in the criminal master file, along with more than 34 million civil prints. Included in our criminal database are fingerprints from thousands of known and suspected terrorists processed by the U.S. or by international law enforcement agencies who work with us.

How fast it works: the average response time for an electronic criminal fingerprint submission is about 27 minutes, while electronic civil submissions are processed within an hour and 12 minutes. IAFIS processed more than 61 million ten-print submissions during Fiscal Year 2010.

When it started: AFIS was launched on July 28, 1999. Prior to this time, the processing of ten-print fingerprint submissions was largely a manual, labor-intensive process, taking weeks or months to process a single submission. The FBI has been the national repository for fingerprints and related criminal history data since 1924, when more than 800,000 fingerprint records from the National Bureau of Criminal Identification and Leavenworth Penitentiary were consolidated with Bureau files. The first use of computers to search fingerprint files took place in October 1980.

What's new: while IAFIS has been an effective system, criminal and terrorist threats have evolved over the past decade. Today's environment demands faster and more advanced identification capabilities. The Next Generation Identification program, or NGI, represents a quantum leap in

fingerprint identification that will help us in solving investigations, preventing crime, and apprehending criminals and terrorists.

NGI — which delivers an incremental replacement of IAFIS — widens automated fingerprint and latent search capabilities, electronic image storage, and electronic exchange of fingerprints to more than 18,000 law enforcement agencies and other authorized criminal justice partners 24 hours a day, 365 days a year. Upon completion, NGI will have the ability to process fingerprint transactions more effectively and accurately.

23. DNA TESTING

Law enforcement agencies use a variety of forensics technologies to assist them in the identification of criminal offenders. One of the most important enhancements to these capabilities in recent decades has been the development of identification tests using deoxyribonucleic acid, commonly known as DNA. DNA tests identify unique individual genetic codes from DNA samples that are extracted from biological evidence such as blood, semen, hair, and saliva.

Developed in the 1980s, DNA testing has become a common method of identification, particularly for sex crimes and other violent offenses, and it is widely viewed as the state of the art in offender identification. In the United States, DNA testing is mostly used in violent crime cases due to its expense, but its use for property crimes is also expanding.

Police may collect and use DNA evidence in a number of ways. They may use DNA testing to determine whether a particular suspect can be linked to physical evidence from a particular crime scene. They may use recovered DNA evidence from a crime scene to identify suspects, though it seems that many agencies do not understand or take advantage of this potential DNA application. Finally, police and other criminal justice agencies take DNA samples from convicted offenders and in some states from arrestees to test them for matches to evidence from unsolved crimes and for use in future investigations.

COMPREHENSION CHECK

1. Match the words to their description:

1) hot spot	**A)** the buying or selling of something, or an exchange of money
2) Internet	**B)** programs that you use to make a computer do different things
3) transaction	**C)** to watch something carefully and record your results
4) software	**D)** small area of crime concentration
5) to monitor	**E)** to prove that something is true
6) applications	**F)** the system that connects computers all over the world
7) to validate	**J)** a computer program designed for a particular purpose

2. Explain the difference between “information system” and “information technology”.

3. What IT jobs do you know?

4. What is the meaning of “information and communications technology”?

5. How is information technology used in law enforcement?

6. Name the major categories of IT systems used in police work.

7. How can information technology change and improve police practices and performance?

8. How may information technology strengthen crime control?

9. What is information-led policing?

DISCUSSION

Discuss the following statements:

A. Information technology has the potential to change and improve police practices and performance in various ways.

B. The importance of sharing information about crimes and criminals is a key factor in the fight against terrorism.

C. Technology acquisition and deployment decisions are high-priority topics for police.

D. Technological advancements in automobiles, protective gear, weapons, and surveillance capabilities can reduce injuries and deaths to officers.

UNIT 2
DATA ACCESS AND DATA CONTROL. DATABASES IN LAW ENFORCEMENT

1. DATA

Data, in the context of databases, refers to all the single items that are stored in a database, either individually or as a set. Data in a database is primarily stored in database tables, which are organized into columns that dictate the data types stored therein. So, if the “Customers” table has a column titled “Telephone Number,” whose data type is defined as “Number,” then only numerals can be stored in that column.

Data, even in a database, is rarely useful in its raw form. For example, in a banking application, data is the whole collection of bank account numbers; bank customers’ names, addresses, and ages; bank transactions and so on. Being presented with this mass of numbers will simply overwhelm the average human — an individual simply cannot process it all. However, when data is arranged relationally, it then becomes information, which is much more useful to users. For example, if the mass of numbers stored in the banking database above is used to extract the names and addresses of the top 100 clients by size of deposit, then the data has been used to provide useful information.

Data, in the context of computing, refers to distinct pieces of digital information. Data is usually formatted in a specific way and can exist in a variety of forms, such as numbers, text, etc. When used in the context of transmission media, data refers to information in binary digital format. Data is a broad term in computer technology, but it is often used to identify and separate information from mere bits. In telecommunications, data often refers to digital, rather than analog, information. Unlike analog transmissions, which require a hard-line connection for the duration of a transmission, digital data is sent in packets.

2. DATA ACCESS

Data access refers to a user's ability to access or retrieve data stored within a database or other repository. Users who have data access can store, retrieve, move or manipulate stored data, which can be stored on a wide range of hard drives and external devices.

There are two ways to access stored data: random access and sequential access. The sequential method requires information to be moved within the disk using a seek operation until the data is located. Each segment of data has to be read one after another until the requested data is

found. Reading data randomly allows users to store or retrieve data anywhere on the disk, and the data is accessed in constant time. Oftentimes when using random access, the data is split into multiple parts or pieces and located anywhere randomly on a disk. Sequential files are usually faster to load and retrieve because they require fewer seek operations.

An access code is a series of numbers and/or letters that allow access to a particular system. An access code may be a password, although passwords are generally used in conjunction with usernames. Access codes need not be attached to a specific user; many users could use the same access code for a specific system or object without being identified as a specific user. This term is also known as an access key.

The access code is also used for authentication. In telecommunications, an access code is required before a user can be connected to a specific region. National access codes are used in dialing domestic numbers, while international access codes are used in dialing international numbers. A PIN is also a sort of access code that is shared between a specific user and the system. Access codes are also used in digital systems, behaving like a locked door to limit access from the outside world. A person must have the key to gain access to the system, which is the access key or code.

3. ACCESS CONTROL

Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users must present credentials before they can be granted access. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.

For example, a key card may act as an access control and grant the bearer access to a classified area. Because this credential can be transferred or even stolen, it is not a secure way of handling access control. A more secure method for access control involves two-factor authentication. The person who desires access must show credentials and a second factor to corroborate identity. The second factor could be an access code, a PIN or even a biometric reading. There are three factors that can be used for authentication:

- Something only known to the user, such as a password or PIN;
- Something that is part of the user, such as a fingerprint, retina scan or another biometric measurement;
- Something that belongs to the user, such as a card or a key.

For computer security, access control includes the authorization, authentication and audit of the entity trying to gain access. Access control models have a subject and an object. The subject — the human user — is the one trying to gain access to the object — usually the software. In computer systems, an access control list contains a list of permissions and the users to whom these permissions apply. Such data can be viewed by certain people and not by other people and is controlled by access control. This allows an administrator to secure information and set privileges as to what information can be accessed, who can access it and at what time it can be accessed.

4. DATA AVAILABILITY

Data availability is the process of ensuring that data is available to end users and applications — when and where they need it. It defines the degree or extent to which data is readily usable along with the necessary IT and management procedures, tools and technologies required to enable, manage and continue to make data available. Data availability is primarily used to create service level agreements (SLA) and similar service contracts, which define and guarantee the service provided by third-party IT service providers. Typically, data availability calls for implementing products, services, policies and procedures that ensure that data is available in normal and even in disaster recovery operations. This is usually done by implementing data/storage redundancy, data security, network optimization, data security and more. Storage area networks (SAN), network attached storage and RAID-based storage systems are popular storage management technologies for ensuring data availability.

5. DATA FORENSICS

Data forensics, often used interchangeably with computer forensics, is essentially the study of digital data and how it is created and used for the purpose of an investigation. Data forensics is part of the greater discipline of forensics, in which various types of evidence are studied to investigate an alleged crime.

Data forensics can involve many different tasks, including data recovery or data tracking. Data forensics might focus on recovering information on the use of a mobile device, computer or other device. It might cover the tracking of phone calls, texts or emails through a network. Digital forensics investigators may also use various methodologies to pursue data forensics, such as decryption, advanced system searches, reverse engineering, or other high-level data analyses. Some experts make

a distinction between two types of data collected in data forensics. One is persistent data, which is permanently stored on a drive and is therefore easier to find. The other is volatile data, or data that is transient and elusive. Data forensics often focuses on volatile data, or on a mix of data that has become difficult to recover or analyze for some reason. In other cases, data forensics professionals focus on persistent data that is easy to come by but must be assessed in depth in order to prove criminal intent.

6. DATABASE (DB)

A database (DB), in the most general sense, is an organized collection of data. More specifically, a database is an electronic system that allows data to be easily accessed, manipulated and updated. In other words, a database is used by an organization as a method of storing, managing and retrieving information. Modern databases are managed using a database management system (DBMS). Software programmers are well acquainted with database concepts through relational databases like Oracle, SQL SERVER and MySQL, etc. Typically, a database structure stores data in a tabular format. Database architecture may be external, internal or conceptual. The external level specifies the way in which every end-user type comprehends the organization of its corresponding relevant data in the database. The internal level deals with the performance, scalability, cost and other operational matters. The conceptual level perfectly unifies the different external views into a defined and wholly global view. It consists of every end-user required generic data.

7. DATABASE BACKUP

Database backup is the process of backing up the operational state, architecture and stored data of database software. It enables the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost. Database backup is a way to protect and restore a database. It is performed through database replication and can be done for a database or a database server. Typically, database backup is performed by the RDBMS or similar database management software. Database administrators can use the database backup copy to restore the database to its operational state along with its data and logs. The database backup can be stored locally or on a backup server. Database backup is also created/performed to ensure a company’s compliance with business and government regulations and to maintain and ensure access to critical/essential business data in case of a disaster or technical outage.

8. DATABASE ENCRYPTION AND DECRYPTION

Database encryption is the process of converting data, within a database, in plain text format into a meaningless cipher text by means of a suitable algorithm. Database decryption is converting the meaningless cipher text into the original information using keys generated by the encryption algorithms. Database encryption can be provided at the file or column level. Encryption of a database is costly and requires more storage space than the original data. The steps in encrypting a database are:

- Determine the criticality of the need for encryption;
- Determine what data needs to be encrypted;
- Determine which algorithms best suit the encryption standard;
- Determine how the keys will be managed.

Numerous algorithms are used for encryption. These algorithms generate keys related to the encrypted data. These keys set a link between the encryption and decryption procedures. The encrypted data can be decrypted only by using these keys. Different databases, such as SQL, Oracle, Access and DB2, have unique encryption and decryption methods.

9. DATABASE SECURITY

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment. Database security covers and enforces security on all aspects and components of databases. This includes:

- Data stored in database;
- Database server;
- Database management system (DBMS);
- Other database workflow applications.

Database security is generally planned, implemented and maintained by a database administrator and or other information security professional.

Some of the ways database security is analyzed and implemented include:

- Restricting unauthorized access and use by implementing strong and multifactor access and data management controls;
- Load stress testing and capacity testing of a database to ensure it does not crash in a distributed denial of service (DDoS) attack or user overload;

- Physical security of the database server and backup equipment from theft and natural disasters;
- Reviewing existing system for any known or unknown vulnerabilities and defining and implementing a road map/plan to mitigate them.

10. DATABASES IN LAW ENFORCEMENT

Data Exchange

The success of international police investigations is dependent upon the availability of up-to-date, global data. At Interpol, we provide our member countries with instant, direct access to a number of criminal databases. These contain millions of records, contributed by countries across the world. All databases, except IBIN (Interpol Ballistic Information Network), are accessible real-time through the I-24/7 network which connects all Interpol National Central Bureaus (NCBs). We have developed web server solutions to extend access beyond our NCBs to frontline law enforcement officers, such as border guards, allowing them to search the databases on wanted persons, stolen and lost travel documents and stolen motor vehicles.

As national boundaries become increasingly meaningless to criminals, effective and timely police communication across borders is more important than ever before. At Interpol, one of our priorities is to enable the world's police to exchange information securely and rapidly. Two tools deliver this aim: I-24/7 and I-link. I-24/7 is a secure global police network. We developed the I-24/7 global police communications system to connect law enforcement officers in all our member countries. It enables authorized users to share sensitive and urgent police information with their counterparts around the globe, 24 hours a day, 365 days a year. I-link is a dynamic web application that allows officers in member countries to manage their data directly, and standardizes the format of the data exchanged.

I-24/7 is the network that enables investigators to access Interpol's range of criminal databases. Authorized users can search and cross-check data in a matter of seconds, with direct access to databases on suspected criminals or wanted persons, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of art.

Empowering frontline officers. With I-24/7 installed at all National Central Bureaus, we are now focusing on extending access to Interpol services beyond the NCB and out to frontline officers such as immigration and customs officials. Different technical solutions are available and give officers in strategic locations direct access to three key Interpol databases:

those on nominal data, stolen and lost travel documents, and stolen motor vehicles.

Supporting all operational activity. The I-24/7 network underpins all Interpol operational activity. From routine checks at border crossings to targeted operations against different crime areas, and from the deployment of specialized response teams to the search for international fugitives, I-24/7 is the foundation of information exchange between the world's police.

11. INDIVIDUALS AND NOTICES

Notices and nominal data. Interpol Notices are international requests for cooperation or alerts allowing police in member countries to share critical crime-related information. Interpol’s system of Notices is used to issue international alerts for fugitives, suspected criminals, persons linked to or of interest in an ongoing criminal investigation, persons and entities subject to UN Security Council Sanctions, potential threats, missing persons and dead bodies. Details are stored in a database known as the Interpol Criminal Information System, which also contains personal data and the criminal history of people subject to request for international police cooperation. In the case of Red Notices, the persons concerned are wanted by national jurisdictions for prosecution or to serve a sentence based on an arrest warrant or court decision. Interpol's role is to assist the national police forces in identifying and locating these persons with a view to their arrest and extradition or similar lawful action. In addition, Notices are used by the United Nations, International Criminal Tribunals and the International Criminal Court to seek persons wanted for committing crimes within their jurisdiction, notably genocide, war crimes, and crimes against humanity.

Child abusers and victims. Managed by Interpol, the International Child Sexual Exploitation image database (ICSE DB) is a powerful intelligence and investigative tool which allows specialized investigators to share data with colleagues across the world. Available through Interpol's secure global police communications system (known as I-24/7), the International Child Sexual Exploitation image database uses sophisticated image comparison software to make connections between victims, abusers and places. The aim is to identify, locate and arrest perpetrators, and to remove victims from harm.

Backed by the G8 and funded by the European Commission, the ICSE DB was launched in March 2009 as the successor to the Interpol Child Abuse Image Database (ICAID) which had been in use since 2001. The ICSE DB enables certified users in member countries to access the

database directly and in real time, thereby providing immediate responses to queries related to child sexual exploitation investigations. In February 2016 the third version of ICSE was released, extensively expanding the database's features to include video analysis tools as well as cutting-edge technology aimed at supporting investigators' efforts to identify victims depicted in child sexual exploitation images and videos. By the end of 2015, the ICSE DB included data on more than 8,000 identified victims from nearly 50 countries, as well as data related to numerous unidentified victims, whose cases are yet to be investigated.

12. INTERPOL'S DNA DATABASE

Deoxyribonucleic acid (DNA) molecules contain the information all living cells in the human body need to function. They also control the inheritance of characteristics from parents to offspring. With the exception of identical twins, each person's DNA is unique, which makes DNA sampling useful for solving crimes, identifying victims of disasters, and locating missing persons.

The first step in obtaining DNA profiles for comparison is the collection of samples from crime scenes and reference samples from suspects. Samples are commonly obtained from blood, hair or body fluids. Advances in DNA technology enable samples to be obtained from decreasingly smaller traces of DNA found at crime scenes. Using forensic science methods, the sample is analysed, resulting in a DNA profile that can be compared against other DNA profiles within a database. This creates the opportunity for 'hits' — person-to-scene, scene-to-scene or person-to-person matches — where no previous connection was known.

Police in member countries can submit a DNA profile from offenders, crime scenes, missing persons and unidentified bodies to Interpol's automated DNA database. The database search result is provided within 15 minutes. Known as the DNA Gateway, the database was initiated in 2002 and by October 2015 contained more than 158,000 DNA profiles contributed by 73 member countries.

Participating countries actively use the DNA Gateway as a tool in their criminal investigations, and it regularly detects potential links between DNA profiles submitted by member countries. Searches of the database by member countries led to 72 international hits during the period from January to October 2015. Member countries can access the database via the organization's I-24/7 global police communications system and, upon request, access can be extended beyond the member countries' National Central Bureaus to forensic centres and laboratories.

Data protection**.** Interpol serves only as the conduit for the sharing and comparison of information. We do not keep any nominal data linking a DNA profile to any individual. A DNA profile is simply a list of numbers based on the pattern of an individual's DNA, producing a numerical code which can be used to differentiate individuals.

13. FINGERPRINTS DATABASE

Fingerprint evidence plays a crucial role in criminal investigations. Since a person's fingerprints are unique and do not change during the course of their life, they can be used to quickly and efficiently confirm or disprove a person's identity, for example, in checking a suspect at a border crossing. In addition, finger marks can be collected at a crime scene and have the potential to link a series of crimes together, or to place a suspect at the scene. Fingerprints play an equally important role in identifying victims following a disaster such as a cyclone, earthquake, bombing or other attack.

At Interpol, we manage a database of fingerprints, containing more than 233,000 fingerprint records (as of October 2015). Authorized users in member countries can view, submit and cross-check fingerprint records using I-24/7, Interpol's secure global police communications network, via a user-friendly automatic fingerprint identification system (AFIS).

Law enforcement officers can either take fingerprints using an electronic device or can take them manually using ink and paper, then use a special scanner to save the data electronically in the appropriate format. They then submit the data to the Interpol General Secretariat to be uploaded to the database. Records are saved and exchanged in the format set by the National Institute of Standards and Technology (NIST). We actively encourage member countries to use the database as extensively as possible, in accordance with Interpol's Rules on the Processing of Data, and increase the number of relevant fingerprints in the system. In order to assist member countries improve the quality and quantity of fingerprint records submitted to Interpol AFIS, we have prepared two documents: Guidelines concerning Fingerprints Transmission and Guidelines concerning transmission of Fingerprint Crime Scene Marks. During the period from January to October 2015, we made more than 1,900 identifications as a result of increased data sharing and comparison by member countries.

Innovation. The Interpol Fingerprint Unit provides a service called AFIS gateway, which allows member countries to submit remotely a fingerprint search against the Interpol AFIS database and receive an

automated response. We implemented in 2010 a new AFIS which is capable of searching and filing palm prints and latent palm marks. Automated ten-print verification has been introduced, along with a high-volume search facility that allows more than 1,000 comparisons per day against the Interpol fingerprint database which runs 24 hours a day, seven days a week.

14. DISASTER VICTIM IDENTIFICATION (DVI) DATABASE

The process of identifying victims of major disasters such as terrorist attacks or earthquakes is rarely possible by visual recognition. Comparison of fingerprints, dental records or DNA samples with ones stored in databases or taken from victims' personal effects are often required to obtain a conclusive identification. As people are traveling more and more, there is also a high probability that a disaster will result in the deaths of nationals from many different countries.

International coordination. When a major disaster occurs, one country alone may not have sufficient resources to deal with mass casualties. In some cases, the incident may have damaged or destroyed the country's existing emergency-response infrastructure, making the task of victim identification even more difficult. A coordinated effort by the international community can significantly speed up the victim recovery and identification process, enabling victims' families to begin the healing process and societies to rebuild, and, in the event of a terrorism incident, assisting investigators to identify possible attackers.

A range of support. Member countries can call on Interpol for assistance in disaster victim identification (DVI) immediately in the aftermath of a disaster. The services offered by Interpol include:

- A downloadable DVI guide;
- Assistance from the Command and Coordination Centre at the Interpol General Secretariat in Lyon, France, to send messages between National Central Bureaus 24 hours a day in Arabic, English, French or Spanish;
- An Incident Response Team to provide further assistance upon request, such as on-site investigative support or connection to Interpol's databases.

Multi-dimensional approach. Interpol's DVI activities are supported by a Steering Group and a Standing Committee on Disaster Victim Identification, both of which are made up of forensic and police experts. The Steering Group formulates Interpol DVI policy and strategic planning while the Standing Committee meets regularly to discuss improvements to

procedures and standards in DVI matters. Policies and guidelines have been produced in the following areas and are backed up by training programmes:

- Victim care and family support;
- Occupational care for DVI teams;
- Compliance with international standards and forensic quality assurance controls;
- Information-sharing and exchange;
- Operational assistance to countries which lack DVI capacity.

15. FACIAL RECOGNITION DATABASE

Facial recognition is an important and rapidly evolving biometric science which opens up many new opportunities for identifying individuals and solving crimes. Interpol has created a database of facial images. This tool will enable the global law enforcement community to share and compare data in order to:

- Identify fugitives and missing persons;
- Identify unknown persons of interest;
- Identify subjects in public media images;
- Verify mugshots received against a database.

In a related project, we plan to make selected images available through mobile devices in order to assist operations and investigations in the field. This will enable the Organization to carry out facial recognition checks in real time against specific watchlists.

Promoting standards and best practice. A Facial Expert Working Group (IFEWG) meets twice a year and serves as Interpol's advisory group in this biometric field. The group has produced a best practice guide for the quality, format and transmission of images to be used in the Interpol facial recognition system. The guide will help improve the quality of data received, promoting accurate and effective facial recognition.

16. STOLEN PROPERTY DATABASE

Stolen motor vehicles, vessels and works of art are likely to be trafficked across borders. We maintain global databases in order to assist the law enforcement community in identifying stolen items and to increase the chance of their recovery.

Motor vehicles. This database contains extensive identification details from all types of motor vehicles (cars, trucks, trailers, heavy machinery, motorbikes) and identifiable spare parts reported as stolen.

Vessels. The Stolen Vessels database serves as a centralized tool for tracing and tracking stolen vessels and engines.

Works of art. The Works of Art database contains descriptions and pictures of cultural objects reported as stolen by Interpol member countries and international partners such as the International Council of Museums and UNESCO. It includes items looted during crisis periods in Afghanistan, Iraq and Syria.

Vehicle crime is a highly organized criminal activity affecting all regions of the whole world and with clear links to organized crime and terrorism. Vehicles are not only stolen for their own sake, but are also trafficked to finance other crimes. They can also be used as bomb carriers or in the perpetration of other crimes.

17. STOLEN MOTOR VEHICLE DATABASE

The Interpol Stolen Motor Vehicle (SMV) database is a vital tool in the fight against international vehicle theft and trafficking. It allows police in our member countries to run a check against a suspicious vehicle and find out instantly whether it has been reported as stolen. An international database of this nature is crucial as vehicles are often trafficked across national borders, sometimes ending up thousands of miles away from the location where they were stolen. In 2015, around 123,000 motor vehicles worldwide were identified as stolen, thanks to the SMV database. By the end of the year, the number of database records had risen to 7.4 million.

Global initiatives. At Interpol, we have set up a number of working groups, bringing together experts from across the world. These working groups have developed a range of projects focusing on specific issues, for example:

- Delivering training (Project Formatrain);
- Working with car manufacturers (Project INVEX);
- Supporting operations (SMV Task Force).

We also organize the Global Conference on Vehicle Crime, bringing together the law enforcement community, international organizations and the private sector in order to share expertise and best practices. The most recent edition of the conference took place in Thailand in February 2016.

Analytical report. This report presents an analytical overview of vehicle crime in a global perspective. The findings are based on a joint initiative with Europol in which information was submitted by more than 50 member countries. The report will serve as a starting point for future in-depth analysis of the different aspects of international car trafficking.

