мые, совершают тяжкие насильственные преступления»[4].

[1] В основу исследований положены материалы 311 уголовных дел об истязании, рассмотренных судами Российской Федерации (Архангельская, Астраханская, Омская и Свердловская области, Республика Бурятия) в 2007-2015 гг.

[2] Были опрошены 68 участковых уполномоченных полиции в г. Омске и Омской области.

[3] Средний возраст участковых уполномоченных полиции в г. Омске составил 32 года, средний стаж работы по специальности – 5,6 лет. При этом стаж работы по специальности до 5 лет имеют 45,1% участковых, от 5 до 10 лет – 40,4%, от 10 лет и выше – 14,5%.

[4] Чечель Г.И. Жестокий способ совершения преступлений против личности: уголовно-правовое и криминологическое исследование. Нальчик : Ставропольское книжное издательство, 1991. С. 153.

Шерстяных А.С.,

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

Методы социальной инженерии, используемые при совершении преступлений в сети Интернет

В 2016 г. Указом Президента была утверждена Доктрина информационной безопасности Российской Федерации, в которой одной из основных информационных угроз признано «увеличение масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, а также числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий»[1].

С каждым годом Интернет становится все более необходимым элементом повседневной жизни обычного человека. На это не могут не отреагировать всевозможные мошенники, стремящиеся улучшить свое материальное положение за счет доверчивых граждан. Количество преступлений, совершенных с использованием интернет-технологий, увеличивается во всем мире и в России в частности. Например, в 2016 г. конфиденциальные сведения 3 миллиардов аккаунтов Yahoo были украдены злоумышленниками. Эта утечка персональных данных до сих пор считается одной из самых масштабных и резонансных. В 2017 г. данные 412 миллионов пользователей «взрослого» сервиса FriendFinder были похищены в результате хакерской атаки.

В России в последние годы количество преступлений, совершенных с использованием компьютерных технологий, неуклонно растет: в 2013 г. таких преступлений было зарегистрировано 11 тысяч, в 2014 г. – 44 тысячи, а в 2017 г. – уже 90 тысяч.

По сведениям, опубликованным Генеральной прокуратурой Российской Федерации, за январь-сентябрь 2018 г. были зарегистрированы 121 247 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, или в сфере компьютерной информации, что на 33% больше, чем за весь 2017 г. При этом доля таких преступлений в общем количестве зарегистрированных за девять месяцев 2018 г. преступлений составляет 8,1% (против 4,4% в 2017 г.).[2] Причем реальное количество таких преступлений гораздо больше. Например, когда злоумышленники воруют какой-нибудь «навороченный» объект в популярной сетевой игре или похищают логины или пароли от кошельков с криптовалютой, пострадавшие не всегда заявляют в полицию о совершенном преступлении и, следовательно, по ним не возбуждаются уголовные дела.

Жертвами кибермошенников являются как различные кампании, так и

обычные пользователи Интернета, причем последних гораздо больше, поскольку рядовые пользователи, в отличие от сотрудников службы информационной безопасности крупных компаний, не знакомы с методами социальной инженерии и не могут им достойно противостоять.

Одним из самых распространенных методов мошенничества является фишинг (англ. phishing, от fishing – рыбная ловля, выуживание и password – пароль) – вид интернет-мошенничества, целью которого является получение различных идентификационных данных пользователей (логинов, паролей, номеров кредитных карт и пр.). Техника фишинга заключается в следующем: пользователю отправляют ссылку на якобы официальную страницу какого-либо ресурса, причем ссылка будет выглядеть очень правдоподобно и, на первый взгляд, узнаваема пользователем. Только в адресе может быть одна или несколько лишних букв. Перейдя по этой ссылке, пользователь попадет не на оригинальный сайт, а на очень похожий сайт мошенников, на котором его попросят ввести конфиденциальную информацию, после чего перенаправят на подлинный сайт организации.

Иногда злоумышленники могут прикрываться не известной пользователю компанией, а рекламировать свою. Например, в 2018 г. появились несколько тождественных друг другу сайтов «Активный гражданин». На этих сайтах пользователям предлагалось поучаствовать в некотором опросе, естественно, не безвозмездно: участникам было обещано вознаграждение в размере 65 тысяч рублей. После прохождения опроса пользователям предлагалось создать новый аккаунт, с помощью которого они смогут получить обещанные деньги, заплатив за активацию 170 рублей. Понятно, что никто из них обещанных денег не получил.

Часто злоумышленники играют на таких чувствах жертвы, как желание заработать, выполняя небольшую и несложную работу либо обеспокоенность за свои сбережения (прикидываясь сотрудниками банка).

