Шерстяных А.С.,

кандидат технических наук, доцент
Сибирский юридический институт МВД России (г. Красноярск)

Фишинг как инструмент социальной инженерии

В последнее время приобрел популярность такой вид кибермошенничества, как фишиг. По результатам опроса, проведенного аналитиками антивирусной компании Avast в 2021 г., 45% респондентов столкнулись с фишинговыми атаками[1].

Фишинговая атака – это относящий к методам социальной инженерии вид мошенничества, направленный на получение конфиденциальной информации пользователей (учетные данные для входа на сайт, номер карты, пин-код или CVC/CVV-код, и т.д.).

По мнению экспертов[2], в 2021 г. основными фишиговыми схемами, которые использовали кибермошенники, были:

– имитация внутрикорпоративной деловой переписки (опрос от имени кадровой службы о прохождении вакцинации, извещения от руководства об изменениях графика выплаты заработной планы или размера премии и пр.);

– поддельные письма от банков об изменении тарифов и цен за банковское обслуживание, обещание выплат пострадавшим от мошенничества, предложение выигрыша при прохождении опроса и т.д.;

– мошеннические сайты, идентичные сайту госуслуг, на которые заманивали рассылками о полагающихся выплатах, сообщениями об откреплении от поликлиники, генерацией «липового» qr-кода о вакцинации и т.п.;

– рассылка от стриминговых сервисов о выходах новых фильмов и сериалов (цель – завладеть учетными данными аккаунта либо предложить оформить/продлить подписку);

– предложения просмотра спортивных репортажей Олимпийских игр в Пекине (эксперты Group-IB уже выявлено более 140 фишинговых сайтов)[3];

– сообщения от службы доставки (проверить статус посылки, оплата пошлины или ячейки хранения);

– предложения забронировать билеты на концерты или спектакли, авиа- или железнодорожные билеты, а также номер в отеле, привлекая пользователей воспользоваться фиктивными акциями и скидками (например, министерство торговли Турции[4] сообщило о фейковых сайтах гостиниц и рекомендовало выяснить, зарегистрирован ли сайт в системе электронной торговли ETBIS);

– рассылки от имени известных брендов или компаний, сулящие денежные призы или скидку на следующую покупку за прохождение опроса на сайте, в конце которого жертве предлагается перечислить небольшую комиссию для получения приза. При этом мошенники для получения награды за опрос стали требовать разослать свое сообщение определенному количеству друзей или знакомых, справедливо полагая, что рекламе, присланной конкретным человеком, люди доверять будут больше.

Весьма популярна стала тема инвестиций – банки ежедневно предлагают клиентам инвестиционные и брокерские счета. Кибермошенники также не

[1] Avast: 45% россиян столкнулись с фишингом в 2021 году // Avast : сайт. URL: https://blog.avast.com/ru/pochti-polovina-rossiyan-stalkivalas-s-fishingovymi-atakami (дата обращения: 10.01.2022).

[2] 10 популярных «фишинговых» тем в 2021 году по версии Positive Technologies // Positive Technologies : сайт. URL: https://www.ptsecurity.com/ru-ru/research/analytics/10-populyarnyh-fishingovyh-tem-v-2021-godu-po-versii-positive-technologies/ (дата обращения: 10.01.2022).

[3] Мошенники начали обманывать россиян на теме Олимпиады // ruposters : новостной сайт. URL: https://ruposters.ru/news/10-02-2022/moshenniki-nachali-obmanivat-olimpiadi (дата обращения: 12.01.2022).

[4] Правила съема: Турция предупредила о мошенничестве с отелями // Известия : новостной сайт. URL: https://iz.ru/1183155/mariia-nemtceva/pravila-sema-turtciia-predupredila-o-moshennichestve-s-oteliami (дата обращения: 18.01.2022).

обошли вниманием этот способ, по выражению Остапа Бендера, «сравнительно честного отъема денег». Для привлечения «клиентов» они используют имена известных и успешных бизнесменов или названия крупных бизнес-компаний. Например, в мае прошлого года они от имени Илона Маска[1] предлагали удвоить переведенную на счет сумму в криптовалюте Dogecoin. В итоге на счете мошенников оказалось около 9,7 млн единиц Dogecoin, общая стоимость которых составила 5 млн долларов.

В новостях появились сообщения о деятельности мошенников, которые под видом брокеров или от имени крупных банков предлагают потенциальным жертвам открыть и пополнить инвестиционный счет. Для привлечения внимания чаще всего злоумышленник используют один из трех базовых сюжетов (на просторах Интернета можно встретить и другие, но в конце 2021 г. чаще всего встречались именно эти)[2]:

– альтернатива банкам (мошенники рекламируют «совершенно новую инвестиционную технологию», с помощью которой пользователи смогут получить значительный доход);

– «недра – народу». На сайте размещена реклама несуществующих национальных проектов, в которых предлагается поучаствовать населению с гарантированным получением сверхдоходов от торговли нефтью и газом. Для придания «достоверности» излагаемой информации в рекламу включены фрагменты новостных сюжетов с участием первых лиц страны, но фальсифицированной озвучкой и наложенными субтитрами;

– финансы для людей. Для этого они создают сайты, имитирующие деятельность инвестиционных платформ, на которых жертве предлагается внести определенную сумму, чтобы якобы начать торги, либо рассылают от имени крупных банков предложения поучаствовать в инвестиционных проектах. Для этого злоумышленники предлагают заполнить анкету и, конечно же, сообщить данные банковской карты для проверки счета (включая CVC/CVV-код с обратной стороны карты).