18. WORKS OF ART DATABASE

The illicit traffic in cultural heritage is a transnational crime that affects the countries of origin, transit and final destination. The illicit trade in works of art is sustained by the demand from the arts market, the opening of borders, the improvement in transport systems and the political instability of certain countries. Over the past decade we have seen an increasing trend of illicit trafficking in cultural objects from counties in the Middle East affected by armed conflict. The black market in works of art is becoming as lucrative as those for drugs, weapons and counterfeit goods. In February 2015, the United Nations Security Council approved Resolution 2199, calling for countries to take appropriate steps to prevent the trade in stolen Iraqi and Syrian cultural property. It also recognized the global role of Interpol in addressing this illicit trade.

At Interpol, we are working to raise awareness of the problem among the relevant organizations and the general public. We encourage not only police, but also art and antiques dealers and owners of works of art to play an active role in the exchange of information. This combined action will strengthen our efforts to curb the erosion of our cultural heritage.

International data. The efficient exchange of data is central to these efforts. Interpol's database of stolen works of art is a key tool, accessible to law enforcement agencies and other authorized users across the world. In addition, certain types of data can be accessed openly by the general public:

- The most recent stolen works of art reported to Interpol;
- Recovered works of art;
- Works of art that have been recovered but remain unclaimed by their owners;
- Stolen Afghan items;
- Stolen Iraqi items;
- Stolen Syrian items;
- Stolen Libyan items.

The database contains only those objects that have been officially reported as stolen by member countries. An object may have been stolen, but is not included in the database for one of the following reasons:

- It has not yet been reported as stolen to the police;
- The theft report has not yet been received at Interpol through official channels;
- The object has not yet been entered into the database;
- Searches for the object are being carried out at national level only;

- The object has been looted from an archaeological site and is not known to the police.

We therefore encourage users to interpret database results with caution as an object may have been stolen, even if it does not appear in the Interpol database. A database of stolen works of art combines descriptions and pictures of around 48,768 items (as at 7 June 2016). Direct access to the database was made available in 2009, enabling authorized users to check in real-time if an item is among the registered objects.

19. FIREARMS AND DANGEROUS MATERIALS DATABASE

We offer powerful tools which can help member countries to collect data, trace items and analyse trends related to firearms and radiological and nuclear materials.

Identification of firearms. The Interpol Firearms Reference Table provides a standardized methodology to identify and describe firearms, and enables an investigator to obtain or verify the details of a firearm. The Interpol Firearms Reference Table (IFRT) is an interactive online tool available to authorized users via Interpol's restricted website. It utilizes a standardized methodology to identify and describe firearms, and enables an investigator to obtain or verify the details of a firearm — including the make, model, calibre and serial number. This information is regularly updated in consultation with firearm experts. Interpol also welcomes input from the law enforcement community to identify additional firearms for inclusion in the IFRT. The IFRT contains:

- More than 250,000 firearm references;
- More than 57, 000 firearm images;
- Extensive information on firearm markings including trademarks, logos and insignias;
- Thousands of useful definitions and terms for firearm parts, accessories, functions and processes;
- Company histories;
- Acronyms;
- Manufacturers' codes.

The proper identification and description of a specific firearm is a fundamental aspect of a firearm-related crime investigation, and significantly increases the chances of acquiring firearm ownership history through an international trace request. As such, we recommend that all iARMS users consult the IFRT in order to verify the unique identifiers of a firearm for which a search will be conducted, or for which a trace request will be created.

20. EXCHANGE OF FIREARMS DATA

The Interpol Illicit Arms Records and tracing Management System (iARMS) facilitates information exchange and investigative cooperation between law enforcement agencies on firearm-related crime, and allows them to trace a firearm from the point of manufacture or of legal importation into a country, through the lines of supply to the last known point of possession. iARMS is an integral part of the international strategy and operational framework to combat the illicit trade in small arms and light weapons. iARMS is an information technology system which provides a common global platform for firearm-related information exchange and cooperation, namely through:

- Providing a centralized system for the reporting and querying of lost, stolen, trafficked and smuggled firearms by law enforcement agencies globally;
- Facilitating the submission of, and responses to, international firearms trace requests including support to monitor the status of trace requests.

Firearms of interest. For the purposes of iARMS, a firearm is deemed to be "illicit" if:

- It is considered illicit under the law of the country in whose territorial jurisdiction it is found; or
- It is transferred in violation of an arms embargo decided by the United Nations Security Council in accordance with the Charter of the United Nations; or
- It is not marked in accordance with the International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons (International Tracing Instrument); or
- It is manufactured or assembled without a license or authorization from the competent authority of the country where the manufacture or assembly takes place; or
- It is transferred without a license or authorization as required by a competent national authority.

Radiological and nuclear materials. The Project Geiger database is used to collate and analyse information on illicit trafficking and other unauthorized activities involving radiological and nuclear materials. It combines data from the International Atomic Energy Agency, open-source reports and law enforcement channels.

COMPREHENSION CHECK

1. Match the words to their description:

1) database	**A)** to change electronic information into a secret system of letters, numbers, or symbols:
2) access code	**B)** an organized collection of data
3) recovery	**C)** a way of limiting access to a system or to physical or virtual resources
4) to encrypt	**D)** to add new information
5) to update	**E)** information in the form of text, numbers, or symbols that can be used by or stored in a computer
6) access control	**F)** a series of numbers and/or letters that allow access to a particular system
7) data	**J)** a process in which a system or situation returns to the way it was before something bad happened

2. Why DNA sampling is useful for solving crimes, identifying victims of disasters, and locating missing persons?

3. Why does fingerprint evidence play a crucial role in criminal investigations?

4. Explain the purpose of two-factor authentication.

5. What tasks does data forensics involve?

6. What is a database backup?

7. Name some of the ways database security is analyzed and implemented.

8. What are the steps in encrypting a database?

9. Why can fingerprints be used to quickly and efficiently confirm or disprove a person's identity?

10. What is the purpose of Interpol's system of Notices?

DISCUSSION

Discuss the following statements:

A. For computer security, access control includes the authorization, authentication and audit of the entity trying to gain access.

B. As national boundaries become increasingly meaningless to criminals, effective and timely police communication across borders is more important than ever before.

C. The success of international police investigations is dependent upon the availability of up-to-date, global data.

UNIT 3
INFORMATION ASSURANCE AND INFORMATION SECURITY. SECURE CODING

1. INFORMATION ASSURANCE (IA)

Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. There are commonly five terms associated with the definition of information assurance: Integrity, Availability, Authentication, Confidentiality, Nonrepudiation.

IA is a field in and of itself. It can be thought of as a specialty of Information Technology (IT), because an IA specialist must have a thorough understanding of IT and how information systems work and are interconnected. With all of the threats that are now common in the IT world, such as viruses, worms, phishing attacks, social engineering, identity theft and more, a focus on protection against these threats is required. IA is that focus. Essentially, Information Assurance is protecting information systems through maintaining these five qualities of the system.

Integrity involves making sure that an information system remains unscathed and that no one has tampered with it. IA takes steps to maintain integrity, such as having anti-virus software in place so that data will not be altered or destroyed, and having policies in place so that users know how to properly utilize their systems to minimize malicious code from entering them.

Availability is the facet of IA where information must be available for use by those that are allowed to access it. Protecting the availability can involve protecting against malicious code, hackers and any other threat that could block access to the information system.

Authentication involves ensuring that users are who they say they are. Methods used for authentication are user names, passwords, biometrics, tokens and other devices. Authentication is also used in other ways — not just for identifying users, but also for identifying devices and data messages.

IA involves keeping information confidential. This means that only those authorized to view information are allowed access to it. Information needs to be kept confidential. This is commonly found, for example, in the military, where information is classified or only people with certain clearance levels are allowed access to highly confidential information.

The final pillar is nonrepudiation. This means that someone cannot deny having completed an action because there will be proof that they did it.

2. INFORMATION SECURITY (IS)

Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. This triad has evolved into what is commonly termed the Parkerian hexad, which includes confidentiality, possession (or control), integrity, authenticity, availability and utility.

Information security handles risk management. Anything can act as a risk or a threat to the CIA triad or Parkerian hexad. Sensitive information must be kept — it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient. Good cryptography tools can help mitigate this security threat.

Digital signatures can improve information security by enhancing authenticity processes and prompting individuals to prove their identity before they can gain access to computer data.

3. CIA TRIAD OF INFORMATION SECURITY

The CIA (Confidentiality, Integrity, and Availability) triad of information security is an information security benchmark model used to evaluate the information security of an organization. The CIA triad of information security implements security using three key areas related to information systems including confidentiality, integrity and availability.

The CIA triad of information security was created to provide a baseline standard for evaluating and implementing information security regardless of the underlying system and/or organization. The three core goals have distinct requirements and processes within each other.

- Confidentiality: Ensures that data or an information system is accessed by only an authorized person. User Id’s and passwords, access control lists (ACL) and policy based security are some of the methods through which confidentiality is achieved.
- Integrity: Integrity assures that the data or information system can be trusted. Ensures that it is edited by only authorized persons and remains in its original state when at rest. Data encryption and hashing algorithms are key processes in providing integrity.
- Availability: Data and information systems are available when required. Hardware maintenance, software patching/upgrading and network optimization ensure availability.

4. CONFIDENTIALITY

Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders. Confidentiality is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, integrity and nonrepudiation. Sensitive information or data should be disclosed to authorized users only. In IA, confidentiality is enforced in a classification system. For example, a U.S. government or military worker must obtain a certain clearance level, depending on a position's data requirements, such as, classified, secret or top secret. Those with secret clearances cannot access top secret information.

Best practices used to ensure confidentiality are as follows:

- An authentication process, which ensures that authorized users are assigned confidential user identification and passwords. Another type of authentication is biometrics.
- Role-based security methods may be employed to ensure user or viewer authorization. For example, data access levels may be assigned to specified department staff.
- Access controls ensure that user actions remain within their roles. For example, if a user is authorized to read but not write data, defined system controls may be integrated.

5. INTEGRITY

Integrity, in the context of computer systems, refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification. Integrity is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, confidentiality and nonrepudiation. Data integrity maintenance is an information security requirement. Integrity is a major IA component because users must be able to trust information. Untrusted data is devoid of integrity. Stored data must remain unchanged within an information system (IS), as well as during data transport.

Events like storage erosion, error and intentional data or system damage can create data changes. For example, hackers may cause damage by infiltrating systems with malware, including Trojan horses, which overtake computer systems, as well as worms and viruses. An employee may create company damage through intentionally false data entry. Data integrity verification measures include checksums and the use of data comparisons.

6. AVAILABILITY

Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format. Availability is one of the five pillars of Information Assurance (IA). The other four are integrity, authentication, confidentiality and nonrepudiation. When a system is regularly non-functioning, information availability is affected and significantly impacts users. In addition, when data is not secure and easily available, information security is affected, i.e., top secret security clearances. Another factor affecting availability is time. If a computer system cannot deliver information efficiently, then availability is compromised.

Data availability must be ensured by storage, which may be local or at an offsite facility. In the case of an offsite facility, an established business continuity plan should state the availability of this data when onsite data is not available. At all times, information must be available to those with clearance.

7. NONREPUDIATION

Nonrepudiation is a method of guaranteeing message transmission between parties via digital signature and/or encryption. It is one of the five pillars of information assurance (IA). The other four are availability, integrity, confidentiality and authentication. Nonrepudiation is often used for digital contracts, signatures and email messages. By using a data hash, proof of authentic identifying data and data origination can be obtained. Along with digital signatures, public keys can be a problem when it comes to nonrepudiation if the message recipient has exposed, either knowingly or unknowingly, their encrypted or secret key.

While nonrepudiation is a worthy electronic security measure, professionals in this arena caution that it may not be 100 percent effective. Phishing or man-in-the-middle (MITM) attacks can compromise data integrity. In addition, it is important to note that a digital signature is the same whether it is authentic or faked by someone who has the private key. This problem has been countered by the U.S. Department of Defense with the development of the common access card, a type of smart card designed for active duty military personnel, civilian personnel, the National Guard and others that are privy to confidential defense information.

Imagine receiving a harassing email from someone who denies sending the message. How do you determine the truth? Digital signatures prove the delivery and receipt of email transmissions, guaranteeing nonrepudiation. Thus, nonrepudiation protects the recipient and the sender

when a recipient denies receiving an email. Without nonrepudiation, an essential pillar of IA, information security would be significantly flawed.

8. AUTHORIZATION

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification. System administrators (SA) are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

Modern and multiuser operating systems depend on effectively designed authorization processes to facilitate application deployment and management. Key factors include user type, number, credentials requiring verification and related actions and roles. For example, role-based authorization may be designated by user groups requiring specific user resource tracking privileges. Additionally, authorization may be based on an enterprise authentication mechanism, like Active Directory (AD), for seamless security policy integration.

For example, ASP.NET works with Internet Information Server (IIS) and Microsoft Windows to provide authentication and authorization services for Web-based .NET applications. Windows uses New Technology File System (NTFS) to maintain Access Control Lists (ACL) for all resources. The ACL serves as the ultimate authority on resource access. The .NET Framework provides an alternate role-based security approach for authorization support. Role-based security is a flexible method that suits server applications and is similar to code access security checks, where authorized application users are determined according to roles.

9. AUTHENTICATION

In the context of computer systems, authentication is a process that ensures and confirms a user’s identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and nonrepudiation.

Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers.

A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e., retina or fingerprints). This technology makes it more difficult for hackers to break into computer systems. The Public Key Infrastructure (PKI) authentication method uses digital certificates to prove a user's identity. There are other authentication tools, too, such as key cards and USB tokens. One of the greatest authentication threats occurs with email, where authenticity is often difficult to verify. For example, unsecured emails often appear legitimate.

10. INFORMATION SYSTEMS SECURITY (INFOSEC)

Information systems security, more commonly referred to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.

It also refers to:

- Access controls, which prevent unauthorized personnel from entering or accessing a system;
- Protecting information no matter where that information is, i.e. in transit (such as in an email) or in a storage area;
- The detection and remediation of security breaches, as well as documenting those events.

Information systems security does not just deal with computer information, but also protecting data and information in all of its forms, such as telephone conversations. Risk assessments must be performed to determine what information poses the biggest risk. For example, one system may have the most important information on it and therefore will need more security measures to maintain security. Business continuity planning and disaster recovery planning are other facets of an information systems security professional. This professional will plan for what could happen if a major business disruption occurs, but still allow business to continue as usual.

The term is often used in the context of the U.S. Navy, who defines INFOSEC as: COMPUSEC + COMSEC + TEMPEST = INFOSEC. Where COMPUSEC is computer systems security, COMSEC is communications security, and TEMPEST is compromising emanations.

11. COMPUTER SECURITY (COMPUSEC)

COMPUter SECurity (COMPUSEC) is a military term used in reference to the security of computer system information. Today it can relate to either the military or civilian community. COMPUSEC also concerns preventing unauthorized users from gaining entry to a computer system.

The differences between communications security (COMSEC) and COMPUSEC is that COMSEC is involved with data that is being transmitted and protecting the data while being transmitted. COMPUSEC concerns itself with protecting data during the act of processing or while being stored. One of the first devised standards for COMPUSEC was the DoD 5200.28-M, ADP Security Manual. This document contains certain essential computer system requirements, including:

- Labeling of any classified information. This involves compartmented computers — those holding information only accessible by individuals holding appropriate clearance levels.
- Keeping an audit trail of anything related to security. This could include keeping track of anyone who logged into or out of the system.
- Verifying privileges, such as whether a user can read or write. Letting only certain users have access to the memory.
- Utilizing identification, such as logins and passwords, to authenticate computer users.

Though COMPUSEC started out as a set of guidelines for protecting national assets, it now is more widespread. Later, other tools for COMPUSEC were developed and included CSC-STD-001-83, the Trusted Computer System Evaluation Criteria (TCSEC) or the Orange Book. The Orange Book took a layered approach to rating computer system requirements. It included ratings on security policy, accountability, assurance and documentation.

12. COMMUNICATIONS SECURITY (COMSEC)

Communications security (COMSEC) ensures the security of telecommunications confidentiality and integrity — two information assurance (IA) pillars. Generally, COMSEC may refer to the security of any information that is transmitted, transferred or communicated.

There are five COMSEC security types:

- Cryptosecurity: This encrypts data, rendering it unreadable until the data is decrypted;
- Emission Security (EMSEC): This prevents the release or capture of emanations from equipment, such as cryptographic equipment, thereby preventing unauthorized interception;
- Physical Security: This ensures the safety of, and prevents unauthorized access to, cryptographic information, documents and equipment;
- Traffic-Flow Security: This hides messages and message characteristics flowing on a network;
- Transmission Security (TRANSEC): This protects transmissions from unauthorized access, thereby preventing interruption and harm.

13. DATA PROTECTION

Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy.

Data protection should always be applied to all forms of data, whether it be personal or corporate. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it. The context of data protection varies and the methods and extent also vary for each; there is data protection on the personal level, that of business or public entities, and that of data so highly classified that it should never fall into the hands of others aside from its owners — or in other words, top secret.

In the United States data privacy is not highly regulated, so by extension there are no strict data protection laws that apply, although that is quickly changing as people become aware of the value of privacy and data protection. In the United Kingdom however, the legislative body passed the Data Protection Act of 1998, a revision of the very basic Act of 1984 which stated rules for data users and defined individuals' rights in regard to data that is directly related to them. The Act became effective on March 1, 2000. The law itself strives to balance the individual rights to privacy and the ability of more public organizations to use this data in the process of conducting business. The Act gives guidelines, eight principles, which a data controller must observe when handling personal data in the course of doing business, in the name of protection. These principles go along the lines of having been obtained fairly and lawfully, to it not leaving the country or territory unless under certain conditions of protection. Not all countries have data protection laws, however.

14. DATA SECURITY

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and genre. Data security is also known as information security (IS) or computer security.

Examples of data security technologies include software/hardware disk encryption, backups, data masking and data erasure. A key data security

technology measure is scrambling, where digital data, software/hardware, and hard drives are scrambled and rendered unreadable to unauthorized users and hackers. Data security is also very important for health care records, so health advocates and medical practitioners in the U.S. and other countries are working toward implementing electronic medical records (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities.

15. CODE

Code, in a general sense, is the language understood by the computer. Computers don't understand natural language. As such the human language has to be converted into a set of «words» that are understood by the computer. The words that initiate a standard action when used in a program are called keywords. The arrangement of keywords for successful execution of a desired computation is called syntax. The set of keywords and syntax form a programming language.

The term code by itself is so general that it doesn't convey much information. It can be useful to think of code in terms of instructions versus data. That is, computer code uses data as an input, does some processing, then spits out the output. In addition to referring to the code itself, you can use the term as a verb — to code is synonymous with coding or programming.

16. SECURE CODING

Secure coding is the practice of writing a source code or a code base that is compatible with the best security principles for a given system and interface. IT professionals understand that each type of device technology and operating system has its own vulnerabilities to a range of security issues, including cyber-attacks and hacking. With that in mind, the principle of secure coding helps software engineers and other developers anticipate these challenges and prepare for these issues in design.

The principle of secure coding is supported by various particular categorical strategies. For example, one strategy is to «validate input» to make sure that input comes from trusted sources. Another strategy is to check for buffer overflow vulnerability. In a general sense, developers look to design a secure user interface that limits the number of backdoors, loopholes and vulnerabilities that can invite cyber-attacks. As the security community becomes more cognizant of common hacking and cyber-attack strategies, it builds appropriate security measures into newer platforms and devices. As a result, many of the traditional vulnerabilities in PC operating

system environments have been engineered out of newer mobile or smartphone interfaces. However, as hackers, cyber-attackers and other «black hat» parties are also directing more attention toward mobile, this has become the new playground for secure coding and security work.

17. CODE EFFICIENCY

Code efficiency is a broad term used to depict the reliability, speed and programming methodology used in developing codes for an application. Code efficiency is directly linked with algorithmic efficiency and the speed of runtime execution for software. It is the key element in ensuring high performance. The goal of code efficiency is to reduce resource consumption and completion time as much as possible with minimum risk to the business or operating environment. The software product quality can be accessed and evaluated with the help of the efficiency of the code used.

Code efficiency plays a significant role in applications in a high-execution-speed environment where performance and scalability are paramount. One of the recommended best practices in coding is to ensure good code efficiency. Well-developed programming codes should be able to handle complex algorithms. Recommendations for code efficiency include:

- To remove unnecessary code or code that goes to redundant processing;
- To make use of optimal memory and nonvolatile storage;
- To ensure the best speed or run time for completing the algorithm;
- To make use of reusable components wherever possible;
- To make use of error and exception handling at all layers of software, such as the user interface, logic and data flow;
- To create programming code that ensures data integrity and consistency;
- To develop programming code that's compliant with the design logic and flow;
- To make use of coding practices applicable to the related software;
- To optimize the use of data access and data management practices;
- To use the best keywords, data types and variables, and other available programming concepts to implement the related algorithm.

18. CRYPTOGRAPHY

Cryptography involves creating written or generated codes that allows information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data. Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The

information maintains its integrity during transit and while being stored. Cryptography also aids in non-repudiation. This means that neither the creator nor the receiver of the information may claim they did not create or receive it. Cryptography is also known as cryptology.

Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include:

- Secret Key Cryptography (SKC) — Here only one key is used for both encryption and decryption. This type of encryption is also referred to as symmetric encryption;
- Public Key Cryptography (PKC): Here two keys are used. This type of encryption is also called asymmetric encryption. One key is the public key and anyone can have access to it. The other key is the private key, and only the owner can access it. The sender encrypts the information using the receiver's public key. The receiver decrypts the message using his/her private key. For non-repudiation, the sender encrypts plain text using a private key, while the receiver uses the sender's public key to decrypt it. Thus, the receiver knows the sender;
- Hash Functions: These are different from SKC and PKC. They have no key at all and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged.

19. CRYPTANALYSIS

Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems. Cryptanalysis attack types include:

- Known-Plaintext Analysis (KPA): Attacker decrypt ciphertexts with known partial plaintext;
- Chosen-Plaintext Analysis (CPA): Attacker uses ciphertext that matches arbitrarily selected plaintext via the same algorithm technique;
- Ciphertext-Only Analysis (COA): Attacker uses known ciphertext collections;
- Man-in-the-Middle (MITM) Attack: Attack occurs when two parties use message or key sharing for communication via a channel that appears secure but is actually compromised. Attacker employs this attack for the interception of messages that pass through the communications channel. Hash functions prevent MITM attacks;

- Adaptive Chosen-Plaintext Attack (ACPA): Similar to a CPA, this attack uses chosen plaintext and ciphertext based on data learned from past encryptions.

20. ENCRYPTION

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. Symmetric-key and asymmetric-key are the two primary types of encryption. Encryption is essential for ensured and trusted delivery of sensitive information.

Symmetric-key encryption uses two secret, often identical keys or codes for computers involved in message transmission. Each secret key's data packet is self-encrypted. The first symmetric encryption algorithm is the Data Encryption Standard (DES), which uses a 56-bit key and is not considered attack-proof. The Advanced Encryption Standard (AES) is considered more reliable because it uses a 128-bit, a 192-bit or a 256-bit key.

Asymmetric-key encryption, also known as public-key encryption, uses private and public keys in tandem. The public key is shared with computers attempting to communicate securely with the user’s computer. This key handles encryption, rendering the message indecipherable in transit. The private matching key remains private on the user’s computer. It decrypts the message and makes it readable. Pretty good privacy (PGP) is a commonly used public-key encryption system.

21. DATA ENCRYPTION KEY (DEK)

A data encryption key (DEK) is a type of key designed to encrypt and decrypt data at least once or possibly multiple times. DEKs are created by an encryption engine. Data is encrypted and decrypted with the help of the same DEK; therefore, a DEK must be stored for at least a specified duration for decrypting the generated cipher text.