Рассмотрим наиболее часто встречающие примы социальной инженерии, используемые злоумышленниками, чтобы привлечь потенциальную жертву:

– организация рассылок электронных писем о выигрыше различных денежных или ценных призов, при этом для получения выигрыша нужно заплатить небольшую сумму, мотивируя это требование транспортными издержками или налоговой ставкой;

– рассылка рекламной информации о достаточно низких ценах в несуществующем интернет-магазине, однако при заказе требуется небольшая предоплата (для того, чтобы обмануть как можно большее количество клиентов, через непродолжительное время интернет-ресурс закрывается и открывается новый);

– создание поддельных сайтов по продаже авиабилетов онлайн, при этом обман выясняется только при посадке на самолет;

– фишинговые рассылки от имени банка о том, что обнаружены подозрительные или мошеннические действия пользователя с вашими учетными данными, и служба безопасности банка рекомендует незамедлительно войти в свой аккаунт и обновить конфиденциальную информацию (такая тактика может быть эффективной, поскольку большинство пользователей переживает за сохранность своих денежных средств, что заставляет их перейти по ссылке и ввести учетные данные);

– с приходом облачных технологий в повседневную жизнь, мошенники начали охотиться за учетными данными для входа в облачные хранилища данных, поскольку на таких сервисах многие хранят различную конфиденциальную информацию (например, резервные копии служебной информации, личные фотографии и видео, логины и пароли к другим интернет-сервисам).

Способы защиты от подобного рода мошенничества достаточно просты и в целом представляют собой одну рекомендацию – будьте бдительны:

– внимательно проверьте URL-адрес, который содержится в письме, на

правильность написания (вас должны насторожить незначительные отличия);

– старайтесь всегда использовать только безопасные https-соединения (URL-адрес без буквы s не гарантирует вам безопасности, скорее наоборот, вам предлагают вводить персональные данные, не защитив передачу данных);

– при получении писем с различными вложенными файлами или ссылками для немедленного перехода рекомендуется связаться с отправителем и подтвердить у него отправку полученного письма);

– для работы с онлайн-банком не рекомендуется использовать открытые Wi-Fi сети (поскольку подключиться к незащищенному соединению для злоумышленников не составит труда);

– старайтесь чаще менять учетные данные от различных сервисов, особенно тех, к которым привязаны кредитные или банковские карты;

– при переводе денег на благотворительность не поленитесь найти в Интернете информацию о фонде или личности, которым хотите перевести пожертвование;

– должны настораживать просьбы о переводе небольшой суммы денег для оформления или получения крупного выигрыша;

– никогда не переводите денег на незнакомые номера телефонов и не перезванивайте по сомнительным номерам, с которых приходят смс от «банков», «страховых компаний» или от лица близкого человека.

При этом всегда имейте в виду, что злоумышленники постараются ввести вас в состояние стресса, в котором вам будет весьма сложно принять объективное и продуманное решение. В случае, если вы чувствуете с их стороны прессинг, старайтесь не совершать поспешных действий, а отложите его на некоторое время.

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646.

[2] Генпрокуратура сообщила почти о двукратном росте числа киберпреступлений в Российской Федерации в 2018 году // ТАСС. URL: https://tass.ru/proisshestviya/5733551 (дата обращения: 17.01.2019).

Пальчик М.В.

Сибирский юридический институт МВД России (г. Красноярск)

Криминологическая характеристика присвоения или растраты

Согласно общепризнанной в криминологии классификации[1] преступление, предусмотренное ст. 160 УК РФ относится к такому виду преступности, как корыстная. Следует при этом отметить, что все корыстные преступления по характеру преступного поведения дифференцированы на корыстно-насильственные и на собственно корыстные преступления. Не вызывает сомнения с учетом способов хищения, предусмотренных ст. 160 УК РФ, что присвоение и растрата являются разновидностью последних.

В рамках криминологической характеристики любого вида преступности всегда в первую очередь актуальны ее количественно-качественные показатели. Что касается состояния присвоения или растраты, то, по данным ГИАЦ МВД России, количество зарегистрированных заявлений по факту совершения этих преступлений сокращается: 2010 г. – 44 894 преступлений, 2011 г. – 34 256, 2012 г. – 30 651, 2013 г. – 28 049, 2014 г. – 20 526, 2015 г. – 19 494, 2016 г. – 17 633, 2017 г. – 13 419, 11 месяцев 2018 г. – 14 539 преступлений.[2] На региональном уровне фактически находят отражение общероссийские тенденции. Так, в г. Красноярске и Красноярском крае, по сведениям ИЦ ГУ МВД России по Красноярскому краю, количество зарегистрированных заявлений по факту присвоения или