Затем жертве предлагается либо скачать поддельное мобильное приложение, либо перейти на сайт, где злоумышленники постараются выманить персональные данные. Специалисты из Group-IB571 сообщают, что в ходе исследования, посвященному фишинговым мошенничествам, были выявлены более 8000 доменов, являющихся мошенническими инвестиционными проектами. Всех пользователей, заинтересовавшихся подобными «привлекательными» инвестиционными проектами, как правило, ждет один и то же финал: не только ничего не приобрести, но и потерять свои сбережения.

Компании и банки стараются бороться с действиями злоумышленников. Например, многие в Интернете видели предложение заработать на акциях Газпрома[3]. На официальном сайте компании «Газпромнефть» опубликованы опровержения и описаны мошеннические схемы. Также приведены признаки, которые помогут пользователям распознать мошенников. В Тинькофф-журнале[4] опубликована схема мошенничества якобы от имени Тинькофф-инвестиций.

В ноябре 2021 г. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации заключило контракт с IT-компанией «Рубитех» для создания единой информационной системы мониторинга фи-

[1] Поддельный стрим: как мошенники используют имя Илона Маска // газета.ru : новостной сайт. URL: https://www.gazeta.ru/tech/2021/05/12/13589642/ musk_snl_scam.shtml (дата обращения: 10.02.2022).

[2] Набрали кредитов и вложили последние деньги: как работает мошенническая схема с инвестициями в акции и криптовалюты // Хабр (habr.com) : сайт // URL: https://habr.com/ru/company/group-ib/blog/649977/ (дата обращения: 10.02.2022).

[3] Предупреждение о мошеннических действиях // Официальный сайт компании «Газпромнефть» : сайт. URL: https://www.gazprom-neft.ru/company/contacts/feedback/ warning (дата обращения: 02.02.2022).

[4] Мошенники прикидываются известными брокерами, чтобы украсть ваши деньги // Тинькофф-журнал : сайт. URL: https://journal.tinkoff.ru/hustle/fake-invest/ (дата обращения: 10.02.2022).

шинговых сайтов[1]. По условиям контракта компании необходимо провести комплексное исследование, включающее в себя: анализ нормативно-правовой базы противодействия фишинговым атакам (и подготовить предложения по ее совершенствованию); изучение способов мошеннических действий на основе фишинга и методов их обнаружения. Указанная система должна заработать к 1 июня 2022 г.

Щеглова Н.Н.

Владивостокский филиал Дальневосточного юридического института МВД России

Использование признаков внешности человека в раскрытии и расследовании преступлений

Рассматриваемое криминалистическое учение заняло надлежащее место в числе частных криминалистических теорий. Содержащиеся в нем выводы и рекомендации служат своеобразной методологической основой для разработки тактических положений производства ряда следственных действий, иных процессуальных действий поисково-познавательного характера, а кроме того, следственных мероприятий, используемых в розыскной деятельности субъекта, осуществляющего предварительное расследование.

К числу современных перспективных разработок в сфере криминалистической габитоскопии относится идентификация человека по рисунку радужной оболочки глаза, по рисунку сетчатки глаза, по форме ушной раковины. Наряду с традиционными методами исследования растет востребованность биометрических технологий идентификации личности по этим характерным признакам.

Биометрика – сфера знаний, которая используется при создании автоматизированных систем распознавания человека по его физическим и физиологическим характеристикам – форме кисти руки, термограмме лица (схеме кровеносных сосудов), голосу, подписи, узору радужной оболочки глаза, папиллярному узору пальца, фрагментам генетического кода.

По мнению Р.В. Бондаренко, «современные способы фиксации криминалистической важной информации с использованием видеокамер, видеорегистраторов и смартфонов значительно расширяют имеющиеся возможности для применения и развития биометрических технологий»[2].

В современной криминалистической литературе также аргументируется целесообразность комплексного исследования не только характеристик внешнего облика, но и внутренних признаков человека с целью идентификации его личности.

Дискуссионным является вопрос о соотношении криминалистической габитоскопии и криминалистической физиогномики. Существует точка зрения о рациональности применения анализа внешнего облика человека при решении диагностических вопросов, связанных со свойствами личности, ее темпераментом, способностями, предпочтениями и психологической совместимостью[3].

[1] В России к 1 июня 2022 года должна быть создана система мониторинга фишинговых сайтов – Минцифры определило подрядчика // D-russia.ru : сайт. URL: https://d-russia.ru/v-rossii-k-1-ijunja-2022-goda-dolzhna-byt-sozdana-sistema-monitoringa-fishingovyh-sajtov-mincifry-opredelilo-podrjadchika.html (дата обращения: 18.02.2022).

[2] Бондаренко Р.В. Перспективы развития криминалистического учения о признаках внешности человека // Вестник Московского университета МВД России. 2018. № 12. С. 59.

[3] Зинин А.М., Подволоцкий И.Н. Судебная портретная экспертиза // Судебная экспертиза в цивилистических процессах / под ред. Е.Р. Россинской. М., 2018. С. 114.