The time period for storing data prior to its retrieval may vary significantly, and some data may be kept for many years or even decades prior to accessing it. In order to ensure that the data is still available, DEKs may also have to be retained for very long periods. A key-management system provides life-cycle supervision for every DEK generated by an encryption engine. Key-management systems are usually offered by third-party vendors. Regardless of the life-cycle length, there are four levels in a DEK life cycle:

1. The key is created using the crypto module of the encryption engine;
2. The key is then provided to a key vault and to various other encryption engines;
3. This key is utilized for encrypting and decrypting data;
4. The key is then suspended, terminated or destroyed.

A DEK may be customized to expire during a particular time frame in order to prevent data from being compromised. Under such circumstances, it should be used once more for decrypting the data and then the resulting clear text is encrypted with the help of a new key (re-keyed).

22. ENCRYPTION ALGORITHM

An encryption algorithm is a component for electronic data transport security. Actual mathematical steps are taken and enlisted when developing algorithms for encryption purposes, and varying block ciphers are used to encrypt electronic data or numbers. Encryption algorithms help prevent data fraud, such as that perpetrated by hackers who illegally obtain electronic financial information. These algorithms are a part of any company's risk management protocols and are often found in software applications. Encryption algorithms assist in the process of transforming plain text into encrypted text, and then back to plain text for the purpose of securing electronic data when it is transported over networks. By coding or encrypting data, hackers or other unauthorized users are generally unable to access such information. Some encryption algorithms are considered faster than others, but as long as algorithm developers, many of whom have math backgrounds, stay on top of advancements in this technology, this type of encryption should continue to flourish as hackers continue to become more sophisticated.

In 1977, RSA became one of the first encryption algorithms developed by U.S. mathematicians Ron Rivest, Adi Shamir and Len Adleman. RSA has had ample staying power as it is still widely used for digital signatures and public key encryption. Encryption algorithms can vary in length, but the strength of an algorithm is usually directly proportional to its length.

23. DECRYPTION

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords. One of the foremost

reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information.

24. CIPHER

A cipher is a method of hiding words or text with encryption by replacing original letters with other letters, numbers and symbols through substitution or transposition. A combination of substitution and transposition is also often employed. Cipher also refers to the encrypted text, cryptography system or encryption key for the original text. Encrypted text is also known as ciphertext. Plaintext is the original, unencrypted text. A cipher enables private communication and is often used in email, so that if an encrypted message is intercepted by an unauthorized user, the message cannot be read.

A block cipher encrypts plaintext with a key and algorithm, which affects a complete block of data containing several bits. This may mean 64 bits of encryption for every one bit of data. A stream cipher encrypts plaintext with a key and algorithm applied to every binary digit (ones and zeros) for every bit in the data stream. Today, this type of cipher is not as common as the block cipher.

A number of other cipher types exist. Two typical examples are:

- Atbash: The letter A is changed to a Z. B is changed to a Y, and so on.
- Baconian: This hides a message inside another message with various fonts, typefaces or characteristics.

25. BLOCK CIPHER

A block cipher is a symmetric cryptographic algorithm that operates on a fixed-size block of data using a shared, secret key. Plaintext is used during the encryption, and the resulting encrypted text is called a ciphertext. The same key is used for both the encryption of the plaintext and the decryption of the ciphertext. Block cipher encrypts/decrypts its input one block at a time instead of one bit at a time using a shared, secret key. The block is fixed in size; otherwise, padding is necessary. This algorithm is symmetric. During encryption, it uses the shared key to transform its plaintext input into a cyphertext (encrypted text). During decryption, it uses the same key to transform the cyphertext back to the original plaintext. The length of the output is the same as the input. Well-known implementations of the block

cipher algorithm are the Data Encryption Standard (DES), TripleDES and the Advanced Encryption standard (AES). The counterpart of block cypher is the stream cypher, which operates on its input one bit at a time, also using a shared key. An alternative to the block cipher algorithm is public-key cryptography or asymmetric cryptography. This algorithm uses a public key to encrypt plaintext and a private key to decrypt the resulting ciphertext.

26. DIGITAL SIGNATURE

A digital signature guarantees the authenticity of an electronic document or message in digital communication and uses encryption techniques to provide proof of original and unmodified documentation. Digital signatures are used in e-commerce, software distribution, financial transactions and other situations that rely on forgery or tampering detection techniques.

A digital signature is applied and verified, as follows:

- The document or message sender (signer) or public/private key supplier shares the public key with the end user(s);
- The sender, using his private key, appends the encrypted signature to the message or document;
- The end user decrypts the document and verifies the signature, which lets the end user know that the document is from the original sender.

27. CRYPTOSECURITY

Cryptosecurity is a component of communications security that deals with the creation and application of measures leading to secure ciphers and codes, which are used to protect encryption systems and methods from enemy discovery, decryption, interception and tampering. This specialty area of communications security is tasked with ensuring that messages and data retain full confidentiality and authenticity.

In communications security, controlling messages and data is key. This involves ensuring that no unauthorized source has the ability to acquire or even discover the message's existence. But in the event that the message is intercepted by unauthorized sources, it should be in a form that is encrypted so that no information can be derived from it. Cryptosecurity discipline ensures proper maintenance and use of cryptosystems that are in place.

28. NETWORK SECURITY

Network security is an over-arching term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.

This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing or altering secure information.

The first layer of network security is enforced through a username/password mechanism, which only allows access to authenticated users with customized privileges. When a user is authenticated and granted specific system access, the configured firewall enforces network policies, that is, accessible user services.

However, firewalls do not always detect and stop viruses or harmful malware, which may lead to data loss. An anti-virus software or an intrusion prevention system (IPS) is implemented to prevent the virus and/or harmful malware from entering the network. Network security is sometimes confused with information security, which has a different scope and relates to data integrity of all forms, print or electronic.

COMPREHENSION CHECK

1. Match the words to their description:

1) access control	**A)** a process that ensures and confirms a user's identity
2) classified information	**B)** prevents unauthorized personnel from entering or accessing a system
3) cryptography	**C)** refers to protective digital privacy measures
4) authentication	**D)** the process of transforming information to make it unreadable for unauthorized users
5) communications security	**E)** sensitive information to which access is restricted by law or regulation to particular classes of people
6) data security	**F)** security of any information that is transmitted, transferred or communicated
7) encryption	**J)** involves creating written or generated codes that allows information to be kept secret

2. Explain the purpose of information assurance.
3. What does information systems security deal with?
4. What is CIA Triad of information security?
5. For what purpose do users commonly enter usernames and passwords logging into a computer?
6. Name five terms associated with the definition of information assurance.
7. How can digital signatures improve information security?
8. Explain the difference between communications security and computer security.
9. Name five communications security types.

DISCUSSION

Discuss the following statements:

A. Information systems security refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.

B. Sensitive information should be disclosed to authorized users only.

C. Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions.

D. Data integrity maintenance is an information security requirement.

UNIT 4
DATA SECURITY.
PROTECTING LAW ENFORCEMENT INFORMATION

1. DATA LOSS

Data loss is any process or event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application. It occurs when one or more data elements can no longer be utilized by the data owner or requesting application. Data loss is also known as data leakage. Data loss is applicable on data both at rest and when in motion (transmitted over the network). Data loss can occur for various reasons, including:

- Data corruption;
- Data being intentionally or accidentally deleted or overwritten by a user or an attacker;
- Data stolen over the network by network penetration or any network intervention attack;
- Data storage device physically damaged or stolen;
- Virus infection deleting one or more files.

Data loss is usually prevented by implementing data backup solutions and adding strong data access controls and security mechanisms on data storage assets.

2. DATA BREACH

A data breach is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location. A data breach is also known as a data spill or data leak.

A data breach occurs when an unauthorized hacker or attacker accesses a secure database or repository. Data breaches are typically geared toward logical or digital data and often conducted over the Internet or a network connection. A data breach may result in data loss, including financial, personal and health information. A hacker also may use stolen data to impersonate himself to gain access to a more secure location. For example, a hacker's data breach of a network administrator's login credentials can result in access of an entire network.

3. SECURITY BREACH

A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter. A security breach is also known as a security violation. A security breach is one of the earliest stages of a security attack by a malicious intruder, such as a hacker, cracker or nefarious application. Security breaches happen when the security policy, procedures and/or system are violated. Depending on the nature of the incident, a security breach can be anything from low-risk to highly critical. In an organization, security breaches are typically monitored, identified and mitigated by a software or hardware firewall. If an intrusion, abnormality or violation is detected, the firewall issues a notification to the network or security administrator.

4. RISK ANALYSIS

Risk analysis is the review of the risks associated with a particular event or action. It is applied to projects, information technology, security issues and any action where risks may be analyzed on a quantitative and qualitative basis. Risk analysis is a component of risk management. Risks are part of every IT project and business endeavor. As such, risk analysis should occur on a recurring basis and be updated to accommodate new potential threats. Strategic risk analysis minimizes future risk probability and damage.

The risk management process involves a few key steps. First, potential threats are identified. For example, risks are associated with individuals using a computer either incorrectly or inappropriately, which creates security risks. Risks are also related to projects that are not completed in a timely manner, resulting in significant costs. Next, quantitative and/or qualitative risk analysis is applied to study identified risks. Quantitative risk analysis measures expected risk probability to forecast estimated financial losses from potential risks. Qualitative risk analysis does not use numbers but reviews threats, and determines and establishes risk mitigation methods and solutions. A contingency plan may be used during risk analysis. If a risk is presented, contingency plans help minimize damage.

5. VULNERABILITY

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat. Vulnerabilities are what information security and information assurance professionals seek to reduce. Cutting down vulnerabilities provides fewer options for malicious users to gain access to secure information. Computer users and network personnel can protect computer systems from vulnerabilities by keeping software security patches up to date. These patches can remedy flaws or security holes that were found in the initial release. Computer and network personnel should also stay informed about current vulnerabilities in the software they use and seek out ways to protect against them.

6. MALICIOUS SOFTWARE (MALWARE)

Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user. Malware is software designed to cause harm to a computer and user. Some forms of malware “spy” on user Internet traffic. Examples include spyware and adware. Spyware monitors a user’s location and if enabled, it can capture sensitive information, e.g., credit card numbers, promoting identity theft. Adware also acquires user information, which is shared with advertisers and then integrated with unwanted, triggered pop-up ads. Worms and viruses behave differently, as they can quickly proliferate and undermine an entire computer system. They also may perform unsavory activities from a user’s computer without the user’s knowledge. In the wake of a virus or worm, a computer system can experience significant damage. Anti-malware should determine if there are threats by scanning a computer and removing them, if found. Prevention is better than corrective action after infection. Although anti-virus programs should be continually enabled and updated, certain types of threats, like spyware, often make their way into a computer system. At all times, a firewall should be in place for additional security. Multiple, compatible protective sources are encouraged as additional insurance against malware.

7. ANTI-MALWARE

Anti-malware is any resource that protects computers and systems against malware, including viruses, spyware and other harmful programs. Anti-malware resources are comprehensive solutions that maintain computer

security and protect sensitive data that is transmitted by a network or stored on local devices. Anti-malware tools often include multiple components, including anti-spyware and phishing tools, as well as antivirus solutions for prominent viruses, which are isolated and identified by security resources. Anti-malware tools may employ scanning, strategies, freeware or licensed tools to detect rootkits, worms, Trojans and other types of potentially damaging software. Each type of malware resource carries its own interface and system requirements, which impact user solutions for a given device or system.

8. VIRUS

A virus is a type of malicious software (malware) comprised of small pieces of code attached to legitimate programs. When that program runs, the virus runs. Viruses are malicious programs that spread throughout computer files without user knowledge. Most widespread virus infections spread through email message attachments that activate when opened. The vicious cycle of a virus perpetuates as infected emails are forwarded to multiple users. Viruses also spread through shared media, such as Universal Serial Bus (USB) drivers. Initially created as pranks, viruses are responsible for widespread and significant computer system and file destruction. Installing anti-virus software helps prevent, block or remove previously installed viruses.

9. ANTI-VIRUS SOFTWARE

Antivirus software is a type of utility used for scanning and removing viruses from your computer. While many types of antivirus programs exist, their primary purpose is to protect computers from viruses and remove any viruses that are found. Most antivirus programs include both automatic and manual scanning capabilities. The automatic scan may check files that are downloaded from the Internet, discs that are inserted into the computer, and files that are created by software installers. The automatic scan may also scan the entire hard drive on a regular basis. The manual scan option allows you to scan individual files or your entire system whenever you feel it is necessary.

Since new viruses are constantly being created by computer hackers, antivirus programs must keep an updated database of virus types. This database includes a list of «virus definitions» that the antivirus software references when scanning files. Since new viruses are frequently distributed, it is important to keep your software's virus database up-to-

date. Fortunately, most antivirus programs automatically update the virus database on a regular basis.

While antivirus software is primarily designed to protect computers against viruses, many antivirus programs now protect against other types of malware, such as spyware, adware, and rootkits as well. Antivirus software may also be bundled with firewall features, which helps prevent unauthorized access to your computer. Utilities that include both antivirus and firewall capabilities are typically branded «Internet Security» software or something similar.

While antivirus programs are available for Windows, Macintosh, and Unix platforms, most antivirus software is sold for Windows systems. This is because most viruses are targeted towards Windows computers and therefore virus protection is especially important for Windows users. If you are a Windows user, it is smart to have at least one antivirus program installed on your computer. Examples of common antivirus programs include Norton Antivirus, Kaspersky Anti-Virus, and ZoneAlarm Antivirus. Broadly speaking, the two main approaches to virus detection are:

- Dictionary Approach: The anti-virus software checks a file and automatically refers to a dictionary of known viruses. If there is a match, the file is deleted, quarantined or repaired.
- Suspicious Behavior Approach: The anti-virus software monitors the behavior of all programs and flags any suspicious behavior. For example, a program might be flagged if it tries to change settings to the operating system or write to a certain directory.

10. FIREWALL

A firewall is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet.

A firewall may be implemented using hardware, software, or a combination of both. A firewall is recognized as the first line of defense in securing sensitive information. For better safety, the data can be encrypted.

Firewalls generally use two or more of the following methods:

- Packet Filtering: Firewalls filter packets that attempt to enter or leave a network and either accept or reject them depending on the predefined set of filter rules;
- Application Gateway: The application gateway technique employs security methods applied to certain applications such as Telnet and File Transfer Protocol servers;

- Circuit-Level Gateway: A circuit-level gateway applies these methods when a connection such as Transmission Control Protocol is established and packets start to move;
- Proxy Servers: Proxy servers can mask real network addresses and intercept every message that enters or leaves a network;
- Stateful Inspection or Dynamic Packet Filtering: This method compares not just the header information, but also a packet's most important inbound and outbound data parts. These are then compared to a trusted information database for characteristic matches. This determines whether the information is authorized to cross the firewall into the network.

11. ROOTKIT

A rootkit is a software program designed to provide a user with administrator access to a computer without being detected. Rootkits are considered one of the most serious types of malware since they may be used to gain unauthorized access to remote systems and perform malicious operations. The name «rootkit» includes the word «root», because the goal of a rootkit is to gain root access to a computer. By logging in as the root user of a system, a hacker can perform nearly any operation he or she wishes. This includes installing software and deleting files. The word «kit» refers to the software files that make up the rootkit. These may include utilities, scripts, libraries, and other files.

Rootkits often work by exploiting security holes in operating systems and applications. Others create a «back door» login to the operating system, which allows a user to bypass the standard login procedure when accessing a system. Once root access has been enabled, a rootkit may attempt to hide any traces of unauthorized access by modifying drivers or kernel modules, hiding certain files, and quitting active processes. Fortunately, most operating systems and software programs are designed to prevent unauthorized access via rootkits or other malware. Therefore, it is difficult to use a rootkit to gain access to modern systems. However, rootkits are constantly modified and updated in order to try and breach security holes. Therefore, it is wise to install antivirus or other security software on your computer to monitor any attempts of unauthorized access to your system.

12. CRIMEWARE

Crimeware is any computer program designed for the express purpose of conducting malicious and illegal activities online. Although adware, spyware and malware can all be used to conduct illegal activity,

crimeware refers to programs that are meant to automate the theft of information, allowing the thief to gain access to a person's financial accounts online. The term was coined by Peter Cassidy, the Secretary General of the Anti-Phishing Group. Criminals employ a variety of methods to steal information through crimeware, including:

- Crimeware can redirect a user's Web browser to a counterfeit website controlled by the thief;
- Crimeware can enable remote access of applications, allowing criminals to break into networks;
- Crimeware can be used to steal passwords cached on a user's system;
- Crimeware can install keystroke loggers to collect data, such as password and login information for online bank accounts.

13. TROJAN HORSE

A Trojan horse is a seemingly benign program that when activated, causes harm to a computer system. A Trojan horse is also known as a Trojan virus or Trojan. The Trojan horse is named for ancient Greece's apparent gift of peace to the Trojans, when a giant wooden horse was secretly filled with Greek warriors. After the Trojans allowed the horse to enter their great city, the Greek warriors emerged from the horse gained control of the city of Troy. The following are types of Trojan horses:

- Backdoor Trojan: opens a back door for a user to access a victim's system at a later time;
- Downloader: This Trojan downloads malicious software and causes harm to the victim's computer system;
- Infostealer: This Trojan attempts to steal information from the victim's computer;
- Remote Access Trojan (RAT): This can be hidden in games or other programs of a smaller variety and give the attacker control of the victim's computer;
- Data Sending Trojan: This gives the perpetrator sensitive information like passwords or other information programmed to be hijacked;
- Destructive Trojan: This destroys the victim's files;
- Proxy Trojan: As a proxy server, this allows the attacker to hijack a victim's computer and conduct illegal activities from the victim's computer.

14. INTERNET WORM

An Internet worm is type of malicious software (malware) that self-replicates and distributes copies of itself to its network. These independent virtual viruses spread through the Internet, break into computers, and replicate without intervention from and unbeknownst to computer users.

Internet worms can be included in any type of virus, script or program. These worms typically infect systems by exploiting bugs or vulnerabilities that can often be found in legitimate software. Unlike Trojans or other viruses that require user intervention to spread, Internet worms can spread on their own. This makes them extremely dangerous. Internet worms are also known as computer worms.

Internet worms use various techniques to multiply over the Internet. Initial worms just scanned local network hard drives and folders, and then inserted themselves into programs. In the 1990s, Internet worms came in the form of Visual Basic scripts that replicated on computers running on Windows. These worms used the user's email to spread themselves to all the addresses available in the user's address book.

In 2001, Internet worms began to exploit vulnerabilities in the Windows OS to infect machines directly via the Internet. Later, Microsoft released automatic OS updates to prevent this problem. Probably the most powerful Internet worm in terms of its scope was the Code Red Worm, which scanned the Internet and attacked susceptible computers that ran the Windows IIS Web server. Internet worms are embedded in software and penetrate most firewalls and other forms of network security. Anti-virus software applications combat worms along with other forms of malware such as viruses.

15. SPYWARE AND ANTI-SPYWARE

Spyware is infiltration software that secretly monitors unsuspecting users. It can enable a hacker to obtain sensitive information, such as passwords, from the user's computer. Spyware exploits user and application vulnerabilities and is often attached to free online software downloads or to links that are clicked by users. Peer-to-peer (P2P) file sharing has increased the proliferation of spyware and its ramifications. Anti-spyware applications locate and remove spyware and are recommended as a preventative line of defense against infiltration and damage. Anti-virus software removes PC viruses, but anti-virus scans do not always detect spyware. Spyware and cookies are similar, but spyware conducts infiltration activity continuously

until it is removed by specific anti-spyware tools. Users should take the following precautions to prevent spyware attacks:

- Maintain anti-virus and anti-spyware updates and patches;
- Download from well-known and reputable sites only;
- Use a firewall for enhanced security.

Spyware can pose a security risk to the user, but more frequently spyware degrades system performance by taking up processing power, installing additional software, or redirecting users' browser activity

Anti-spyware may also be called apyware on the Internet. Because «a» and «s» sit next to each other on the keyboard, many people accidentally type «apyware» when they try to search «spyware».

Manufacturers and other interested parties capitalize on this by advertising «apyware». Anti-spyware software detects spyware through rules-based methods or based on downloaded definition files that identify common spyware programs. Anti-spyware software can be used to find and remove spyware that has already been installed on the user's computer, or it can act much like an anti-virus program by providing real-time protection and preventing spyware from being downloaded in the first place. Most modern-day security suites bundle anti-spyware functionality alongside anti-virus protection, personal firewalls, etc.

16. BOT

A bot (short for «robot») is an automated program that runs over the Internet. Some bots run automatically, while others only execute commands when they receive specific input. There are many different types of bots, but some common examples include web crawlers, chat room bots, and malicious bots.

Web crawlers are used by search engines to scan websites on a regular basis. These bots «crawl» websites by following the links on each page. The crawler saves the contents of each page in the search index. By using complex algorithms, search engines can display the most relevant pages discovered by web crawlers for specific search queries.

Chat bots were one of the first types of automated programs to be called «bots» and became popular in the 1990s, with the rise of online chatrooms. These bots are scripts that look for certain text patterns submitted by chat room participants and respond with automated actions. For example, a chat bot might warn a user if his or her language is inappropriate. If the user does not heed the warning, the bot might kick the user from the channel and may even block the user from returning. A more advanced type of chat bot, called a «chatterbot» can respond to messages in plain English, appearing to be an

actual person. Both types of chat bots are used for chatroom moderation, which eliminates the need for an individual to monitor individual chatrooms.

While most bots are used for productive purposes, some are considered malware, since they perform undesirable functions. For example, spambots capture email addresses from website contact forms, address books, and email programs, then add them to a spam mailing list. Site scrapers download entire websites, enabling unauthorized duplication of a website's contents. DoS bots send automated requests to websites, making them unresponsive. Botnets, which consist of many bots working together, may be used to gain unauthorized access to computer systems and infect computers with viruses.

17. DOS

A denial of service attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system. Denial of service (DoS) attacks may be initiated from a single machine, but they typically use many computers to carry out an attack. Since most servers have firewalls and other security software installed, it is easy to lock out individual systems. Therefore, distributed denial of service (DDoS) attacks are often used to coordinate multiple systems in a simultaneous attack.

A distributed denial of service attack tells all coordinated systems to send a stream of requests to a specific server at the same time. These requests may be a simple ping or a more complex series of packets. If the server cannot respond to the large number of simultaneous requests, incoming requests will eventually become queued. This backlog of requests may result in a slow response time or a no response at all. When the server is unable to respond to legitimate requests, the denial of service attack has succeeded.

DoS attacks are a common method hackers use to attack websites. Since flooding a server with requests does not require any authentication, even a highly secured server is vulnerable. However, a single system is typically not capable of carrying out a successful DoS attack. Therefore, a hacker may create a botnet to control multiple computers at once. A botnet can be used to carry out a DDoS attack, which is far more effective than an attack from a single computer.

Denial of service attacks can be problematic, especially when they cause large websites to be unavailable during high-traffic times. Fortunately, security software has been developed to detect DoS attacks and limit their effectiveness. While many well-known websites, like Google, Twitter, and WordPress, have all been targets of denial of service attacks in the past, they

have been able to update their security systems and prevent further service interruptions.

18. SNIFFER

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

While sniffers do not cause network damage, they have the potential to cause personal harm because they can allow a hacker to confiscate PINs, passwords and other confidential information, especially data that is in plain text. Sniffer users can even include co-workers who seek to benefit from unauthorized data searches within a work setting. This risk is compounded by the fact that a sniffer program is relatively inexpensive to purchase and easy to use.

There are ethical reasons to use sniffer software, such as when a network administrator monitors network traffic flow. Anti-sniff scans are useful when guarding against sniffer attacks, as are switched networks. However, when one considers how easy it is to obtain and use sniffer software for malicious reasons, its illegitimate use is a cause for concern.

19. PASSWORD CRACKING

Password cracking refers to various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from, a computer system. Password cracking is done by either repeatedly guessing the password, usually through a computer algorithm in which the computer tries numerous combinations until the password is successfully discovered.

Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner's awareness. This results in cybercrime such as stealing passwords for the purpose of accessing banking information. Other,

nonmalicious, reasons for password cracking occur when someone has misplaced or forgotten a password. Another example of nonmalicious password cracking may take place if a system administrator is conducting tests on password strength as a form of security so that hackers cannot easily access protected systems.

The best way that users can protect their passwords from cracking is to ensure they choose strong passwords. Typically, passwords must contain a combination of mixed-case random letters, digits and symbols. Strong passwords should never be actual words. In addition, strong passwords are at least eight characters long. In many password-protected applications, users are notified of the strength of the password they've chosen upon entering it. The user can then modify and strengthen the password based on the indications of its strength.

Other, more stringent, techniques for password security include key stretching algorithms like PBKDF2. Algorithms create hashes of passwords that are designed to protect passwords from being readily cracked. Security tokens constantly shift passwords so that even if a password is cracked, it can be used for a very limited amount of time. The shift to sophisticated technology within computing methods gave rise to software that can crack passwords. Password-cracking computers working in conjunction with each other are usually the most effective form of password cracking, but this method can be very time consuming.

20. BACKUP

Backup refers to the process of making copies of data or data files to use in the event the original data or data files are lost or destroyed. Secondarily, a backup may refer to making copies for historical purposes, such as for longitudinal studies, statistics or for historical records or to meet the requirements of a data retention policy. Many applications, especially in a Windows environment, produce backup files using the .BAK file extension.

Not all backup systems or backup applications are capable of completely restoring a computer system or other complex system configurations such as a database server, computer cluster or active directory servers. Managing the backup process involves organization and is a complicated process. An unstructured backup may simply consist of a stack of floppy disks, CDs or DVDs. However, it is obvious that security and ease of data recovery are both severely compromised.

Full and Incremental Backups: These begin with all data being backed up. Then, only new or modified data or data files are backed up, a much smaller segment of all data. Restoring the entire system to the data

state at a specific point in time would require the last full system backup plus all the incremental backups done up to that point in time.

Differential Backup: This copies all data and data files that have changed since the last full backup. However, there is no archive attribute or record, meaning there is no record of when the backup occurred or how the data was changed.

Full System Backup: This allows the computer system to be restored as it was at a given point in time, including the operating system, all applications and all data. It makes a complete image of the computer, then the user may reconstruct any data changes after that point in time, possibly with an incremental backup.

21. LAW ENFORCEMENT CYBER CENTER

The mission of the Law Enforcement Cyber Center is to serve as a one-stop shop for cyber-related information for local, state and tribal law enforcement. The design and content contained on the site is developed to help law enforcement executives, their agencies, and their partners protect against, respond to, and recover from cyber threats and cyber crime by providing a clearinghouse of cyber-related information. The information on the website portal is vetted, relevant, and easily accessible to help users understand the cyber environment, identify emerging trends, leverage promising practices, facilitate training and technical assistance, encourage collaboration, and provide innovative solutions to address the cyber needs of your community.

The Cyber Center is a collaborative project of the International Association of Chiefs of Police (IACP), Research and Development Corporation (RAND), and the Police Executive Research Forum (PERF), and is made possible by funding from the Bureau of Justice Assistance, at the U.S. Department of Justice’s Office of Justice Programs.

The Cyber Center was developed to enhance the awareness, expand the education, and build the capacity of justice and public safety agencies to prevent, investigate, prosecute, and respond to cyber threats and cyber crimes. It is intended to be a national resource for law enforcement and related justice and public safety entities. The Cyber Center addresses three principal functional areas: Cyber crime investigations, Digital forensics, Information systems security.

It provides the information pertaining to cyber security, investigations, digital forensics, and legal considerations, but is intended to provide interested readers with links to further information. It will be helpful to police chiefs and executives, patrol officers, digital forensic investigators, and detectives investigating crimes that involve electronic devices. Further, while large law

enforcement agencies may already be well equipped to handle large volumes of sophisticated cyber crimes, most law enforcement agencies are less well equipped and this website will be of particular value to them.

22. PROTECTING LAW ENFORCEMENT INFORMATION

Today's records management systems, including those used by law enforcement, are nearly all computer-based digital files. The Next Generation 911 Systems are Internet Protocol based and allow for text messaging and the sharing of photographs and video from citizens to call centers. Computer-aided dispatch systems are also a type of digital technology. In this ever-changing world, securing law enforcement information requires much more than just physical security. Police executives must begin to take cybersecurity very seriously and recognize the potential threat to public safety service delivery.

By now most police executives have heard the stories of agencies being targeted by computer hackers. In some cases, sensitive information about law enforcement operations, officers' personal information, and even detailed information on officers' families have been stolen from the police agencies' digital files and then released to the public. As serious as these incidents are, just imagine if an agency's computer systems were hacked and individual criminal records were edited, added, or deleted. The agency's ability to depend upon their computer records being accurate for the purposes of developing reasonable suspicion or probable cause would become nonexistent.

Today many chiefs believe the threat of a cyber attack is quite serious; however, just as many admit that current policies, practices, and technology are not sufficient to minimize their agencies' risk. Historically, the greatest threat to an agency's computerized systems were disgruntled employees; however, in today's cyberworld, one controversial arrest or incident can bring the attention of local, national, and international hackers to the jurisdiction with the shared mission to breech confidential files and exploit them as a form of punishment. Police executives are encouraged to educate themselves as to how secure their departments are from cyber attacks.

23. SEPARATING THE DATA AND SEGMENTING THE NETWORK

An agency must first determine the types of data that are stored on computers throughout the network before deciding the most appropriate way to protect them. Understanding which kinds of data exist where on the network will also help the agency determine which employees should have access to the systems.

To separate data and segment a network, an agency should:

- Catalogue the types of information (employee records, crime information, email accounts, etc.);
- Differentiate the information according to sensitivity. One way to think about this is to ask, “What are the harmful consequences that would occur if this information were lost, corrupted, stolen, or destroyed?”;
- Once identified, the data and all related applications should be segmented into separate network environments, which are then protected with appropriate network and user access restrictions, including data encryption, if necessary. While segmenting networks can be tricky, to be truly secure, segments should be separated by internal firewalls. Firewall rules and access controls will determine what information passes between segments and how staff move from one segment to another.

Whenever possible, rely on security and network professionals to design and implement network segments.

24. EDUCATING USERS AND PROTECTING THE HOST

Proper security does not stop at the network. Every computer connected to the network, whether a web, email or database server, or employee laptop or desktop, should also be configured to minimize the number of applications installed. Oftentimes it is seldom-used applications that serve as conduits into an organization’s network, so they need to be updated and patched routinely.

In addition to uninstalling or disabling unnecessary applications, employee workstations and laptops should also be equipped with anti-virus software. This will reduce the number of opportunities attackers have to use malicious software to steal information or corrupt data. This software is available from many reputable security agencies.

But of course, humans can also be used to attack networks. Many data security incidents are caused by tricking employees into opening or executing corrupted email attachments. It is therefore critical for law enforcement executives and managers to communicate the harms that can occur by opening email attachments. Anti-virus software can detect and prevent harmful outcomes in many cases, but they are not fool-proof. Effective information security awareness training that discusses threats and safe computing practices is essential.

Similarly, phishing scams (fake emails soliciting confidential information from the user) are a common and sometimes successful method used by fraudsters and cyber hackers. An employee clicking on a spear phishing email message will render useless the best perimeter defenses, and it is unrealistic to expect that no one will click on a phishing message. Therefore, your

information security strategy must be able to account for the fact that some phishing attacks will be successful. For example, there will be intrusions into your network. Email hosting providers can help reduce the amount of spam and phishing email received by a department, but as with anti-virus software, are not fool-proof. Employees of all ranks must be diligent and never respond over email with one's personal information (such as username, password, or social security or credit card number). Only an effective monitoring capability that can detect and respond to malware introduced through phishing provides the degree of protection most organizations require.

It is critical to backup any important information. The easiest way to accomplish this task is to copy all relevant data to an external hard drive, network file server, or dedicated backup server. These drives are easy to use and serve as a way to restore information if it becomes lost, corrupted, or stolen. In traditional organizations, the protocols for backing up data are part of a disaster recovery or business continuity plan. Of course, any backups created should be appropriately secured against unauthorized access.

Precautions also must be taken when employees work remotely. Employees who access agency servers from a remote location may be doing so from an unsecure network. Additional security measures, such as two factor authentication and encryption, should be used to provide added security. Departments may also want to consider only granting remote access to specific users (for example, command staff) and/or to specific computers or networks.

COMPREHENSION CHECK

1. Match the words to their description:

1) vulnerability	**A)** a component of risk management
2) backup	**B)** a flaw in a system that can leave it open to attack
3) risk analysis	**C)** any software that brings harm to a computer system
4) denial of service attack	**D)** malicious program that spread throughout computer files without user knowledge
5) malware	**E)** infiltration software that secretly monitors unsuspecting users
6) spyware	**F)** an effort to make one or more computer systems unavailable
7) virus	**J)** the process of making copies of data or data files

2. How is data loss usually prevented?
3. How are security breaches typically monitored, identified and mitigated?
4. What key steps does the risk management process involve?
5. Why must antivirus programs keep an updated database of virus types?
6. What types of Trojan horses do you know?
7. Give an example of nonmalicious reasons for password cracking.
8. Name two main approaches to virus detection.
9. What do anti-spyware applications do?
10. What should users do to prevent spyware attacks?

DISCUSSION

Discuss the following statements:

A. It is important to keep your software's virus database up-to-date.

B. Criminals employ a variety of methods to steal information through crimeware.

C. Anti-spyware applications are recommended as a preventative line of defense against infiltration and damage.

D. Distributed denial of service (DDoS) attacks are often used to coordinate multiple systems in a simultaneous attack.

E. Law Enforcement Cyber Center is intended to be a national resource for law enforcement and related justice and public safety entities.

UNIT 5
CYBERCRIME AND CYBERCRIMINALS

1. CRIMES IN CYBERSPACE

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

2. CYBERWARFARE

Cyberwarfare is any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems. Waged via the Internet, these attacks disable financial and organizational systems by stealing or altering classified data to undermine networks, websites and

services. Cyberwarfare is also known as cyber warfare or cyber war. Cyberwarfare involves the following attack methods:

- Sabotage: Military and financial computer systems are at risk for the disruption of normal operations and equipment, such as communications, fuel, power and transportation infrastructures.
- Espionage and/or security breaches: These illegal exploitation methods are used to disable networks, software, computers or the Internet to steal or acquire classified information from rival institutions or individuals for military, political or financial gain.

On the flip side, systems procedures are continuously developed and tested to defend against cyberwarfare attacks. For example, organizations will internally attack its system to identify vulnerabilities for proper removal and defense. A common perception of a hacker is that of a teenage geek who fools breaks into computer systems for fun. While this perception was perhaps once true, modern cyberwarfare involves well trained, well funded professionals backed by nation states. Much more is happening behind the scenes, and the front lines in future wars will be digital.

3. CYBERSECURITY

Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management. A cybersecurity plan is critical to highly sensitive company information, such as U.S. Department of Defense or associated federal agency data.

User cybersecurity may be employed in the following ways:

- Continuous antivirus software updates;
- Strong passwords;
- Never disclosing personal information.

Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment. Every time we connect to the Internet — at home, at school, at work, or on our mobile devices — we make decisions that affect our cybersecurity. Emerging cyber threats require engagement from the entire community to create a safer cyber environment — from government and law enforcement to the private sector and, most importantly, members of the public.

Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals. The field of cyber

crime has rapidly developed and evolved, leaving some unsure of what it encompasses and the meaning of some common terms that relate to cyber crime. One definition is at crime where a computer is either the target or the tool used to commit a crime.

The term cyber crime is frequently used to cover a wide range of criminal activity and sometimes creates confusion. The term cyber can encompass identity theft and fraudulent schemes; cyber bullying and stalking; computer hacking; system intrusions; denial of services; and even espionage and terrorism.

Because the term is so broad, experts have suggested using the term cyber with appropriate modifiers to differentiate the type of crime or intrusion and the required law enforcement response or action, such as cyber investigation and forensics, cyber infrastructure protection, cyber intrusion, and so forth.

The use and consistent application of relevant terms would help everyone better understand the various dimensions of the cyber crime challenge and help us speak a common language in coordinating our activities. As we enhance our national capability to respond to the cyber challenge, speaking a common language is only one challenge; building expertise and capacity through training and technical assistance and coordinating our nation's resources and law enforcement response is another.

4. COMBATING CYBER CRIME

Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyberattacks such as corporate security breaches, spear phishing, and social media fraud. Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our nation's cybersecurity objectives by investigating a wide range of cyber crimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. The Department of Homeland Security (DHS) works with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools. Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents.

5. INTERNET CRIME

Internet crime is any crime or illegal online activity committed on the Internet, through the Internet or using the Internet. The widespread Internet crime phenomenon encompasses multiple global levels of legislation and oversight. In the demanding and continuously changing IT field, security experts are committed to combating Internet crime through preventative technologies, such as intrusion detection networks and packet sniffers. Internet crime is a strong branch of cybercrime. Identity theft, Internet scams and cyberstalking are the primary types of Internet crime. Because Internet crimes usually engage people from various geographic areas, finding and penalizing guilty participants is complicated. Internet crimes are a constant threat to Internet users.

Types of Internet crime include:

- Cyberbullying and harassment;
- Financial extortion;
- Internet bomb threats;
- Classified global security data theft;
- Password trafficking;
- Enterprise trade secret theft;
- Personally data hacking;
- Copyright violations, such as software piracy;
- Counterfeit trademarks;
- Illegal weapon trafficking;
- Online child pornography;
- Credit card theft and fraud;
- Email phishing;
- Domain name hijacking;
- Virus spreading.

To prevent becoming an Internet crime, online vigilance and common sense are critical. Under no circumstances should a user share personal information (like full name, address, birth date) to unknown recipients. Moreover, while online, a user should remain suspicious about exaggerated or unverifiable claims.

6. CYBERCRIMINAL

A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both. Cybercriminals use computers in three broad ways:

- Select computer as their target: These criminals attack other people's computers to perform malicious activities, such as spreading viruses, data theft, identity theft, etc.;
- Uses computer as their weapon: They use the computer to carry out «conventional crime», such as spam, fraud, illegal gambling, etc.;
- Uses computer as their accessory: They use the computer to save stolen or illegal data.

Cybercriminals often work in organized groups. Some cybercriminal roles are:

- Programmers: Write code or programs used by cybercriminal organization;
- Distributors: Distribute and sell stolen data and goods from associated cybercriminals;
- IT experts: Maintain a cybercriminal organization's IT infrastructure, such as servers, encryption technologies and databases;
- Hackers: Exploit systems, applications and network vulnerabilities;
- Fraudsters: Create and deploy schemes like spam and phishing;
- System hosts and providers: Host sites and servers that possess illegal contents;
- Cashiers: Provide account names to cybercriminals;
- Money mules: Manage bank account wire transfers;
- Tellers: Transfer and launder illegal money via digital and foreign exchange methods;
- Leaders: Often connected to big bosses of large criminal organizations. They assemble and direct cybercriminal teams, and usually lack technical knowledge.

Clearly, there is much overlap between roles, but as cybercrime becomes a greater issue, more and more specialization is being seen. For example, hackers were once more often than not hobbyists who broke into systems for personal gratification. While white-hat hacking has not disappeared, it is much more common now to see hackers as professionals who sell their services to the highest bidder.

7. CYBERATTACK

A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Cyberattack is also known as a computer network attack (CNA).

Cyberattacks may include the following consequences:

- Identity theft, fraud, extortion;
- Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses;
- Stolen hardware, such as laptops or mobile devices;
- Denial-of-service and distributed denial-of-service attacks;
- Breach of access;
- Password sniffing;
- System infiltration;
- Website defacement;
- Private and public Web browser exploits;
- Instant messaging abuse;
- Intellectual property (IP) theft or unauthorized access.

Security Technology Services all over the world research and investigate cyberattack issues facing law enforcement investigations and focus on the continuous development of IP tracing, data analysis, real-time interception and data sharing.

8. CYBERTERRORISM

Cyberterrorism is threat, harm or extortion via the Internet. With the increasing prevalence and power of computers, terrorism has gone beyond physical attacks to include computer-based, or "cyber" terrorism. Through well-planned computer attacks, cyberterrorists may target key services that are computer-controlled, such as water and electricity.

One U.S. definition describes cyberterrorism as "the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (Cybercrimes: Infrastructure Threats from Cyberterrorists, Cyberspace Lawyer, 4 NO. 2 Cyberspace Law. 23). Many government Web sites are likely targets for a cyberterrorism attack because an attacker could use the Web site to access confidential information on national security and individual citizens.

Cyberterrorists also attack personal or corporate Web sites and demand ransom in return for stopping the attack and any resulting damage. For example, a user who gains administrative access to a Web site through social engineering or other means could later threaten the owner of the Web site with publishing the owner's account information on the Internet if the owner does not pay the ransom.

9. CYBERSTALKING

Cyberstalking is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging clients and any other online medium. Cyberstalking can also occur in conjunction with the more traditional form of stalking, where the offender harasses the victim offline. There is no unified legal approach to cyberstalking, but many governments have moved toward making these practices punishable by law. Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking.

Cyberstalking is one of several cybercrimes that have been enabled by the Internet. It overlaps with cyberbullying and cyberluring in that many of the same techniques are used. Social media, blogs, photo sharing sites and many other commonly used online sharing activities provide cyberstalkers with a wealth of information that helps them plan their harassment. By collecting personal data (profile pages) and making notes of frequented locations (photo tags, blog posts), the cyberstalker can begin to keeping tabs on an individual’s daily life.

The National Center for Victims of Crime (NCVC) suggests that victims of cyberstalking take the following steps:

- For minors, inform parents or a trusted adult;
- File a complaint with the cyberstalker's Internet service provider;
- Collect evidence, document instances and create a log of attempts to stop the harassment;
- Present documentation to local law enforcement and explore legal avenues;
- Get a new email address and increase privacy settings on public sites;
- Purchase privacy protection software;
- Request removal from online directories;

The NCVC also emphasizes that a victim of cyberstalking should never agree to meet the stalker in person.

10. CYBERBULLYING

Cyberbullying is a practice where an individual or group uses the Internet to ridicule, harass or harm another person. The social and emotional harm inflicted by cyberbullies grows out of — or leads to — physical bullying in the offline world. Cyberbullying is a prosecutable offense in some jurisdictions, but a globally uniform legal approach has not yet been established.

Cyberbullies use social media and smartphones to harass victims from remote or local areas. Traditional bullying usually stops when a victim returns to the safety of his home, but cyberbullying is a continuous process maintained through email, texting, forum/blog posts and other communication vehicles. Even if cyberbullying victims change profile settings and avoid certain websites, cyberbullies may easily continue public bullying activities. The National Crime Prevention Council (NCPC) offers the following recommendations for victims of cyberbullying:

- Block cyberbullies on all social media sites;
- Report cyberbullies to website administrators;
- Avoid sharing personal details online;
- If you are a minor, speak to a trusted adult about cyberbullying.

The NCPC also encourages those who are not victims to become anti-bullying advocates by refusing to participate in cyberbullying campaigns, flagging cyberbullies and raising cyberbullying awareness.

11. CYBERLURING

Cyberluring refers to the practice of using false pretexts to deceive another individual into meeting in person with the intent of perpetrating a crime. Cyberlurers use chatrooms, instant messaging applications or email to establish online rapports with their targets. Once they've gained the trust of the target, they arrange to meet in the real world. Upon meeting, the target may be sexually assaulted, robbed or even murdered. Cyberluring is also known as Internet luring. Cyberluring is an insidious practice in that the majority of cases involve adult lurers targeting underage children. These cases frequently end in sexual assault. The problem is serious enough that the FBI has released guidelines on protecting children from cyberlurers. These include steps such as:

- Keeping the computer in a common room;
- Maintaining access to your child's email and accounts;
- Using parental control software to block certain sites.

Many groups, schools and local police departments present programs whose goal is to educate parents and youth about the dangers of cyberluring and about how perpetrators go about luring innocent Internet users into their grip.

12. CYBERSPYING

Cyberspying is a form of cybercrime in which hackers target computer networks in order to gain access to classified or other information that may be profitable or advantageous for the hacker. Cyberspying is an ongoing process

that occurs over time in order to gain confidential information. It can result in everything from economic disaster to terrorism. The potentially harmful outcomes of cyberspying not only cause government security breaches but can also lead to the declassification of company secrets. This can be disastrous for companies if the attackers use stolen information to manufacture copy-cat products and gain market share.

Cyberspying can be conducted by an individual, a group or groups. During the process, specific computers that contain exact information the hacker wants to obtain are targeted. Cyber spies can lurk in networks for weeks, months or years — however long it takes them to obtain the intellectual property they are seeking, or be caught. Cyberspying often targets government agencies in order to infiltrate top-secret military or security information.

13. PHISHING

Phishing is the fraudulent act of acquiring private and sensitive information, such as credit card numbers, personal identification and account usernames and passwords. Using a complex set of social engineering techniques and computer programming expertise, phishing websites lure email recipients and Web users into believing that a spoofed website is legitimate and genuine. In actuality, the phishing victim later discovers his personal identity and other vital information have been stolen and exposed.

Similar to fishing in a lake or river, phishing is computer lingo for fishing over the Internet for personal information. The term was first used in 1996, when the first phishing act was recorded. Phishing uses link manipulation, image filter evasion and website forgery to fool Web users into thinking that a spoofed website is genuine and legitimate. Once the user enters vital information, he immediately becomes a phishing victim. Fortunately, phishing victimization is preventable. The following security precautions are recommended:

- Use updated computer security tools, such as anti-virus software, spyware and firewall;
- Never open unknown or suspicious email attachments;
- Never divulge personal information requested by email, such as your name or credit card number;
- Double check the website URL for legitimacy by typing the actual address in your Web browser;
- Verify the website's phone number before placing any calls to the phone number provided via email.

14. PHREAKING

Phreaking is a slang term that describes the action of experimenting with or manipulating a telephone system. Since phreaking took place before personal computers became popular, it is sometimes considered to be the precursor to computer hacking.

While not all phreaking activities are illegal, the term is often associated with using a phone system to make free long distance calls. Early phone systems has limited security features, which allowed «phreaks» to tap into analog phone lines and make calls free of charge. This was often done using a device called a «blue box», which simulated a telephone operator's console. Phreaks could use these devices to route their own calls and bypass the telephone company switches, allowing them to make free calls. This activity was more prominent before the turn of the century, when cell phone companies began including free long distance service.

Phreaking has evolved over past several decades along with telecommunications technology. In the 1980s and 1990s, phreaks began using modems to access to computer systems over telephone lines. Once connected via modem, tech-savvy users could access private data or exploit computers connected on the local network. This activity also faded out around the turn of the century as dial-up modems were replaced by DSL and cable modems and new security measures were put into place. While phreaking still exists, it is much less common than other types of computer hacking.

15. SMISHING

Smishing is a combination of the terms «SMS» and «phishing.» It is similar to phishing, but refers to fraudulent messages sent over SMS (text messaging) rather than email. The goal of smishing is to capture people's personal information. In order to do this, «smishers» send out mass text messages designed to capture the recipients' attention. Some messages may be threatening, e.g., «Visit this URL to avoid being charged $5.00 per day», while others may provide a fake incentive, such as «You have won a free gift card, visit this website to claim your prize». If you click on a link in the text message, you will be directed to a fraudulent website that will ask you to enter your personal information, such as your name, address, phone number, and email address. In some cases, a smishing website will ask you to enter your bank account information or social security number.

Smishing has become increasingly common now that smartphones are widely used. Many smartphones allow you to simply click on a link in a text message to view the website in your phone's browser. This makes text

messages an effective «bait» for luring unsuspecting users to fraudulent websites. Therefore, just like when you receive email spam, is best to not visit websites mentioned in text messages from unknown sources.

16. VISHING

Using fake phone numbers to trick you into giving away personal information. Vishing is short for voice phishing. It is similar to phishing in that the objective is to obtain personal information fraudulently, but in vishing attacks, the user is tricked into making a phone call, rather than visiting a Web site. In an instance of vishing, a victim receives a phone call or an email saying that his credit card account has been breached and he needs to call a particular number to correct the problem. The victim then dials the number to fix the account, without realizing that the number is spurious. The number dialed is actually a Voice over IP (VoIP) phone. The victim then enters his credit card number through keystrokes that the VoIP phone can recognize and record.

Although people are becoming increasingly aware of phishing, vishing attacks are not well known. VoIP phone subscribers can get an area code and prefix of their choice, making it possible to have area codes and prefixes of valid banks. Such numbers make it easier for attackers to lure people into leaking their confidential data.

17. SOCIAL ENGINEERING

Social engineering is a technique used by hackers and non-hackers to get access to confidential information. With social engineering, attackers use manipulation and deceit to trick victims into giving out confidential information.

Some of the social engineering methods attackers use include:

- Sending messages that contain dangerous attachments (e.g., malware) with text that encourages people to open the attachments;
- Pretending to be the main administrator of a local network and asking for the victim’s password in order to perform a maintenance check;
- Telling a victim over the phone that he/she has won a prize, and asking for a credit card number in order to deliver it;
- Asking for a user’s password for a certain Internet service, such as a blog, and using the same password later to access the user’s computer. This technique works because users often use the same passwords for many different services.

18. SPOOFING

The word «spoof» means to hoax, trick, or deceive. Therefore, in the IT world, spoofing refers to tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

Spoofing can take place on the Internet in several different ways. One common method is through email. Email spoofing involves sending messages from a bogus email address or faking the email address of another user. Fortunately, most email servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP, which allows them to use fake email addresses. Therefore, it is possible to receive email from an address that is not the actual address of the person sending the message.

Another way spoofing takes place on the Internet is via IP spoofing. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions.

Finally, spoofing can be done by simply faking an identity, such as an online username. For example, when posting on any Web discussion board, a user may pretend he is the representative for a certain company, when he actually has no association with the organization. In online chat rooms, users may fake their age, gender, and location.

While the Internet is a great place to communicate with others, it can also be an easy place to fake an identity. Therefore, always make sure you know who you are communicating with before giving out private information.

19. IDENTITY THEFT

Identity theft is the unauthorized collection of personal information and its subsequent use for criminal reasons such as to open credit cards and bank accounts, redirect mail, set up cellphone service, rent vehicles and even get a job. These actions can mean severe consequences for the victim, who will be left with bills, charges and a damaged credit score.

There are many ways in which an individual's identity can be stolen, but people may be particularly vulnerable to this crime online, where

savvy criminals can gain access to personal information through a number of avenues. This theft is increasingly being perpetrated electronically.

Identity thieves have a number of avenues for stealing personal information via electronic means. These include:

- Retrieving stored data from discarded electronic equipment such as PCs, cellphones and USB memory sticks;
- Stealing personal information using malware such as keystroke logging or spyware;
- Hacking computer systems and databases to gain unauthorized access to large amounts of personal data;
- Phishing, or impersonating trusted organizations (such as a bank or large retailer) via email or SMS messages and prompting users to enter personal financial information;
- Compromising weak login passwords (often through calculated guesswork) to gain access to a user's online accounts;
- Using social networking sites to attain enough personal details to guess email passwords or impersonate the victim in other ways online;
- Diverting victims' emails to attain personal information such as bank and credit card statements, or to prevent the victim from discovering that new accounts have been opened in his or her name.

There are some steps consumers can take to protect their identities, including ensuring that any transactions they make online use secure data encryption, limiting the amount of personal information they share online, remaining alert to phishing scams and keeping a close eye on their banking and credit card statements.

20. DATA THEFT

Data theft is the illegal transfer or storage of any information that is confidential, personal, or financial in nature, including passwords, software code, or algorithms, proprietary process-oriented information, or technologies. Considered a serious security and privacy breach, the consequences of data theft can be severe for individuals and businesses.

Common modes of data theft are as follows:

- USB drive — The information can be moved to a thumb drive or USB drive. It is considered as the easiest method of data theft as the storage capacity of USB devices are increasing over time with the cost decreasing;
- Portable hard drive — Large information can be transferred using portable hard drive;

- Devices using memory cards, PDAs — Pod slurping is possible with devices using memory cards and PDAs;
- Email — Another popular way of transmitting information is through emails;
- Printing — Another method used in data theft is by printing information and illegally storing or distributing the same;
- Remote sharing — Using remote access, data can be transferred to another location from where the data can be distributed;
- Malware attack — Malware attacks are potentially capable of extracting sensitive information;

How data theft can be prevented:

- Encryption of confidential information or personal information;
- Data management system to have necessary security measures to ensure the corporate files are not moved or accessed illegally;
- Periodic reviews on devices and systems which can pose high risk;
- Usage of restricted network in organization;
- Restricted usage of devices capable of data storage;
- Laptop lockdown and biometric security measures;
- Protecting confidential and personal information using password;
- Use of anti-malware software.

21. HACKING

Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose. Hackers employ a variety of techniques for hacking, including:

- Vulnerability scanner: checks computers on networks for known weaknesses;
- Password cracking: the process of recovering passwords from data stored or transmitted by computer systems;
- Packet sniffer: applications that capture data packets in order to view data and passwords in transit over networks;
- Spoofing attack: involves websites which falsify data by mimicing legitimate sites, and they are therefore treated as trusted sites by users or other programs;
- Root kit: represents a set of programs which work to subvert control of an operating system from legitimate operators;

- Trojan horse: serves as a back door in a computer system to allow an intruder to gain access to the system later;
- Viruses: self-replicating programs that spread by inserting copies of the same program into other executable code files or documents;
- Key loggers: tools designed to record every keystroke on the affected machine for later retrieval.

Certain corporations employ hackers as part of their support staff. These legitimate hackers use their skills to find flaws in the company security system, thus preventing identity theft and other computer-related crimes.

22. BLACK HAT HACKER

A black hat hacker is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons. This differs from white hat hackers, which are security specialists employed to use hacking methods to find security flaws that black hat hackers may exploit.

Black hat hackers can inflict major damage on both individual computer users and large organizations by stealing personal financial information, compromising the security of major systems, or shutting down or altering the function of websites and networks. The term «black hat hacker» is derived from old Western movies, in which the good guys wore white hats and the bad guys wore black hats.

Black hat hackers can range from teenage amateurs who spread computer viruses to networks of criminals who steal credit card numbers and other financial information. Black hat hacker activities include planting keystroke-monitoring programs to steal data and launching attacks to disable access to websites. Malicious hackers sometimes employ non-computer methods to obtain data, for example, calling and assuming an identity in order to get a user's password. Black hat hackers have their own conventions, of which two of the more prominent are DEFCON and BlackHat. Black hat conventions are often attended by security professionals and academics who want to learn from black hat hackers. Law enforcement officials also attend these conventions, sometimes even making use of them to apprehend a black hat hacker, as occurred in 2001 when a Russian programmer was arrested the day after DEFCON for writing software that decrypted an Adobe e-book format.

23. WHITE HAT HACKER

A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them.

White hat hackers are usually seen as hackers who use their skills to benefit society. They may be reformed black hat hackers or they may simply be well-versed in the methods and techniques used by hackers. An organization can hire these consultants to do tests and implement best practices that make them less vulnerable to malicious hacking attempts in the future. For the most part, the term is synonymous with «ethical hacker». The term comes from old Western movies where the cliché was for the «good guy» to wear a white cowboy hat. Of course, the «bad guys» always seemed to wear a black hat.

24. GRAY HAT HACKER

A gray hat hacker (also spelled grey hat hacker) is someone who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers. Gray hat hackers may engage in practices that seem less than completely above board, but are often operating for the common good. Gray hat hackers represent the middle ground between white hat hackers, who operate on behalf of those maintaining secure systems, and black hat hackers who act maliciously to exploit vulnerabilities in systems.

25. PHARMING

Pharming refers to redirecting website traffic through hacking, whereby the hacker implements tools that redirect a search to a fake website. Pharming may cause users to find themselves on an illegitimate website without realizing they have been redirected to an impostor site, which may look exactly like the real site.

Pharming occurs when hackers locate vulnerabilities in domain name server (DNS) software. Pharming can also occur by rearranging the host’s file on the targeted computer. Online banking websites as well as e-commerce organizations have become popular pharming targets. Desktops are also vulnerable to pharming threats due to their lack of security administration. Pharming and phishing threats have been used simultaneously and these can cause the most potential for online identity theft. Unfortunately, antivirus and

anti-spyware software are often incapable of protecting against this type of cybercrime.

Routers have been surfacing as being just as vulnerable to pharming as hosts files. Unfortunately, router pharming is much more difficult to detect. Harmful DNS information can land on routers in two ways:

- Existing administrator settings can be incorrectly configured;
- Entire rewrites of embedded software (also known as firmware) can occur.

Routers give administrators the option to choose a trusted DNS as opposed to a suggested one. If the administrator isn't well-versed in computers, he or she should avoid a custom DNS, because hackers are more able to choose a DNS under the administrator's control compared to a legitimate one.

Pharming is certainly nothing new, but it is being used more often and is causing increasing harm in the computing world. Computer experts point the finger of blame at domain registrars for security loopholes and a general lack of standards for keeping domains exclusive. Suggestions for mitigating these problems include asking registrars for their written policies as well as insisting on immediate notification should a registrar receive a domain move request. Other suggestions include keeping domains locked and keeping authoritative contact information current, as well as using registrars with round-the-clock availability. If none of these suggestions works in preventing pharming, contacting VeriSign, which is the domain registry for .com and .net, may be useful.

26. KEYSTROKE LOGGER

A keystroke logger is a device or program that allows the user to monitor what another user types into a device. In some cases, a keystroke logger is hardware that attaches to the keyboard or another part of a hardware system. In other cases, it is a program that is considered a type of spyware that can be slipped into a system and used in various ways, many of which are illegal. A keystroke logger may also be called a keylogger.

In terms of the makeup of a keystroke logger spyware program, its most basic elements often include a dynamic link library (DLL), and an executable that runs the file. As the keystroke logger represents a somewhat common type of spyware or malware, there is a focus on how to identify, isolate and disarm these types of monitoring programs. Some users rely on utilities like tcpview to catch keystroke loggers, while others purchase anti-malware and anti-spyware programs that specialize in identifying these threats.

27. CYBERSQUATTING

Cybersquatting refers to illegal domain name registration or use. Cybersquatting can have a few different variations, but its primary purpose is to steal or misspell a domain name in order to profit from an increase in website visits, which otherwise would not be possible. Trademark or copyright holders may neglect to reregister their domain names, and by forgetting this important update, cybersquatters can easily steal domain names. Cybersquatting also includes advertisers who mimic domain names that are similar to popular, highly trafficked websites. Cybersquatting is one of several types of cybercrimes. Cybersquatting is also known as domain squatting.

The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization charged with overseeing domain name registration. As cybersquatting complaints throttle up worldwide, ICANN has implemented thorough standards of acceptance such that domain name assigning is done with much more scrutiny. ICANN has also put solid requirements for domain name recovery in place for instances of trademark registration lapses by trademark owners. ICANN urges trademark owners to renew their registrations yearly and to report misuse to the agency as soon they become aware that they've neglected to reregister a domain.

COMPREHENSION CHECK

1. Match the words to their description:

1) phishing	**A)** is deliberate exploitation of computer systems, technology-dependent enterprises and networks
2) cyberattack	**B)** threat, harm or extortion via the Internet
3) smishing	**C)** the fraudulent act of acquiring private and sensitive information
4) vishing	**D)** fraudulent messages sent over SMS (text messaging) rather than email
5) identity theft	**E)** using fake phone numbers to trick you into giving away personal information
6) cyberterrorism	**F)** tricking or deceiving computer systems or other computer users
7) spoofing	**J)** unauthorized collection of personal information and its subsequent use for criminal reasons

2. Why is cyberspace particularly difficult to secure?
3. How may user cybersecurity be employed?
4. Name the types of Internet crime you know.
5. Why is finding and penalizing cybercriminals a complicated task?
6. What social engineering methods do attackers use to get access to confidential information?
7. Name the possible consequences of cyberattacks.
8. What are the steps consumers can take to protect their identities?
9. What are the most common modes of data theft?
10. How can data theft be prevented?

DISCUSSION

Discuss the following statements:

A. Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment.

B. Spoofing can take place on the Internet in several different ways.

C. Always make sure you know who you are communicating with before giving out private information.

D. Identity thieves have a number of avenues for stealing personal information via electronic means.

E. Gray hat hackers represent the middle ground between white hat hackers and black hat hackers.

UNIT 6
COMPUTER AND INTERNET SECURITY

1. CYBERSPACE

Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

Cyberspace allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities. The term cyberspace was initially introduced by William Gibson in his 1984 book, “Neuromancer”. Gibson criticized the term in later years, calling it “evocative and essentially meaningless.” Nevertheless, the term is still widely used to describe any facility or feature that is linked to the Internet.

According to many IT specialists and experts, including F. Randall Farmer and Chip Morningstar, cyberspace has gained popularity as a medium for social interaction, rather than its technical execution and implementation.

2. INTERNET

The Internet is a globally connected network system that uses TCP/IP to transmit data via various types of media. The Internet is a network of global exchanges — including private, public, business, academic and government networks — connected by guided, wireless and fiber-optic technologies. The terms Internet and World Wide Web are often used interchangeably, but they are not exactly the same thing; the Internet refers to the global communication system, including hardware and infrastructure, while the Web is one of the services communicated over the Internet. Communication systems were first developed for radio communication. However, as computing advanced, peer-to-peer (P2P) communication was gradually delivered and enhanced. During the last two decades, the Internet has influenced and upgraded networking to global standards. Billions of Internet users rely on multiple application and networking technologies, including:

Internet Protocol (IP): The Internet’s primary component and communications backbone. Because the Internet is comprised of hardware and software layers, the IP communication standard is used to address

schemes and identify unique connected devices. Prominent IP versions used for communications include Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

Communications: The Internet is the most cost-effective communications method in a world that is now a global village, in which the following services are instantly available: Email/Web email; Web-enabled audio/video conferencing services; Online movies and gaming; Data transfer/file-sharing, often through File Transfer Protocol (FTP); Instant messaging; Internet forums; Social networking; Online shopping; Financial services.

The Internet is believed to have originated with the U.S. government, which began building a computer network in the 1960s known as ARPANET. In 1985, the U.S. National Science Foundation (NSF) commissioned the development of a university network backbone called NSFNET. The system was replaced by new networks operated by commercial Internet service providers in 1995. The Internet was brought to the public on a larger scale at around this time. By 2011, 30 percent of the world's population was using the Internet.

3. INTERNET SECURITY

Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol. Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks or devices to monitor Internet traffic for dangerous attachments.

Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency’s servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

4. INTERNET PRIVACY

Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data,

communications, and preferences. Internet privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development. Internet privacy is also known as online privacy. Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.

Internet privacy risks include:

- Phishing: An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number;
- Pharming: An Internet hacking activity used to redirect a legitimate website visitor to a different IP address;
- Spyware: An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source;
- Malware: An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Internet privacy violation risks may be minimized, as follows:

- Always use preventative software applications, such as anti-virus, anti-malware, anti-spam and firewalls;
- Avoid shopping on unreliable websites;
- Avoid exposing personal data on websites with lower security levels;
- Clear the browser's cache and browsing history on a consistent basis;
- Always use very strong passwords consisting of letters, numerals and special characters.

5. SECURITY AND PRIVACY

Security and privacy are closely linked, and both are part of the emerging debate on new technologies. However, security and privacy are two different sides of how the use of data and modern devices affects us.

Security is an overarching principle in IT. As more new technologies become connected by networks such as global IP and wireless telecom networks, there is more attention paid to how to control data and how to make it secure. Security architectures can include very different components, from endpoint security practices that control the display of data on smartphones and tablets, to «data in use» network security practices that protect network data and infrastructure from hacking or cyberattacks.

Privacy is a bit of a different issue having to do with an individual's right to own the data generated by his or her life and activities, and to restrict the outward flow of that data. It’s true that in many cases, security and privacy are tandem operational goals. In other words, the same safeguards that offer data security offer privacy for users. But in another sense, privacy is something that may not be built into security efforts, or seen as a necessary objective by big companies or government agencies.

The debate around the mining of personal data by the government, corporations and other agencies shows the difference between security and privacy. Most major organizations see digital security as paramount, while ignoring the digital privacy of users and others. For example, government agencies may help to ensure that private businesses don’t get access to some kinds of personal information regarding citizens, but at the same time, that same agency may be looking to get their hands on the information for other objectives. Many of these issues will continue to come up as different parties struggle to acquire, control and safeguard data.

6. PRIVACY, CONFIDENTIALITY AND SECURITY

The terms privacy, confidentiality and security have a lot in common as they apply to modern-day information technology, but they also have their own meanings and their own significant roles in their application to data maintenance and data management. First, the issue of privacy is one that often applies to a consumer’s right to safeguard his or her information from any other parties. It involves the protection of vulnerable data such as Facebook data, customer response data and other kinds of demographic data or personal data from being freely disseminated over the Internet or sold to third parties. In general, privacy is the individual’s right to keep his or her data to himself or herself.

Confidentiality is a similar idea, but with a slightly different component. IT professionals often talk about confidentiality in terms of a supplier or service provider and its customers. Confidentiality agreements are often applied to situations where someone trusted with personal data must safeguard this data from being released. Alternately, some may define confidentiality as issues about the data that gets collected, where privacy issues have to do, again, with the core principle of an individual not being recorded or monitored.

Security is a different term that's applied to enterprise or government systems. Security may include the idea of customer privacy, but the two are not synonymous. Likewise, security may provide for confidentiality, but that is not its overall goal. The overall goal of most security systems is to protect

an enterprise or agency, which may or may not house a lot of vulnerable customer or client data. Sometimes, the objectives for privacy and security are the same. In other cases, security may not automatically provide for privacy concerns. One example is where a business or government agency may be able to keep its data safe from outside attackers, but where employees may be able to view consumer information. Another scenario might involve situations where a company doesn't face any liability by releasing customer data, and so chooses to do so. Here, the company's security is not jeopardized, but the consumer's privacy is violated. New contracts between businesses and federal agencies are also good examples of how IT issues cut through the different layers between privacy, confidentiality and security.

7. LOSS OF PRIVACY

There are many ways young people and adults can lose their privacy on the Internet, and all have their own dangers. Disclosing your address, telephone number, or even your name to a stranger can put you or family members in danger. It's also important to warn children not to give out information that could jeopardize others — family members, friends, teachers, and classmates.

Sometimes companies and organizations collect information about children for use in marketing, fundraising, and other activities. Children should also be instructed not to give out personal information to Web sites of companies and organizations, even if they have heard of them or have good feelings about them. That includes registering for contests or filling out forms in exchange for prizes, or for the right to download software, or for any other purpose. Children should never reveal any information about themselves without first checking with their parents. Even reputable companies may not obtain information about children without parents' permission; current law protects the privacy of children online. Besides, it's possible for someone to create a Web site that looks like it's from a reputable company but really is not. Software tools exist to restrict sensitive personal information from being transmitted online.

Parents should read the company's privacy policy carefully prior to disclosing personal information about a family member.

Ways to protect your child and family's privacy include:

- Instruct your child not to reveal any personal information without parental permission;
- Consider installing a filter that prevents your child from entering his or her name, address, phone number, or other material;

- Consider installing monitoring software that will disclose if your child has entered personal information;
- Consider preventing your child from using chat groups;
- Consider monitoring your child's incoming and outgoing email;
- Consider limiting chat only to people your child knows or requiring that he chat only in moderated chat areas run by reputable companies or organizations.

8. PASSWORDS SECURITY

The issue of storing passwords in a database is one that requires looking closely at data encryption and security protocols that will stop these valuable pieces of data from being hacked or stolen. Experts have come up with some fairly reliable standards for keeping stored passwords in a database more secure. In addition to principles and strategies for password protection, it helps to promote the use of relatively strong passwords that resist easy guesses by hackers. In addition, engineers and administrators must look at the vulnerability of traffic coming into or out of a database, to prevent different types of password theft.

One fundamental part of password security, in terms of database storage, is called a hash function. A hash function is a complex function that changes a text password into a more complex set of characters by using more complex operations than a familiar mathematical operation such as multiplication. Using hashes and hexadecimal formats can help those who are storing passwords on a database to confuse hackers. Hashes are also used to substitute shorter character strings for longer ones to make data storage and retrieval more efficient.

Another critical aspect of password storage encryption is often called «salt». The principle of salting passwords involves creating additional characters after a text string that are not part of the actual data being stored, but are just useless and insignificant symbols that help to disguise a password. Some refer to salt characters as «noise».

Using complex values and salt, and keeping different types of password keys in strategic places, can help to encrypt the passwords that are stored on a database. Processes for encryption are always evolving, and new technologies could provide additional opportunities for storing valuable data in secure ways. Professionals often use these emerging standards as a reference. For instance, as the technology Pretty Good Privacy (PGP) (which uses hashes) emerged in the early 1990s, it became a standard for encryption.

9. CYBERBULLYING AND ONLINE «FIGHTS»

People sometimes get angry. It's normal, nothing to be ashamed of. The trouble with expressing anger on the Internet is that it's sometimes difficult to resolve disputes. For one thing, you don't have the normal clues you get when you're with someone in person. When people are communicating with text, or in writing, sarcasm and some humor can be insulting instead of funny. It's difficult to know the intensity of someone's feelings and it's very hard to resolve emotional disputes that occur online. More recently cyber bullying has become a disturbing trend online. Recent research has shown that cyber bullies are also at risk for other online threats.

The best defense is to avoid getting into online arguments or disagreements. That doesn't mean people shouldn't speak their minds in forums, newsgroups, and chat sessions, but it does mean that you should treat others with respect and try not to use words that could be offensive to others. If you are going to use humor or sarcasm, you can sometimes avoid misunderstandings by using emoticons (smileys) that express emotions: A simple «:–)» (for «grin») next to a statement can make all the difference between a hostile response and a collective laugh.

Ways to prevent kids from getting into online fights include:

- Discuss with kids how to deal with anger;
- Consider counseling, if kids have serious problems dealing with anger;
- Inform kids that it's not their fault if someone is rude, obnoxious, belligerent, or mean;
- Teach your kids not to respond to comments that are mean and provocative.

10. FILE-SHARING RISKS

Peer-to-peer or file-sharing programs allow you to share your files with others on the Internet — and vice versa. File-sharing is a new and interesting technology that shows promise for future applications. However, just like you shouldn't open email attachments from people you don't trust, you should be wary about downloading files from them as well. You never know what you or your kids may find on the hard drives of random strangers on the Internet. The best tip for file-sharing is to stop and think before downloading files through these networks. Here are more tips to keep your and your kids' file-sharing safe, secure and legal. Some of the risks associated with using file-sharing programs include:

Computer Security. Sharing files with people you don't trust is a matter of hygiene — and you should keep your computer as clean as possible. Using file-sharing networks creates a risk that viruses or other

malignant code could be spread to your computer over the network. Computer security experts are starting to see viruses and malignant code (spyware) spread through file-sharing services. Viruses may damage your computer or interfere with your files; spyware may track your online activities and send that information to third parties. Spyware has been spotted in many places on file-sharing networks — including packaged with the file-sharing clients themselves.

Kids' Access to Pornography. Many file-sharing programs allow children to access inappropriate audio and video clips — most of a sexually explicit nature. Kids searching for popular music files may sometimes inadvertently pull up sexually explicit files that use the same keywords. For older children, parents should be concerned about their access to other people's video libraries that may contain inappropriate videos. If you're concerned about these things, make sure to check your computer for file-sharing programs. Some parental-control tools on the market do not restrict access to file-sharing technologies.

Copyright Law. Many things available on file-sharing networks, including many movies, songs, and video games, are copyrighted by the owner. That means the law protects the owner's right to limit who copies and distributes their content. What does a copyright mean for you? It means that downloading or sharing copyrighted music, movies and software without the copyright owner's permission could put you in serious legal trouble. In those cases, you or your family could be violating federal law and may be sued by the copyright owners or by the government. So, make sure that you or your family does not infringe copyrights while using file-sharing networks. Be smart, and keep your file-sharing legal. Don't allow users to upload your music files unless you're certain that you have permission to do so. You can simply disable the upload feature in your file-sharing program so that you don't inadvertently share files without permission.

Privacy. If mis-configured, some file-sharing programs may expose your entire hard drive to all other users of the file-sharing software. If you keep sensitive information on your computer, like your tax return information and online bank account data, check to make sure that you are not inadvertently making this available to thousands of strangers on the Internet.

11. MAKING THREATS / LAW BREAKING

Kids aren't just potential victims. They can also be responsible for doing things that can hurt other people. This can range from being rude and obnoxious to committing crimes online. There are several reported cases of kids getting into trouble for posting threatening or harassing material on Web pages, in chat rooms and in newsgroups. Kids should remember that anything they say about anyone can be viewed by people all over the world and can have a damaging effect on the person being talked about. Kids should never post anything about another person that could in any way harm that person. That includes publishing names, addresses, or phone numbers of anyone they know. Kids should refrain from saying bad things about other people in public forums, even if they feel they are true, and even if they are angry with that person. Even what appear to be «positive» comments about someone's appearance can be degrading and have a negative affect on that person.

Making Threats. It is wrong and illegal to threaten, intimidate, or harass other people regardless of whether those threats are delivered in person, on the phone, via the mail, or over the Internet. It can be especially harmful to deliver such threats in a public area such as a Web site, chat room, or bulletin board. If you or your child receives serious and frightening threats online, contact law enforcement. Parents should talk with their children about the proper way to behave online and with other people and stress that threatening other people is not only wrong but can get the child into trouble at home, at school, or with the law.

Legal Risks. A lot of material posted on the Internet is copyrighted, which means that it might be illegal to reprint or post the material without permission. Kids need to understand that they do not have the right to re-post or distribute copyrighted graphics, music, videos, and text from Web sites without permission. This includes giving copies of the material to friends. There are some conditions where it is OK to use copyrighted material as part of a student paper or other project, but students should always check with their teacher first and cite the source of the information. Plagiarism — claiming that you wrote or drew something created by another person — is illegal, and committing plagiarism at school can be grounds for serious punishment.

12. INAPPROPRIATE MATERIAL

Just as in any city, there are areas in cyberspace that are not necessarily appropriate for children or teens. Just what those places are depends on the child, the family, and the community, but these typically include sites which are sexual in nature, which contain violent or hateful material, or which advocate the use of weapons or harmful substances such as alcohol, tobacco, or illegal drugs.

Options (not necessarily recommendations) for preventing your child from being exposed to inappropriate material include:

- Set rules about where kids can go online and what to do if they stumble upon inappropriate sites;
- Keep any connected computer in a public area of the house (not a child's bedroom), and make sure that other family members walk in the room periodically;
- Consider not allowing children and teens to use the Internet if parents aren't home. You may wish to consider using time-limiting software to make sure that kids can go online only when you're around;
- Consider checking the browser history to see where kids have been and having a «talk» if they are visiting inappropriate sites;
- Consider installing monitoring software that tracks where kids have been;
- Consider installing filtering software that blocks kids from visiting sites that you feel are in appropriate.

If I Read it Online, is it True?

Knowing how to search the Internet is one thing, however being able to understand what you find is something else. It's easy to become overwhelmed with all the information on the Internet. Children need to learn the finer points of Internet searching and need to learn critical thinking skills so that they can analyze and make effective use of the material they do find. Parents need to provide guidance to their children to help them make sense of the material they uncover and distinguish between fact, opinion, rumors, and lies.

Ways to avoid being overwhelmed or getting «bad» information:

- Learn how to use search engines and how to limit results of searches;
- Understand the difference between reliable and unreliable sources. Get to know the reliable sources on the Internet;
- Have kids cite all of their sources so that teachers and parents can help distinguish between reliable and unreliable sources.

13. WAYS TO AVOID PROBLEMS IN CHAT ROOMS

Chat is a very popular activity for young people, especially teenagers, but it is also the area where they are most likely to get into trouble. When you're in a chat area, it's easy to forget that you are in a public «place» and that you don't necessarily know the true identity of anyone in the chat room. It's common to «meet» someone in a chat area who gains your confidence by being sympathetic and willing to «listen» to your problems. Children and especially teens need to be extremely careful in chat rooms. They should never reveal their identity and they should never assume that someone is as he or she seems to be. They should never agree to meet someone in person based on a friendly online chat without talking to their parents. If parents agree to the meeting, they or another adult should be present and it should be in a public place.

- Do not let your child chat in unmoderated chat rooms. Only allow him or her in rooms run by a reputable company or organization that monitors activity;
- Because many spammers use names they can easily collect from a chat room, consider giving your child a «chat» screen name. This name would be one that is different than their email address. This could help prevent unwanted Spam mail from coming to your child;
- Instruct your child never to give out personal info in a chat room;
- Instruct your child never to agree to get together with anyone they meet in a chat room without first checking with you;
- Talk with your children about the way some people behave in chat rooms. Remind them that people are not always who they seem to be. Remind them to be very careful about people who offer easy solutions to difficult problems or make offers that are «too good to be true»;
- Consider using software to block sensitive personal information from being transmitted through your children's chat.

Instant Messaging

Instant messaging is like chat, except that it's usually a one-on-one experience instead of a group activity. In some ways that's safer if the person the child is messaging is a friend or relative. But it can be dangerous if it's a stranger. Unlike in some chat rooms, there is never anyone else there to monitor activity, so when your child is messaging another person it's as if the two of them are together in a private room.

14. ADDITIONAL TIPS FOR SPECIFIC TYPES OF CYBERCRIME

Once you discover that you have become a victim of cybercrime, your response will depend, to some degree, on the type and particular circumstances of the crime. Here are useful tips to follow for some specific types of cybercrimes:

IN CASES OF IDENTITY THEFT

- Make sure you change your passwords for all online accounts. When changing your password, make it long, strong and unique, with a mix of upper and lowercase letters, numbers and symbols. You also may need to contact your bank and other financial institutions to freeze your accounts so that the offender is not able to access your financial resources.
- Close any unauthorized or compromised credit or charge accounts. Cancel each credit and charge card. Get new cards with new account numbers. Inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions. Close accounts so that future charges are denied. You may also want to write a letter to the company so there is a record of the problem.
- Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft. For example, if a thief has access to your Social Security number, you should contact the Social Security Administration. You should also contact your state Department of Motor Vehicles if your driver's license or car registration are stolen.
- File a report with your local law enforcement agency. Even if your local police department or sheriff’s office doesn’t have jurisdiction over the crime (a common occurrence for online crime which may originate in another jurisdiction or even another country), you will need to provide a copy of the law enforcement report to your banks, creditors, other businesses, credit bureaus, and debt collectors.
- If your personal information has been stolen through a corporate data breach (when a cyberthief hacks into a large database of accounts to steal information, such as Social Security numbers, home addresses, and personal email addresses), you will likely be contacted by the business or agency whose data was compromised with additional instructions, as appropriate. You may also contact the organization’s IT security officer for more information.

- If stolen money or identity is involved, contact the credit bureau to report the crime. Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent activity (such as opening an account with your identification) from occurring. As soon as one of the bureaus issues a fraud alert, the other two bureaus are automatically notified.

IN CASES OF ONLINE STALKING

- In cases where the offender is known, send the stalker a clear written warning saying the contact is unwanted and asking that the perpetrator cease sending communications of any kind. Do this only once and do not communicate with the stalker again. Ongoing contact usually only encourages the stalker to continue the behavior.
- Save copies of all communication from the stalker (e.g., emails, threatening messages, messages via social media) and document each contact, including dates, times and additional circumstances, when appropriate.
- File a complaint with the stalker's Internet Service Provider (ISP) and yours. Many ISPs offer tools that filter or block communications from specific individuals;
- Own your online presence. Set security and privacy settings on social networks and other services to your comfort level of sharing;
- Consider changing your email address and ISP; use encryption software or privacy protection programs on your computer and mobile devices. You should consult with law enforcement before changing your email account. It can be beneficial to the investigation to continue using the email account so law enforcement can also monitor communication.
- File a report with local law enforcement or contact your local prosecutor's office to see what charges, if any, can be pursued.

IN CASES OF CYBERBULLYING

- Tell a trusted adult about what's going on;
- Save any of the related emails, texts, or messages as evidence;
- Keep a record of incidents;
- Report the incident to the website's administrator; many websites including Facebook and YouTube encourage users to report incidents of cyberbullying;
- Block the person on social networks and in email;
- Avoid escalating the situation**:** Responding with hostility is likely to provoke a bully. Depending on the circumstances, consider ignoring the

issue. Often, bullies thrive on the reaction of their victims. If you or your child receives unwanted email messages, consider changing your email address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.

- If the communications become more frequent, the threats more severe, the methods more dangerous and if third-parties (such as hate groups and sexually deviant groups) become involved — the more likely law enforcement needs to be contacted and a legal process initiated.

15. HOW TO AVOID MALWARE

Many cybercrimes start with malware — short for “malicious software”. Malware includes viruses and spyware that get installed on your computer, phone, or mobile device without your consent — you may have downloaded the malware without even realizing it! These programs can cause your device to crash and can be used to monitor and control your online activity. Criminals use malware to steal personal information and commit fraud. If you think your computer has malware, you can file a complaint.

Avoid malware with the following tips:

- Keep a clean machine by making sure your security software, operating system and web browser are up to date;
- When in doubt throw it out. Don’t click on any links or open attachments unless you trust the source;
- Make your passwords long and strong and unique. Combine capital and lowercase letters with numbers and symbols to create a more secure password. Use a different password for each account;
- Set your browser security high enough to detect unauthorized downloads;
- Use a pop-up blocker (the links in pop-up ads are notorious sources of malware);
- Back up your data regularly (just in case your computer crashes);
- Protect all devices that connect to the Internet. Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from malware;
- Make sure all members of your family follow these safety tips (one infected computer on a home network can infect other computers).

16. TIPS TO SAFELY ENJOY SOCIAL NETWORKING

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post.

Have your family follow these tips to safely enjoy social networking:

- Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.
- Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70 % of job recruiters rejected candidates based on information they found online.
- Your online reputation can be a good thing: Recent research also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.
- Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.
- Know and manage your friends: Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life.
- Be honest if you're uncomfortable: If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.
- Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

COMPREHENSION CHECK

1. Match the words to their description:

1) cyberspace	**A)** privacy and security level of personal data
2) Internet privacy	**B)** critical aspect of password storage encryption
3) Internet	**C)** a very popular activity for young people, especially teenagers
4) chat	**D)** security for transactions made over the Internet
5) malware	**E)** virtual computer world
6) salt	**F)** a globally connected network system to transmit data via various types of media
7) Internet security	**J)** malicious software

2. Why is the Internet the most cost-effective communications method in a world?
3. Name some of the risks associated with using file-sharing programs.
4. Why is Internet security becoming a top priority for both businesses and governments?
5. What risk does using file-sharing networks create?
6. Name the options for preventing children from being exposed to inappropriate material.
7. What does a copyright mean for you?
8. Why should kids refrain from saying bad things about other people in public forums?
9. Name the tips to safely enjoy social networking.
10. How can you avoid malware?

DISCUSSION

Discuss the following statements:

A. Internet security is generally becoming a top priority for both businesses and governments.

B. Internet privacy risks: how to minimize them.

C. The terms privacy, confidentiality and security have a lot in common as they apply to modern-day information technology.

D. Ways to protect your child and family's privacy.

E. Many file-sharing programs allow children to access inappropriate audio and video clips.

GLOSSARY

A

abstain	воздержаться
abstract data type	абстрактный тип данных
abuse	злоумышленное использование, неправильное обращение
access	допуск, доступ
accessible	доступный, открытый для доступа
accommodate	приспосабливаться, подстраиваться
accord	предоставлять
accountability	ответственность, подотчетность, контролируемость, возможность учета
accuracy	точность, безошибочность, правильность
accurate	надежный, безошибочный, достоверный
acquisition	сбор данных, комплектование, освоение
Active Directory	активный каталог
active duty	проходящий действительную службу
actor	действующее лицо
ad hoc query	непрограммируемый запрос, случайный запрос
Adaptive Chosen-Plaintext Attack	атака при возможности адаптивного выбора открытого текста
address bar	адресная строка, строка поиска
admittance	допуск, разрешение
adoption	внедрение, ввод в обращение
advance	продвижение, прогресс, рост
Advanced Encryption Standard	расширенный (усовершенствованный) стандарт шифрования
advanced system search	расширенный системный поиск
advancement	успех, прогресс, достижение
advocate	представитель, сторонник, активист
affordable	возможный, доступный, приемлемый
aftermath	последствия
afterthought	запоздалое соображение
agenda	назревший вопрос, проблематика, план действий
agent	агент, исполнительное устройство, программный агент, исполнительная программа
aggregates	сводные показатели, итоговые данные
alert	предупреждение об опасности
algorithmic efficiency	эффективность алгоритма
alias	кличка
alienated	отчужденный, отвергнутый

alignment	формирование, систематизация
allegations	подозрения
alleged	предполагаемый, подозреваемый
all-out	широкомасштабный, всеохватывающий
allude	подразумевать
ample	достаточный, значительный
anti-malware program	программа для защиты от вредоносного ПО
anxiety	страх, боязнь, тревожное расстройство
AOL, America Online	американский медийный конгломерат, поставщик онлайн-служб и электронных досок объявлений
AOL Instant Messenger	программа обмена короткими сообщениями компании AOL
append	добавлять, прикреплять
appending	дополнение
applicable	применимый, соответствующий
apps, applications	приложения
architect	разработчик, архитектор
ARPANET, Advanced Research Projects Agency Network	Сеть Агентства перспективных исследовательских разработок
articulate	четко формулировать, координировать
as such	в этой связи
ascertain	выяснять, устанавливать
ascribed	приписываемый
assembly	сбор, компоновка
assessment	оценка, экспертиза, анализ
asset value	номинальная стоимость
assume	присваивать себе, притворяться
assurance	гарантия, степень доверия
asymmetric encryption	асимметричное шифрование
at large	в бегах
at random	хаотично, бессистемно, беспорядочно
at rest	при хранении, в состоянии хранения
at the expense of	в ущерб
Atbash cipher	шифр Атбаш (шифр сдвига на всю длину алфавита или того числа символов, которые представлены к замене)
attack surface	виды атак
attack-proof	защищённый от средств поражения, стойкий к криптоанализу
audit trail	контрольный журнал, аудиторский учет, контрольный след, журнал регистрации событий, аудиторское заключение
authentication	подтверждение подлинности, авторизация, проверка прав доступа

authentication token	маркер аутентификации
authenticity	подлинность (в применении к пользователю определяет соответствие участника взаимодействия своему имени; в применении к сообщению — достоверность того, что данные были созданы заявленным источником)
availability	доступность (обеспечение наличия информации и работоспособности основных услуг для пользователя в нужное для него время)
awareness	информированность

B

back door	секретный вход
backbone	сущность, основа
back-end server	внутренний сервер
Baconian cipher	шифр Бэкона
bait	приманка, соблазн, искушение; искушать, поддевать, дразнить
balance protection	балансная защита
bar code	штриховой код
basic drives	базисные установки
beat officers	патрульный
behavioral data	динамические характеристики
belligerent	враждебный, агрессивный
benchmarks	критерии, контрольные показатели
benign	безобидный
best practices	наиболее прогрессивные методы
bidder	покупатель
bilateral	двустороннего действия
binary digit	двоичная единица информации
biometric reading	биометрические данные
bit	бит (сокращение от binary digit — «двоичная цифра»), единица информации; небольшое количество, частица
bit-rate reduction	уменьшение битовой скорости передачи данных
bits structure	битовая структура
black hat hacker	черный хакер (хакер-специалист, который направляет свои знания на уничтожение информации, её порчу или кражу)
blended	смешанный, сложный
block cipher	блочный шифр
bludging	бездельничанье; уклонение от jтветственности; уклонение от работы

blurred	расплывчатый, размытый
bogus	фальшивый, сфальсифицированный
booking	регистрация, процедура записи данных об арестованном, которая выполняется в момент попадания в место задержания
brand	качество, фирменный стиль
breach	нарушение, несанкционированный доступ, проникновение
breakdown	распад, развал, упадок, кризис
broad reach	широкий охват
buffer overflow	переполнение буфера
bulk	масса, большое количество
bullet resistant vest	пуленепробиваемый бронежилет
Bulletin Board	электронная доска объявлений
business continuity plan	план обеспечения непрерывной деятельности
business domain	предметная область бизнеса
business intelligence	интеллектуальный анализ данных, сбор, обработка и анализ деловой информации
business performance	производственные показатели, показатели эффективности
business phone	производственная телефонная связь
business-to-consumer	план взаимодействий «бизнес — клиент»
by extension	если говорить более обобщённо
bypass	обойти

C

call	обращаться, запрашивать, кликать
call for	предполагать необходимость, предусматривать, свидетельствовать о необходимости
capability	возможность, мощность, характеристики
capitalize	извлекать выгоду, пользоваться
CAPTCHA, Completely Automated Public Turing test to tell Humans from Computers Apart	полностью автоматический тест Тьюринга для различения компьютеров и людей
capture	завладеть, перехватить
cart	корзина (в Интернет-магазине)
cashier	кассир
catch-all term	собирательный термин
CCTV, closed circuit TV system	система скрытого видеонаблюдения
CD sleeve	конверт для компакт-диска
censor	подвергать цензуре
censorship	цензура, цензурирование
CEO,	генеральный директор, управляющий

Chief Executive Officer	мероприятием
CERN, *фр.* Conseil Européen pour la Recherche Nucléaire	Европейский совет по ядерным исследованиям
certainty of punishment	неотвратимость наказания
challenge	проблема, задача; бросать вызов, создавать угрозу, бороться
challenge-response authentication	запросно-ответная аутентификация
Challenge-Response Authentication Mechanism	метод запросно-ответной аутентификации
character string	текстовая строка, цепочка символов
charge account	расходный счет
checksum	контрольная сумма
Chief Information Officer	руководитель информационной службы компании
CIA = confidentiality, integrity, availability	конфиденциальность, целостность, доступность
CIA Triad	триада CIA
cipher text	шифрограмма, шифртекст, криптограмма
circular buffer	кольцевой буфер, циклический буфер
circumvent	обманывать, обходить, разрушить
classified	закрытый, секретный, засекреченный
classified global security data theft	хищение секретных данных, относящихся к глобальной безопасности
classified information	сведения, отнесённые к государственной тайне
clearance level	уровень допуска к секретной информации
clearance rates	процент раскрываемости, уровень раскрываемости
clearinghouse	центр обмена информацией
cloud computing	«облачная» вычислительная среда
co-conspirators	члены преступного сообщества
code	программный код, машинный код, алгоритм
code access security	безопасность доступа к коду
code base	база исходного кода
code efficiency	эффективность кода
coerce	принуждать, сдерживать, добиваться путем принуждения
cognizant	осведомленный, компетентный
cohesive	связанный
coincidentally	по случайному совпадению
Collaboration System	система для организации совместной работы
collate	сравнивать, сопоставлять
column level	уровень столбца
come by	получить, раздобыть

Command Center	командный пункт, командный центр, штаб
command-line parameters	параметры командной строки
compartmented	с разграничением доступа по категориям секретности
compatibility	совместность
compel	заставлять, принуждать
compile	собирать материал, накапливать данные
complex values	комплексные числа
comprehensive examination	глубокая всесторонняя проверка
compromise	рассекретить, нарушить нормальное функционирование системы безопасности, подвергать риску, ставить под угрозу; нарушение нормального функционирования системы безопасности, рассекречивание зашифрованных материалов, дискредитация
compromising emanations	излучение работающих радиоэлектронных и вычислительных средств, несущее конфиденциальную информацию
computation	вычисление, вычислительная операция
computer forensics	компьютерная криминалистика, компьютерно-техническая экспертиза
computer network	компьютерная сеть
concerted	совместный, осуществляемый сообща
conclusively	достоверно, окончательно
concurrently	одновременно, параллельно
condense	сжимать, уменьшать в объеме
conduit	средство, канал
conferencing	конференц-связь
confidence	уверенность
confidentiality	конфиденциальность (сохранение информации в тайне, невозможность раскрытия информации без согласия заинтересованных сторон)
confusion	запутывание, неопределенность, смешение
consistency	непротиворечивость, последовательность, согласованность
consistent	корректный, правильный
console	система управления
conspiracy	преступный сговор, подпольная организация
constraint	ограничение
construct	структура, конструкция
contingency plan	план на случай неожиданностей, чрезвычайный план
controversial	сомнительный, конфликтный, неоднозначный, провокационный, скандальный

convention	соглашение
conventional crime	общеуголовное преступление
convergence	совмещение
convey	передавать, сообщать, выражать
copy-cat	подражатель, имитатор
correlated	коррелированный
corroborate	подтвердить
corruption	повреждение
cost-effective	эффективный и экономичный
counseling	психологическое консультирование
count	встречаемость
counter	принять ответные меры, противостоять, противодействовать
counterfeit trademark	фальсификация товарного знака
court brief	записка по делу, представляемая адвокатом в суд
coverage	радиус доступа
credential	удостоверение личности, идентификационные данные
credibility	достоверность
Criminal Background Check	проверка на наличие судимости, фактов уголовного преследования, прекращения уголовного преследования
criminal incident	инцидент с уголовно-правовыми последствиями
cripple	наносить урон, повреждать
critical	решающий, ответственный, особо важный
critical infrastructure	важная инфраструктура
cross examination	перекрестный допрос
cross-platform	межплатформный
crux	ключевой вопрос, решающий вопрос
cryptanalysis	криптографический анализ, анализ зашифрованного текста
crypto module	криптомодуль
cryptography	разработка и применение криптографических средств и систем, криптография
cryptology	криптология, наука о расшифровке тайнописи
cryptosecurity	обеспечение безопасности криптографическими средствами, криптостойкость, криптозащита
cult	культ, культовый
custodian	лицо, владеющее секретной информацией или отвечающее за сохранность секретности информации

custom	самостоятельно настраиваемый, устанавливаемый пользователем, пользовательский
custom layout	пользовательский макет
custom profile	настраиваемый профиль
customer response	система обратной связи с потребителем
customize	настраивать
customized	индивидуализированный
cut through	преодолевать
cutting-edge	самый современный, передовой
cyber bully	киберхулиган
cyber fraudster	кибермошенник
cyberactivism	киберактивизм, гражданская активность в Интернете
cyberattack	кибератака
cyberbalkanization	кибербалканизация — превращение глобальной сети Интернет во множество локальных сетей
cyberbullying	киберзапугивание
cybercide	киберсамоубийство
cyberforensics	компьютерно-техническая экспертиза
cyberlaw	Интернет-право, киберправо законы, относящиеся к Интернету и компьютерным правонарушениям
cyberloafing	использование компьютера на рабочем месте для целей, не связанных со служебной деятельностью сотрудника (от английского loaf — «ничегонеделание»)
cyberluring	виртуальное соблазнение
cyberpunk	киберпанк (поджанр фантастики, фокусирующийся на информационных технологиях)
cyberslacking	трата рабочего времени на Интернет
cyberspace	киберпространство, Интернет-пространство
cyberspying	кибершпионаж
cybersquatting	киберсквоттинг, хапперство (покупка и регистрация доменного имени, могущего служить торговой маркой, с целью последующей его перепродажи)
cyberstalking	виртуальное преследование
cyberwarfare	война в кибернетическом пространстве

D

dash camera	автомобильный видеорегистратор
data availability	доступность данных
data capture	сбор данных, выделение данных, перехват данных
data cleansing	очистка данных
data communication	передача данных
data consolidation	сведение информации
data conversion	преобразование данных
data dictionary	словарь данных
data discovery	обнаружение данных
data encryption key	ключ шифрования данных
Data Encryption Standard	стандарт шифрования данных
data entry	введение новых данных
data erasure	стирание, уничтожение данных
data forensics	компьютерно-техническая экспертиза, компьютерная криминалистика
data governance policies	стратегия управления данными, стратегия руководства данными
data in use	используемые данные, данные во время обработки
data intelligence	интеллектуальный анализ данных
data length	длина данных, количество бит данных
data management	управление данными, менеджмент данных
data masking	маскирование данных (процесс идентификации конфиденциальных данных и наложения на них «защитной маски», которая сохраняет их «неприкосновенность», не нарушая при этом функциональной целостности приложения, использующего эти данные)
data mining	интеллектуальный анализ данных, вскрытие информации, извлечение знаний из данных
data privacy	конфиденциальность данных
data profiling	оперативная проверка данных
data properties	свойства данных, характеристики данных
data purging	очистка данных
data quality	качество данных
data range	диапазон данных
data recovery	восстановление данных
data redundancy	резервирование данных, создание запасных копий с целью сбережения информации
data set	набор или совокупность данных, пакет информации

data source identification	выявление источников информации
data storage units	устройство для хранения данных
data store	информационный массив, массив данных
data terminal equipment	терминальное оборудование обработки данных, оконечная аппаратура приёма и передачи данных
data tracking	отслеживание изменений данных
data transmission	передача данных
data type	тип данных, категория данных
data validation	проверка корректности данных
Data Warehouse	хранилище данных
database engine	процессор базы данных, блок программы, задающий способ управления и манипулирования базой данных
database environment	среда базы данных
database manager	программа управления базой данных
debrief	заслушивать отчет
deceit	обман, мошенничество
Decision Support System	система поддержки принятия решений
declassification	рассекречивание
decryption	дешифровка, расшифровка, декодирование
deduplicating	дедупликация данных, удаление избыточных дублированных данных
defacement	порча, искажение, потеря удобочитаемости
default settings	настройка по умолчанию
defeat	крушение
deficiencies	недоработка, недостатки
degrade	уменьшить, понизить
degrading	унизительный, оскорбительный
deliberate	предумышленный
delineate	описывать, определять
DoS, denial of service	отказ в обслуживании
denial-of-service attack	атака типа «отказ в обслуживании»
denied	отклоненный
Department of Motor Vehicles	Служба регистрации транспортных средств
deploy	применять, использовать
deployment	применение, внедрение, размещение
derivative	неоригинальный, неисконный, переделанный
descriptive statistics	описательная статистика
desktop	оперативная область, рабочий стол, стационарный компьютер
deterioration	деградация, упадок, резкое ухудшение
deterrence	удерживание от совершения действий устрашением
deterrent	фактор сдерживания, средство устрашения

deviant	с отклонением от нормы
devoid	лишенный чего-то, не имеющий чего-то
diffuse	разрядить
digital data	цифровые данные
digital forensics	цифровая криминалистика, компьютерная криминалистика
digital format	формат цифровых данных, цифровой формат
dimension	аспект, показатель, характеристика
directory	хранилище, каталог адресов
directory entries	записи каталога
disaster recovery	восстановление после аварии, обеспечение функционирования в случае чрезвычайных ситуаций
discard	выбросить, списать
disconnect	отключение от сети, разъединение
discrepancy	несоответствие, расхождение
discrete values	дискретные значения
discretion	свобода действий, свобода принимать решение; осторожность, благоразумие, рассудительность
disgruntled	недовольный, возмущенный
disguise	маскировать, скрывать
disobedience	неповиновение
disorders	нарушение, нарушение деятельности
dispatch	диспетчерская служба
disproportionately	несоразмерно, непропорционально
disrupt	подрывать, разрушать, блокировать
distinct	отдельный, обособленный, отличающийся
distorted	искаженный, деформированный
distract	сбивать с толку, отвлекать
distributed	распределённый
DDoS, distributed denial of service attack	распределённая атака «отказ в обслуживании»
diverse	разнообразный, многообразный
divert	переадресовать
divisive	противоречивый, вызывающий разногласия
divulge	разглашать, обнародовать
DLL, dynamic link library	библиотека динамической компоновки, динамически связываемая библиотека
DNS, domain name server	сервер доменных имен, система именования доменов
DOJ, Department of Justice	Министерство юстиции
domain name hijacking	хищение доменного имени
downtime	время простоя
driving under the influence	управление автомобилем в состоянии

	алкогольного опьянения или под действием наркотиков
DSL, digital subscriber line	цифровая абонентская линия

E

eavesdrop	перехватывать информацию
efficiency	оперативность, работоспособность
e-Guardian	система e-Guardian для обмена информацией, связанной с угрозой терроризма, между органами полиции разных штатов
electronic advocacy	правозащитная деятельность, информационно-пропагандистская деятельность
electronic bread crumbs	улики, путь к просматриваемому файлу, «хлебные крошки»
elicit	вызывать, извлечь, добиваться
elusive data	труднонаходимые данные
email scam	мошенничество по электронной почте
emanations	опасное излучение (работающей радиоэлектронной аппаратуры)
embedded	встроенный
embedding	размещение, вложение
embrace	дружелюбно встретить, полюбить, подхватить
emerge	возникать, появляться
emission security	скрытность излучения радиоэлектронной техники, конфиденциальность передачи данных
emoticon	эмограмма, смайлик
encase	упаковать
encompass	охватывать, касаться, включать
encounter	столкновение, точка соприкосновения; встречаться, иметь место, обнаруживаться
encourage	служить стимулом, мотивировать
encryption	криптографическая защита; зашифровывание, кодирование
encryption engine	шифровальная машина, криптографическое устройство
end user	конечный пользователь
endeavor	начинание, проект, попытка
engross	поглощать, занимать
enhance	повышать, усиливать
enhancement	расширение технических возможностей, улучшение, совершенствование
Enterprise Resource Planning	планирование ресурсов предприятия
enterprise trade secret theft	хищение коммерческой тайны

entity	организация, субъект
environment	режим, среда, конфигурация, условия окружающая обстановка, реалии; оборудование; контент
erase	очищать, затирать
ethical	порядочный
evasion	уклонение, обход, увертка
event log data	данные журнала событий
event processing	обработка событий
ever more	все более и более
evidentiary	доказательный
evocative	экспрессивный, выразительный
evolve	претерпевать изменения, разрабатывать, развиваться
exaggerated	находящийся в особо неблагоприятных условиях
exception handling	управление исключительными ситуациями
exclusive	исключительный, с ограниченным доступом
executable	исполняемая программа
executable code	выполняемая программа
executive information system	информационная система руководителя
executive level	руководящее звено
Executive Support System	система обеспечения работы, исполнительная система
exonerate	оправдать, реабилитировать
expedient	надлежащий, соответствующий
expeditiously	в оперативном порядке, немедленно
Expert System	экспертная система
expertise	специальные знания, эрудиция
exploit	компьютерное вторжение, проникновение из Интернета
exposure	представление конфиденциальной информации в открытом виде; уязвимость
extortion	вымогательство, получение информации насильственным путём
extraction	извлечение, изъятие, выемка

F

facet	аспект, сторона, грань
facial recognition technology	технология распознавания лиц
facilitate	облегчать, способствовать, содействовать
fairness	справедливость, непредвзятость, объективность
fake	подделка, фальсификация
fall prey	стать жертвой

FAST, Federation Against Software Theft	Федерация по борьбе с незаконным использованием программного обеспечения
felon	преступник
fervently	горячо, страстно, истово
fiber-optic	оптоволоконный
file a complaint	заявить, подать заявление, подать жалобу
file level	уровень файла
File Transfer Protocol	протокол передачи файлов
file-sharing program	программа обмена файлами
financial extortion	вымогательство денег
findings	полученные сведения, полученные данные
finer point	тонкость, нюанс, деталь
firewall	система сетевой защиты, система защиты доступа, межсетевая защита, сетевое устройство защиты
firmware	аппаратно-программное обеспечение, прошивка, программно-техническое обеспечение
fiscal year	фискальный год, отчетный год
fitness	пригодность для эксплуатации
flag	отмечать, размечать, сигнализировать
flaw	дыра, брешь
flawed	несовершенный, небезупречный, проблемный
flea market	вещевой рынок, барахолка
fleet management	транспортный отдел
focal point	информационно-координационный центр
focus	концентрация внимания, акцент
follower	подписчик, читатель, фолловер
foolproof	защищенный от неумелого пользования
footing	фундамент, основание
forecast	прогнозировать, предусматривать
foreign exchange	обмен иностранной валюты
foremost	основной, главный, ключевой
foster	способствовать развитию, поощрять
fragments	обрывки
framework	концепция
fraud	мошеннические действия, мошенничество
fraudster	мошенник
fraudulent	мошеннический, совершаемый путем обмана
frequency	частота, частотность, повторяемость
fringe groups	группа радикалов, неформальная группа, маргинальная группа
fuel	активизировать, дать толчок
fugitive	лицо, скрывающееся от правосудия, беглый преступник

functionalities	функциональные возможности
fundraising	сбор пожертвований
furtherance	поддержка, дальнейшее развитие, способствование, продвижение
fusion center	центр обработки информации

G

gain momentum	расти, увеличиваться
gain traction	становиться все более популярным, наращивать обороты
gambling	игра в азартные игры
garbled data	зашифрованные данные, искаженные данные
gateway	межсетевой шлюз, межсетевой интерфейс, шлюз с контролируемым доступом «Гэйтуэй»
geek	помешанный на компьютерах, компьютерный фрик
generic	ничем не выдающийся, ничем особым не примечательный
generic data	универсальные данные
gifted	способный, одаренный, талантливый
Global Information System	глобальная информационная система
global positioning system	глобальная навигационная спутниковая система
global village	глобальная деревня, деревня с Землю величиной (о нашей планете в конце XX века, когда широкое развитие получили электронные средства связи)
go cold turkey	резко и бесповоротно отказываться, бросать раз и навсегда
granular	детализированный
graphical user interface	графический интерфейс пользователя
gray hat hacker	серый хакер (специалист по компьютерной безопасности, использующий как белые, так и черные методы, с незначительной выгодой для себя)
grin	улыбка во весь рот
grind to a halt	застопориться, застрять, прекратить работу
grip	хватка, контроль
guesswork	догадка, предположение
guided	управляемый, направляемый, пошаговый

H

hacking	хакерство
hacktivism	хактивизм (хакерство во имя политических (религиозных) целей)
haphazard	бессистемный, случайный

harass	преследовать, причинять беспокойство
harassing	преследование, третирование
harassment	преднамеренное причинение беспокойства, домогательство
hard tag	охранная этикетка
hard token	токен, аппаратный токен
hash function	функция хэширования, функция расстановки ключей
hash value	хэш-значение или значение хэша (значение хэш-функции, преобразующей данные произвольной длины (обычно, строку) в число фиксированной длины)
hashing algorithm	алгоритм хэширования, алгоритм перемешивания
hashing systems	системы, использующие хэш-функции
hassle	трудности, препятствия, хлопоты
hate crime	преступление на почве ненависти
hate group	группа ненавистников, ксенофобская группировка
hazard	злоумышленное действие, опасная обстановка, стихийное бедствие
heavy user	интенсивный пользователь
heed	обращать внимание
hexadecimal format	шестнадцатиричный формат
high-consequence	значительное последствие
highest bidder	лицо, предложившее наивысшую цену
high-execution-speed	высокоскоростное выполнение
high-impact	высокоэффективный
high-profile case	дело, получившее широкий общественный резонанс
high-rate	высокий показатель, высокий уровень
hinder	не давать, препятствовать
hit	совпадение при поиске
hoax	фальшивка, подделка, сфабрикованная акция
hobble	спотыкаться, стреножить, препятствовать
Homeland Security	национальная безопасность, государственная безопасность
host	выполнять роль принимающей стороны, размещать, хозяин
host file	файл узла (содержит IP-адреса узлов и список соответствующих имен DNS)
hot spot	район напряжённой обстановки, «горячая точка»
hotspots	беспроводная точка доступа
HTML, HyperText Markup Language	язык разметки гипертекста

HTTP, HyperText Transfer Protocol	базовый протокол для соединения клиентов и серверов WWW, протокол передачи гипертекстовых файлов
HTTPS, HyperText Transport Protocol Secure	протокол защищённой передачи гипертекстовой информации

I

I.D., identity document	документ, удостоверяющий личность
ICANN, Internet Corporation for Assigned Names and Numbers	Корпорация по присвоению имен и номеров в Интернете
identity theft	хищение персональных данных, кража идентификационных данных
illegitimate	противозаконный
image database	база данных изображений
immigration	паспортный контроль
impact loss	динамические потери
impersonate	выдавать себя за другое лицо, имитировать
implement	внедрять, вводить в действие
implementation	практическое применение, реализация, внедрение
implore	просить, упрашивать
impostor	мошенник, самозванец, выдающий себя за другого
in and of itself	сам по себе, по своей сути, как таковой
in conjunction with	одновременно, в сочетании с
in motion	во время передачи (данных)
in the name of	с целью, в целях
in the wake	после
in transit	в процессе перемещения, при пересылке
inadvertently	непреднамеренно, нечаянно
inappropriate	некорректный, неуместный, непристойный
incapable	неспособный
incapacitation	лишение преступника возможности совершать преступления заключением его под стражу
incarceration	лишение свободы, арест с содержанием в месте заключения
incentive	стимул, побуждающий мотив, мотивация
inception	возникновение, образование
Incident Management System	система контроля происшествий
incite	стимулировать, поощрять, подстрекать
increment	этап, вариант
incremental	поэтапный
incremental backup	инкрементное резервное копирование
incriminate	изобличать, инкриминировать

indecipherable	не поддающийся расшифровке, недешифруемый
indictable offence	преступление, преследуемое по обвинительному акту
indispensable	необходимый, незаменимый, неотъемлемый
inefficiency	несостоятельность, несовершенство, потеря производительности
infancy	начальная стадия развития
infiltrate	проникнуть, внедриться
infiltration	несанкционированный доступ
inflammatory	подстрекательский, провокационный
information asset	информационный ресурс
information assurance	обеспечение целостности и безопасности информации
information hiding	сокрытие информации, экранирование информации
Information Sharing Environment	система информационного обмена, среда для совместного использования информации
information warfare	информационное противоборство, информационная война
infringement	нарушение, ущемление
initial release	первый выпуск, исходная версия
input	вводить
input validation	проверка вводимых значений
insider	инсайдер, лицо, имеющее доступ к конфиденциальной информации в силу служебного положения
insidious	хитрый, коварный, скрытый
insignias	опознавательные знаки
instant messaging	обмен мгновенными сообщениями
intangible	неосязаемый
Integrated Automated Fingerprint Identification System	интегральная автоматизированная система идентификации по отпечаткам пальцев (дактилоскопической идентификации)
integrity	надежность, безопасность, целостность (непротиворечивость и правильность информации, защита информации от неавторизованной модификации)
intelligence	оперативная информация
intelligent building	компьютеризированное задание, интеллектуальное задание
interagency	межведомственный
intercepting	перехватывать
interception	перехват, прослушивание
interchangeably	взаимозаменяемо

Internet addiction	Интернет-зависимость, синдром привыкания к Интернету
Internet Relay Chat	трансляция чатов в Интернете, ретранслируемый Интернет-чат
Internet scam	Интернет-мошенничество
Internet Service Provider	Интернет-провайдер
Internet-enabled	Интернет-ориентированный, функционирующий через Интернет
interoperability	интероперабельность, способность к взаимодействию, совместимость
intimidate	угрожать, запугивать, шантажировать
intra-agency	внутриведомственный
intranet	интранет, замкнутая корпоративная сеть, работающая по стандартам Интернет
intricate	сложный
intruder	лицо, не имеющее санкционированного доступа, злоумышленник
intrusion	вторжение, нарушение, проникновение
intrusion detection networks	сетевая система обнаружения вторжений
intrusion detection system	система обнаружения вторжений
intrusion prevention system	система предотвращения вторжений
intuitive media	интуитивно-понятная среда
inventory	материально-технические ресурсы
involved	сложный
involvement	задействованность, подключение
IP address	адрес Интернет
IP, Internet Protocol	межсетевой протокол
issuer	банк, выдавший карточку; организация, выставляющая счёт

J

jailbreak	изменение микропрограммы устройства, не предусмотренное производителем, перепрошивка (снятие ограничений на доступ к файловой системе Unix в основном iPhone и iPad)
jeopardize	подвергать опасности, ставить под угрозу
jeopardy	опасность, риск
Joint Terrorism Task Forces	объединённая группа по борьбе с терроризмом
junk mail	нежелательная почта, спам, информационный мусор
justifiably	не без основания, оправданно, правомерно

K

keep pace	не отставать, идти «нога в ногу»
keep tabs on	следить, вести учет
kernel modules	модуль ядра
key agreement system	система согласования ключей
key card	карточка с ключом
key drivers	ключевые движущие силы
key logger	программа для перехвата вводимой с клавиатуры информации
keyed	набранный на клавиатуре
key-management system	система управления пользованием криптографическими ключами
keystroke	нажатие на клавишу
keystroke logger	регистратор работы клавиатуры (программа или аппаратное устройство, регистрирующее каждое нажатие клавиш на клавиатуре компьютера. Аппаратное устройство такого типа прячется в кабель, соединяющий клавиатуру с системным блоком, и не требует ПО на контролируемом компьютере. Применяется для контроля за действиями служащих)
keystroke logging	регистрация нажатий клавиатуры (с помощью программы или аппаратного устройства, регистрирующего каждое нажатие клавиш на клавиатуре компьютера)
keyword	ключевое слово, зарезервированное слово, дескриптор

L

lack	испытывать недостаток, не хватать
lapse	ошибка, оплошность
launder	«отмывать»
layered	многоуровневый
layout	структура, общий вид
leap	скачок
legacy	прежняя версия
legal avenues	юридический механизм, средства защиты
legitimacy	законность, правомерность, легитимность
legitimate	неподдельный, настоящий
liability	ответственность, обязанность, необходимость
license plate reader	система считывания номерных знаков
lifeline	жизненно важная артерия, спасательный круг

limitless	безграничный, неограниченный
linkage	соединение
literally	буквально
load/stress testing	нагрузочное тестирование
loan	ссуда, кредит
lockdown	блокировка
logo	товарный знак
longevity	долговечность, срок службы
loophole	лазейка, место утечки, брешь, дыра
loot	грабить, захватывать трофеи
lossy	с потерями
lowercase letter	знак нижнего регистра, строчная буква
lucrative	прибыльный, доходный
lure	завлекать, заманивать
lurer	соблазнитель, искуситель
lurk around	оставаться незамеченным, прятаться

M

mainframe	мэйнфрейм, «большой компьютер»
maintenance check	плановая проверка технического состояния
make	марка
makeup	составляющие, строение, структура, схема
malicious	злоумышленный, вредоносный
malicious actors	страна-изгой
malicious code	злонамеренный код, вредоносный код
malicious software	программные средства, нарушающие нормальную работу системы, вредоносное программное средство
malignant	опасный, вредоносный
malware	вредоносное программное обеспечение
manage	управлять, организовывать, администрировать
Management Information System	информационная система административного управления
man-in-the-middle attacks	атака «злоумышленник в середине» (атака, при которой злоумышленник может читать, вставлять и изменять по своему желанию данные между двумя сторонами без того, чтобы какая-либо из сторон знала, что канал между ними взломан)
manipulate	обрабатывать
mapping	построение диаграммы
mapping system	картографическая система
marginal	незначительный, минимальный
marginalized	выброшенный из общества, маргинальный, социально отчужденный

maritime piracy	морское пиратство
market share	доля рынка
mastery	совершенное владение, мастерство
matching key	ключ-«напарник», согласованный ключ
maximum up	максимально возможный
MD5, Message Digest 5	часть сообщения, удостоверяемая электронно-цифровой подписью
mean	средний, мерзкий, недостойный
mean-spirited	злонамеренный, подлый, низкий
media	носитель информации
memory cache	кэш, сверхоперативная память
mere	простой; только лишь, всего лишь
merging	объединение, слияние
metadata	данные, описывающие свойства данных, данные о данных
mimic	подделывать, имитировать
mine	разрабатывать; извлекать информацию; собирать, отфильтровывать и анализировать данные
mining	разработка, сбор
mIRC, Microsoft Internet Relay Chat	специальный сервер Microsoft в сети Интернет, обеспечивающий возможность проведения интерактивной конференции в реальном времени
misconfigured	неправильно задать конфигурацию
mission-critical	особой важности
mitigate	уменьшать, смягчить последствия, нивелировать
mixed-mode	смешанный режим
modest	незначительный, не выдающийся
modus operandi	способ совершения преступления, модус операнди
momentum	движущая сила, импульс, стимул
money mules	«дроп», «мул», «деньгонос», курьер
money-wiring service	денежный перевод
monitoring programs	программа-монитор
move request	запрос на перевозку
mug shot	фото арестованного, совмещенное фото в профиль и анфас
multijurisdictional	мультиюрисдикционный, межюрисдикционный
MySQL	Мускуль, свободная реляционная система управления базами данных

N

name calling	охаивание, переход на личности, обзывание
narrative	сведения, информационное сообщение
narrow-minded approach	предвзятый подход
national	гражданин
national assets	национальное достояние
nefarious	вредоносный, злодейский
negligible	ничтожный
netizen	кибергражданин, сетянин, житель Интернета, нетизен, веб-гражданин
network attached storage	система хранения данных, подключаемая к сети; сетевой дисковый массив
network connection	сетевое соединение
NIC, Network Interface Card	сетевой адаптер, плата сетевого интерфейса
network node	сетевой узел
network outage	отказ сети, выход сети из строя
network security	безопасность сетей, сетевая безопасность
Neuromancer	Нейромант
newbie	новичок, начинающий пользователь, нуб
news feed	лента новостей
niche	узкоспециализированный
node	узел, узел сети
nomenclature	терминология, понятийный аппарат
nominal	заданный, номинальный
nominal data	паспортные данные
non-core	непрофильный
nonrepudiation	невозможность отказа от ответственности
nonvolatile storage	энергонезависимое запоминающее устройство
notably	в частности
notice	уведомление, оповещение, информационное письмо
notorious	заведомый, печально известный, общеизвестный
notoriously	общеизвестно
NSF, National Science Foundation	Национальный научный фонд
NSFNET, National Science Foundation Net	Глобальная сеть Национального научного фонда

O

obnoxious	неприятный; беспардонный
offending patterns	алгоритм, закономерность
Office Automation	офисная автоматизация, автоматизация учрежденческой деятельности

offset	уменьшать, нивелировать
offsite	вне границ, за пределами
omitting	упущение, пропуск
omnipresent	повсеместный, всепроникающий
on par	в соответствии
on the flip side	в то же время
one-way encryption	необратимое преобразование открытого текста в шифртекст, одностороннее шифрование
online predatory crime	хищническое, корыстное преступление в режиме он-лайн
online stalking	преследование и застращивание в Интернете
on-the-go	в движении, на ходу
open-minded	восприимчивый, непредвзятый
operational data	оперативные данные
optical character recognition	электронное распознавание буквенно-цифровых знаков, оптическое распознавание символов
Oracle	объектно-реляционная система управления базами данных компании Oracle
Orange Book	критерий оценки пригодности компьютерных систем
otherwise	в прочих случаях
outlets	информационные каналы, информационные источники
outlying	выпадающий, несвойственный, чуждый
outright	настоящий, полный
outsourcing	заимствование извне
outward flow	утечка
over time	в течение продолжительного периода
overarching	ключевой, глобальный, всеобъемлющий
overlap	частично совпадать, перекрывать, совпадение
oversee	обеспечить контроль, курировать
overwhelm	потрясти, ошеломить, перегрузить
overwhelmed	перегруженный
own	отстоять, владеть, взять под контроль

P

packet sniffer	1) средство мониторинга и анализа проблем в компьютерных сетях; 2) средство незаконного сбора и анализа данных в компьютерных сетях с целью получения несанкционированного доступа
padding	дополнение блока данных незначащей информацией или фиктивными битами;

	холостое заполнение
padlock	навесной замок
paper trail	документальное свидетельство, записи
paramount	первостепенный, наиважнейший
Parkerian hexad	гексада Паркера
parody	пародия, карикатура
parole	освобождать заключённого условно
parsing	синтаксический анализ
passcode	код доступа
password cracking	раскрытие пароля, обход системы доступа по паролям
password sniffing	«выслеживание» пароля, выявление пароля незаконными способами
patch	«заплата», вставка в программу, корректирующий файл; делать «заплату» (исправлять программу с помощью подпрограммы)
pathological gambling	патологическое пристрастие к азартным играм
PDA, Personal Digital Assistant	карманный персональный компьютер
P2P, peer-to-peer communication	передача между равноправными узлами
penalizing	наложение штрафа
penitentiary	исправительное учреждение
perceive	понимать, расценивать, воспринимать
perceived	выявленный, кажущийся
percentile	процентиль (характеристики набора данных, которые выражают ранги элементов массива в виде чисел от 1 до 100 и являются показателем того, какой процент значений находится ниже определенного уровня)
perception	понимание, осознание
permanently	постоянно
perpetrate	совершать
perpetration	совершение
perpetuate	сохранять навсегда
persistent	неизменяемый, долговременный
personal effects	вещи личного пользования
personal identification number	персональный идентификационный номер, пароль для доступа к системе
persuade	убеждать
PGP, Pretty Good Privacy	программа защиты сообщений, передаваемых по сетям связи и электронной почты с шифрованием; «надёжная конфиденциальность»

pharming	фарминг (метод Интернет-мошенничества, автоматическое перенаправление пользователей на фальшивые сайты)
phishing	«фишинг», преступная деятельность Интернет-мошенников, действующих под видом благонадёжных компаний и юр. лиц, с целью незаконного получения секретной информации: паролей, данных кредитных карточек, логинов
phony	фальшивый, поддельный
phreaking	телефонное мошенничество
physical security	непосредственная защита (меры, предусматривающие физическую защиту ресурсов от преднамеренных или случайных угроз)
physical storage resources	физический ресурс хранения
pillar	компонент, основа, краеугольный камень
pin	прикалывать, закреплять, прикреплять
PIN, Personal Identification Number	личный номер, средство идентификации
ping	команда ping
plain text format	текстовый формат
plug	подключать, вставлять в контактное гнездо
Pod slurping	«пожирание данных при помощи iPod»
point to a fear	указывать, отмечать
pointless	никчемный, лишенный смысла
police dispatch center	дежурная часть
pop-up blocker	блокировщик всплывающих окон
portable hard drive	внешний жёсткий диск
porting	портирование программного обеспечения, т. е. адаптация некоторой программы или её части с тем, чтобы она работала в другой среде, отличающейся от той среды, под которую она была изначально написана с максимальным сохранением её пользовательских свойств
possession (or control)	управляемость, или владение (гарантия того, что законный владелец является единственным лицом, во власти которого изменить информацию или получить к ней доступ на чтение)
post	размещать пост, поместить сообщение
power down	выключить, отключить питание
precautions	меры предосторожности, меры безопасности
precursor	предшественник, прототип
predatory crime	хищническое, корыстное преступление

predictive analytics	прогнозная аналитика
pre-emptive	превентивный, упреждающий
preferences	установки, параметры, настройки
prefix	код зоны, код города
preoccupied	поглощенный мыслями, озабоченный
pressing	насущный, неотложный, актуальный
pretext	предлог, причина, мотив
pretty good privacy	«надёжная конфиденциальность» (алгоритм шифрования), программа кодировки PGP
prevalent	широко распространенный, общепринятый
prioritize	уделить первостепенное внимание
privacy	неприкосновенность информации, сохранение тайны при хранении информации, секретность информации
privacy protection program	программа защиты частной информации, конфиденциальности
private key	секретный ключ, личный ключ, ключ отдельного пользователя
privileged	конфиденциальный
privy	допущен
proactive	превентивный, действующий на опережение, дальновидный
probation	условное освобождение осужденного под надзор
process	преследовать в судебном порядке, возбуждать дело
process-oriented	процессно-ориентированный
procurement documentation	закупочная документация
profile	портрет, досье
proliferate	быстро распространяться
prolific	богатый, преуспевающий
prominent	известный
promiscuous mode	режим приёма всех сетевых пакетов, неразборчивый режим
promote	продвигать, пропагандировать
prompt	запрос на ввод, диалоговое окно; подталкивать, побуждать
proprietary	закрытый, частный, коммерческий, с закрытым исходным кодом, составляющий собственность,
Protection Order	судебный приказ о защите членов семьи в случае семейных ссор, охранный ордер
Protective Interest	база данных преступников, представляющих угрозу для лиц, нуждающихся в защите
provide for	обеспечивать, предусматривать

provide insight into	позволить понять, проводить детальный анализ
proxy server	прокси-сервер (обеспечивает защиту локальной сети от атак), уполномоченный сервер
public key	ключ общего пользования, открытый криптографический ключ
Public Key Cryptography	криптографическая защита с открытым ключом, криптография множественного доступа
Public Key Infrastructure	инфраструктура сертификации открытых ключей
public perception	общественное понимание, восприятие
pull up	вытянуть, остановиться на
punch cards	перфорированная карта, перфокарта
purging	уничтожение, стирание
pursue	продолжать, проводить, осуществлять

Q

quantum	значительный, существенный

R

radio-frequency identification	радиочастотная идентификация
raft	множество
RAID, Redundant Array of Inexpensive Drives	матрица недорогих дисковых накопителей с избыточностью
raise concerns	беспокоиться, выражать беспокойство
ramifications	разновидности
random access	случайный доступ, прямой произвольный доступ
random access memory	запоминающее устройство с произвольной выборкой, оперативная память
ransom	выкуп
rapport	отношения, взаимоотношения, контакт
RDBMS, Relational Data Base Management System	реляционная система управления базой данных
reach out to	связаться, выйти на диалог, находить общий язык, установить контакт
reactive	ответный, последующий, реактивный
read access	доступ с правом считывания информации
realm	область, сфера, мир
rearranging	изменение конфигурации, реконфигурация
rebellion	восстание, мятеж, бунт, неповиновение
receipt	квитанция об оплате
recognition	распознавание, идентификация

records management systems	информационная система
recovered	изъятый
recruiter	работодатель, специалист по подбору персонала
recurring	регулярно возникающий, периодический
redress	исправлять, корректировать
redundant	дублирующий, резервированный, резервный,
reference	справочная информация, справочное описание
reference sample	контрольный образец
registry	реестр
reinforcement	усиление, подкрепление
relational	реляционный, связанный с описанием отношений
reliability	достоверность, надежность
remediation	способ, средство, ремедиация (устранение нарушений политики хранения конфиденциальных данных в информационных системах)
remedy	лечить, устранять неисправность
remote	удаленный
remote access	удаленный доступ
remote sharing	удаленное совместное пользование
repeat offender	преступник, повторно совершивший преступление
repeatability	повторяемость, возможность повторения
repercussions	негативные последствия
replication	копирование
repository	центральная координационная база данных
reputable	заслуживающий доверия
reside	находиться, локализоваться, храниться
resource allocation	распределение ресурсов
resource consumption	потребление ресурсов
response to	действия при, действия в случае
retailer	магазин розничной торговли
retain	оставлять за собой
retention	сохранность, срок хранения
retrieval	выборка, извлечение (информации)
retrieve	находить, извлекать, истребовать, изымать
return policies	условия возврата товара
reusable components	компонент многократного использования
reveal	рассекречивать, раскрывать, демаскировать
reverse engineering	реверс-инжиниринг, обратное конструирование, восстановление конструкции
revoke	аннулировать

rewrite	перезапись
rich data	данные и средства наглядности
ridicule	высмеивать
rigorous	строгий, тщательный, жесткий
risk acceptance	степень допустимого риска
risk mitigation	снижение риска, ослабление воздействия риска
risky ventures	рискованное предприятие
rival	конкурент, соперник
robust	устойчивый к сбоям, надежный
rogue	жулик, мошенник
rogue access point	подставная точка доступа (неавторизованная точка доступа, имеющая параметры конфигурации, позволяющие кому угодно получить доступ к сетевым ресурсам)
rogue applications	несанкционированное приложение
role-based security	ролевой принцип обеспечения безопасности
rooting	рутинг (процесс получения прав суперпользователя Root на устройствах под управлением операционной системы Android)
rootkit	конструктор корневого каталога
router	маршрутизатор, роутер
RSA, Rivest-Shamir-Adleman	цифровая подпись Райвеста-Шамира-Адлемана
RSS feed	Интернет-ресурс в формате RSS: RSS-фид, RSS-канал, RSS-лента
RSS, Rich Site Summary	семейство XML-форматов (предназначены для описания лент новостей, анонсов статей, изменений в блогах. Обычно с помощью RSS 2.0 даётся краткое описание новой информации, появившейся на сайте, и ссылка на её полную версию)
rule-based	основанный на системе правил
runtime execution	время выполнения программы

S

sabotage	диверсионные действия, вредительство, подрывная деятельность
salt	соль, помеха (строка данных, которая передаётся хэш-функции вместе с паролем, используется для удлинения строки пароля, чтобы увеличить сложность взлома)
savvy	хорошо информированный, подкованный
scalability	универсальность, расширяемость, масштабируемость

scam	надувательство, мошенническая проделка, мошенничество, злоупотребление доверием
scare	паника, страх
scrambling	скремблирование, перестановка элементов, шифрование, кодирование, смешивание
screen lock feature	функция блокировки экрана
screen name	имя пользователя, ник
scrutiny	тщательная проверка, внимательное изучение, экспертиза
seamless	непрерывный, постоянный
secondary storage	внешняя память
Secret Key Cryptography	секретный криптографический ключ
secure shell	защищенный командный процессор
secure socket layer	протокол защиты информации в Интернет, протокол безопасных соединений
securities	ценные бумаги
security	безопасность, защищенность
security architecture	архитектура системы безопасности
security breach	нарушение системы безопасности
security event	событие, изменяющее состояние системы безопасности
security flaw	слабое звено в системе безопасности
security information	информация о безопасности
security practices	методика обеспечения безопасности
security protocol	протокол обеспечения безопасности
security token	маркер доступа, маркер безопасности
seek	поиск, обращаться, просить
seek out	разыскивать, пытаться получить
segment	разбивать на части, сегментировать
segregation	отдельное хранение, изолированное хранение
self-replicating	самовоспроизводящийся
sense of community	чувство общности, дух коллективизма
sensitive	носящий конфиденциальный характер
sensitive asset	конфиденциальный цифровой объект
sensitive information	информация с ограниченным доступом, конфиденциальные данные; информация, содержащая важные сведения
sensitive unclassified information	несекретная, но важная, требующая защиты информация
sensitivity	уязвимость
sensors	средства наблюдения и обнаружения, датчики
sequential access	последовательный доступ
service level agreement	соглашение об уровне услуг, договор о предоставлении услуг
sexually explicit	непристойный, откровенный

show off	хвастаться, афишировать, стремиться произвести впечатление
shutting down	выключение, отключение
simplified	упрощенный
single	взятый в отдельности
site scraper	программа для скачивания веб-сайтов
sit-in	сидячая забастовка
skewed	искаженный
slew	масса
slurp	считывать целиком
smarts	ум, сообразительность, умственные способности
smishing	смишинг
SMTP, Single Mail Transfer Protocol	протокол обмена почтовыми сообщениями
sniffing	анализ трафика, контроль сообщений, передаваемых по сети связи, с целью выявления конфиденциальной информации
so much so	до такой степени, что
social engineering	социальная инженерия (добывание идентификационной, финансовой и прочей ценной информации в ходе общения с человеком путем обмана или злоупотребления доверием); метод проникновения в защищённые системы, основанный на использовании индивидуальной психологии
social media	социальные сети
social media marketing	маркетинг в социальных сетях
Social Security Administration	Администрация социального обеспечения (США)
Social Security number	номер социального страхования
socializing	установление социальных контактов
software agent	программный агент
software media	носитель с программным обеспечением
software piracy	программное пиратство, нарушение авторских прав на программное обеспечение
solicit	запрашивать, требовать
solid-state	твердотельный, полупроводниковый
sophisticated	усложненный, тщательно продуманный, высокой сложности; изощренный, сведущий, эрудированный
source coding	кодирование источника
span	охватывать
spare	беречь, избавлять
spatial	пространственный
spear phishing	точечный фишинг, целевой фишинг

specialty	раздел
specification	инструкция, правила, положение, технические условия
spoof	подделывать
spoofing	«спуфинг», имитация соединения (маскировка ложных сайтов под легальный бизнес, чтобы обманным путём получить от посетителей номера кредитных карточек)
spoofing attack	злонамеренные действия нарушителя под видом законного пользователя, спуфинг-атака
sprinkle	небольшое количество
spurious	поддельный, подложный, сфальсифицированный
spyware	программа-шпион
SQL SERVER	SQL-сервер, сервер баз данных
SQL, Structured Query Language	международный стандартный язык для определения и доступа к реляционным базам данных, язык структурированных запросов
stalker	преследователь
stance	мнение, точка зрения, позиция
state of the art	передовой уровень, последние достижения
staying power	долговечность
Steering Group	координационный совет
still image	статическое изображение
storage	память данных, система хранения данных, запоминающее устройство, накопитель
storage architectures	архитектура хранения данных
storage area network	сетевая система хранения данных
stream cipher	поточное шифрование, шифрование потока данных
stringent	жесткий, строгий
stumble	наткнуться, найти
subsidized	дотируемый
subvert	подрывать, нарушать, дестабилизировать
successor	альтернатива, преемник
suite	набор, комплекс
sum	общий итог
summon	судебная повестка, вызов в суд
supervised release	освобождение под надзор
supplement	дополнение
surface	стать явным, проявиться, внезапно появиться
surveillance	слежка, наблюдение, надзор
suspend	приостанавливать, временно исключать из обращения

swap	обмениваться
swap meets	«блошиный рынок», толкучка
symmetric encryption	симметричное шифрование
synch	синхронизировать, быть в курсе
syntax	синтаксическая конструкция, синтаксические правила

T

tackle	бороться
tally	число, перечень
tamper	подделывать, изменять, портить
tap	подключаться, внедряться
tap into	получить доступ и использовать, подключаться
targeted	специализированный, запланированный
task force	оперативная группа, специальная группа, специализированное полицейское подразделение
TCP/IP protocol, Transmission Control Protocol/Internet Protocol	протокол управления передачей/Интернет-протокол
tcpview	Программа для операционных систем Microsoft Windows, которая показывает детальный список всех процессов и Интернет-соединений, а также удалённые адреса, с которыми были установлены соединения
technical execution	техническое выполнение
technicalities	технические детали, техническая сторона дела
technology-gone-wild scenario	сценарий, в котором технологии выходят из-под контроля
telecom networks	телекоммуникационная сеть
teller	операционист
terminate	прекращать действие
think outside the box	нестандартно мыслить
thought	размышление, мыслительная деятельность
thoughtfulness	глубокомыслие, внимательность, вдумчивость
thrive on	успешно пользоваться
throttle up	набирать обороты
thumb drive	флеш-накопитель, карта флеш-памяти
thwart	мешать, препятствовать, предотвращать
time stamp	метка реального времени
timelines	лента сообщений
timely	своевременно, вовремя
token	аппаратный ключ, устройство идентификации, токен, знак

tolerances	устойчивость, чувствительность, допустимый толерантный предел
top secret	совершенно секретно, сведения особой важности
traction	популярность
trade in	отдавать старую вещь в счёт покупки новой
traffic-flow security	защита трафика, секретность потока трафика
transaction	операция, запрос
Transaction Process System	система обработки финансовых операций
transcribe	преобразовывать, воспроизводить
transient	транзиентный, временный, кратковременный
transmission media	передающая среда, среда передачи данных
transmission security	сохранение конфиденциальности информации при её передаче по сетям связи
transposition	перестановка
trick	обмануть
trigger	приводить к, служить причиной возникновения
TripleDES	стандарт трехкратного шифрования данных
Trojan horse	троян
troll	провокатор (на форумах и в чатах); тролль (автор вызывающих и провокационных сообщений)
Trusted Computer System Evaluation Criteria	критерии оценки степени защищённости компьютерных систем
trusted computing	понятие доверенных вычислений
turnaround	цикл обработки, производственный цикл
tweet	сообщение в Твиттере
typeface	гарнитура шрифта

U

UN laissez-passer	дипломатический паспорт ООН
unacceptable	неприемлемый, недопустимый
unbeknownst	без ведома
uncover	обнаруживать
uncovering	выявление, обнаружение
under development	находящийся в процессе разработки
underlying	лежащий в основе
underpin	лечь в основу, поддержать, подкреплять
underpinning	основа, обоснование, подтекст
undesirable	нежелательный, сомнительный
unfairly	несправедливо
unmoderated	нередактированный
unrecognizable	нераспознаваемый
unrestricted	произвольный

unscathed	неповрежденный
unsolicited commercial e-mail	незапрашиваемая рекламная электронная почта, спам
untrustworthy	не заслуживающий доверия
uphill task	трудная задача
uppercase letter	знак верхнего регистра, заглавная буква
URL address	URL-адрес
URL, Uniform Resource Locator	унифицированный локатор ресурса
USB driver	флеш-накопитель
user-friendly	удобный для использования
user-generated content	пользовательский контент, материалы пользователей
utility	полезность, практичность, удобство доступа; нахождение информации в такой форме, что ее законный владелец не должен для получения доступа тратить неоправданные усилия (такие, как преобразование формата, подбор ключа шифрования и т. д.); утилита, обслуживающая программа, сервисная программа
utility system	система инженерного обеспечения

V

validate	признавать законным, проверять достоверность, придавать юридическую силу
validation	подтверждение, доказательство, признание
validity	достоверность, пригодность, точность
variables	переменные факторы, показатели
vault	хранилище
vendor	фирма-поставщик, подрядчик
VeriSign	регистратор доменных имен Верисайн
vetted	подтвержденный, проверенный
viable	эффективный, успешный
vishing	вишинг
vital	крайне необходимый, жизненно важный
VoIP, Voice over IP	передача голоса/речи через Интернет, IP-телефония
volatile	изменяемый, взрывоопасный
vulnerability	слабое звено, уязвимая сторона, уязвимость слабозащищённый объект

W

walk a fine line	балансировать на грани фола, пытаться найти баланс между двумя сторонами

warrant	требовать, обеспечивать; ордер
wary	осторожный, осмотрительный
watch list	список преступников в розыске правоохранительными органами, розыскной список
wean	отучать, отлучать
web crawler	поисковый робот
web wise	компетентный, грамотный
web-enabled	реализованный на основе веб-приложений, с веб-интерфейсом
website defacement	искажение внешнего вида веб-сайта
welfare benefits	пособие по социальному обеспечению
well-versed	хорошо разбирающийся, компетентный
white hat hacker	белый хакер (хакер, использующий свои знания во благо обществу)
wiki	вики (гипертекстовая среда (обычно Веб-сайт) для сбора и структуризации письменных сведений, может иметь множество авторов. Некоторые вики могут править все посетители); редактируемая страница (веб-страница, которую может редактировать любой авторизовавшийся на ней пользователь, от гавайского wiki — быстрый)
wipe	очистить
wire transfer	электронный денежный перевод
with a view to	с намерением, с целью
work queue	очередь заданий, рабочая очередь
work statement	техническое задание
workstation	рабочая станция, рабочее место
World Wide Web	всемирная компьютерная сеть
XML, eXtensible Markup Language	язык XML, расширяемый язык разметки

Z

zero-knowledge proof	доказательство с нулевым раскрытием конфиденциальных сведений

INDEX

LITERATURE

1. Электронный словарь Мультитран [Электронный ресурс]. — URL: http://www.multitran.ru/ (дата обращения: 22.08.2016).
2. Christopher S. Koper, George Mason University (PI), Cynthia Lum, George Mason University (PI), James J. Willis, George Mason University (Co-PI), Daniel J. Woods, Police Executive Research Forum, Julie Hibdon, Southern Illinois University. — Realizing the Potential of Technology in Policing: A Multisite Study of the Social, Organizational, and Behavioral Aspects of Implementing Policing Technologies. — 2015. — 336 p.
3. Hakan HekimPolice Use of Information Technologies in Criminal Investigations. — European Scientific Journal. — February 2013. — vol. 9, No. 4. — p. 221–240
4. Interpol handbook on DNA data exchange and practice: Recommendations from the Interpol DNA monitoring expert group. — 2009. — 118 p.
5. Investigations Involving the Internet and Computer Networks. — Office of Justice Programs/Partnerships for Safer Communities. 2007. — 137 p.
6. James Chu Law Enforcement Information Technology: A Managerial, Operational, and Practitioner Guide. — CRC Press. 2001. —280 p.
7. Janet Chan, David Brereton, Margot Legosz, Sally Doran E-policing: The Impact of Information Technology on Police Practices. — Queensland, 2001. — 153 p.
8. John S. Hollywood, John E. Boon, Jr., Richard Silberglitt, Brian G. Chow, Brian A. Jackson High-Priority Information Technology Needs for Law Enforcement. — RAND Corporation, Santa Monica, Californ. — 2015. — 95 p.
9. Ask [Электронный ресурс]. — URL: http://www.ask.com (дата обращения: 22.08.2016).
10. Computer Glossary [Электронный ресурс]. — URL: http://whatis.techtarget.com (дата обращения: 22.08.2016).
11. Cybersecurity Overview [Электронный ресурс]. — URL: https://www.dhs.gov/cybersecurity-overview (дата обращения: 22.06.2016).
12. Databases [Электронный ресурс]. — URL: https://www.interpol.int/ INTERPOL-expertise/Databases (дата обращения: 22.01.2017).
13. FBI [Электронный ресурс]. — URL: https://www.fbi.gov (дата обращения: 22.04.2016).

14. How Is Computer Technology Used in Law Enforcement? [Электронный ресурс]. — URL: http://techin.oureverydaylife.com/computer-technology-used-law-enforcement-1233.html (дата обращения: 11.04.2016).
15. Kelly J. Harris, Todd G. Shipley InformationTechnology Security: How to Assess Risk and Establish Effective Policies. — 2006. — 197 p.
16. Law EnforcementCyberCenter [Электронный ресурс]. — URL: http://www.iacpcybercenter.org/chiefs/it-security/ (дата обращения: 22.10.2016).
17. Office of Justice Programs [Электронный ресурс]. — URL: www.ojp.usdoj.gov (дата обращения: 12.05.2016).
18. Online Safety Guide [Электронный ресурс]. — URL: http://kids.getnetwise.org (дата обращения: 22.10.2016).
19. Ralph Ioimo Introduction to Criminal Justice Information Systems. — CRC Press. — 2016. — 335 p.
20. South African portal for resources and information on Cybercrime [Электронный ресурс]. — URL: http://cybercrime.org.za/ (дата обращения: 22.10.2016).
21. Techopedia Technology Dictionary [Электронный ресурс]. — URL: https://www.techopedia.com/dictionary (дата обращения: 11.02.2017).
22. The Tech Terms Computer Dictionary [Электронный ресурс]. — URL: http://techterms.com (дата обращения: 12.07.2016).
23. The Police Chief [Электронный ресурс]. — URL: http://www.policechiefmagazine.org/ (дата обращения: 22.10.2016).
24. Webopedia [Электронный ресурс]. — URL: http://www.webopedia.com/TERM/ (дата обращения: 22.10.2016).

NOTES

Учебное издание

Малкова Татьяна Вячеславовна

АНГЛИЙСКИЙ ЯЗЫК

ХРЕСТОМАТИЯ СПЕЦИАЛЬНЫХ ТЕКСТОВ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

Редактор *Мамедова А.Х.*
Компьютерная вёрстка *Фролова А.В.*

Подписано в печать 24.03.2017. Формат 60×84 $^{1}/_{16}$
Печать цифровая. Тираж 100 экз. Объем 9,5 п.л. Заказ № 22/17

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1