УДК 343.13

И. О. Проваторов
преподаватель кафедры административной деятельности и охраны общественного порядка Волгоградской академии МВД России

ОТДЕЛЬНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-САЙТОВ

В настоящее время электронные информационные системы, социальные сети, технологии беспроводного доступа в сеть Интернет и средства мобильной связи стали неотъемлемыми составляющими повседневной жизни граждан Российской Федерации, при этом процесс цифровизации современного общества продолжает постоянно развиваться: посредством электронной почты пересылаются копии документов, удостоверяющих личность; на сервисы платежных систем направляются реквизиты банковских карт; в социальных сетях размещается информация о личной жизни и иная конфиденциальная информация.

Данные обстоятельства сопровождаются технологическим развитием не только общества в целом, но и различных мошеннических схем, используемых субъектами преступлений в интернет-пространстве для совершения своих противоправных действий.

По статистическим данным, в 2021 году в России зарегистрировано около 518 тыс. киберпреступлений, что на 1,4 % больше, чем годом ранее, но сразу в 1,8 раза превосходит показатель 2019 года. В частности, количество заявлений о мошенничестве (хищение с обманом жертвы) выросло на 5,1 %, превысив 249 тыс. [1].

Отдельной группой мошенничеств можно выделить мошенничества, совершаемые с использованием интернет-сайтов.

Виды подобных мошенничеств разнообразны, самыми распространенными и популярными являются следующие:

1. Фишинг — мошеннические действия, направленные на хищение идентификационных данных (Ф. И. О., пароля и номера банковской карты, реквизитов, переписки, служебной информации и т. д.). Злоумышленники пользуются невнимательностью граждан и завладевают конфиденциальной информацией путем создания сайтов-клонов, фальшивых аккаунтов в мессенджерах и социальных сетях, электронной рассылки писем. Мошенники выдают себя за надежный источник в сети, вынуждая жертву передать им личные данные. В данной ситуации преступниками используется «фишинговый сайт — ресурс, похожий на доверенный источник, например страницу популярной компании или платежной системы» [2].

Нередко мошенниками применяются «фишинговые атаки» по электронной почте, когда преступником организуется рассылка писем с сообщением о выигранном призе или о блокировке счета. Мошенники предлагают победителю перевести определенную сумму для получения крупного выигрыша или внести оплату для разблокировки карты, для чего потерпевший сообщает свои персональные данные.

2. Кардинг — тип интернет-преступлений, при котором мошенники обманным путем совершают кражу конфиденциальной информации о пользователях и снимают деньги со счетов граждан без их ведома. Самым распространенным способом получения доступа к данным банковских карт выступает взлом серверов интернет-магазинов, расчетных и платежных систем. Хакеры используют программы удаленного доступа и вредоносное программное обеспечение для получения персональной информации о человеке и данных о платежной карте.

3. Двойники интернет-магазинов — мошеннические действия злоумышленников заключаются в создании сайта, похожего на официальный интернет-магазин с лаконичным и стильным дизайном, аккуратными карточками товаров, без баннеров и кричащей рекламы. Данные сайты отличаются дешевыми ценами на товары и скидочными предложениями за полцены и призваны завлечь ничего не подозревающих онлайн-покупателей. Через поисковые системы пользователи переходят по ссылке, проходят регистрацию и вводят информацию о своем банковском счете для завершения покупки. В итоге продавец-мошенник получает оплату и пропадает с денежными средствами, поступившими за оплату товара, или присылает совершенно иной товар.

Гражданам, использующим интернет-сайт для приобретения какого-либо товара, рекомендуется в подобной ситуации проверять адресную строку в браузере, которая должна начинаться с https (безопасный протокол передачи данных). Это означает, что ресурс имеет защищенное (шифрованное) соединение, хотя и не гарантирует полной безопасности.

4. Копии сервисов интернет-банкинга — мошеннические действия злоумышленников направлены на создание сайтов-клонов банков. Преступники направляют потерпевшему электронное письмо или СМС-сообщение, в котором приглашают пользователя пройти авторизацию. Введенные в заблуждение о подлинности сайта граждане регистрируются в личном кабинете, предоставляя свои персональные данные, и переходят на фальшивый сайт, создавая тем самым возможность мошенникам получить доступ к банковским счетам и завладеть денежными средствами.

5. Взлом аккаунтов и рассылка от друзей — тип мошенничества, когда преступники отправляют СМС-сообщения на почту или в социальные сети

родственникам и знакомым владельца страницы после ее взлома с просьбой срочно перевести деньги, придумывая различные ситуации.

6. Фальшивые сайты благотворительности, туроператоров или авиакомпаний.

7. Предложения выгодного заработка — в указанной ситуации мошенники предлагают удаленную работу, но предварительно требуют оплатить организационные нужды. После того как потерпевший переводит денежные средства, выдуманная организация пропадает с похищенным имуществом.

8. Размещение объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах — тип мошеннических действий, направленный на привлечение своих жертв заниженными ценами и выгодными предложениями, при этом преступники с целью похищения денежных средств требуют от потерпевшего перечисления предоплаты путем перевода денежных средств на электронный кошелек.

9. Вирусы на сайте — принцип действия мошенников основан на внедрении шпионских программ, например, внедряют кейлоггеры, которые представляют собой «любой компонент программного обеспечения или оборудования, который умеет перехватывать и записывать все манипуляции с клавиатурой компьютера» [3].

Кейлоггер либо хранит перехваченную информацию на зараженном компьютере, либо, если является частью более крупной атаки, передает все данные сразу на удаленный компьютер организаторов атаки.

10. Сторонний контент. SSL-сертификат представляет собой «цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение» [4]. Если такого сертификата нет, то на сайт можно внедрить сторонний контент — рекламу, виджеты. Добавленный контент может содержать вирусы, с помощью которых злоумышленники проникнут на устройство пользователя и смогут похитить его персональные данные.

Предполагаем, что представленный нами перечень мошенничеств, совершаемых с использованием интернет-сайтов, не является исчерпывающим, так как преступники на современном этапе технологического развития быстрыми темпами совершенствуют алгоритмы и схемы преступных действий, придумывая новые и более сложные способы обмана граждан, в связи с чем проблема раскрытия и расследования сотрудниками правоохранительных органов подобных преступлений продолжает оставаться весьма актуальной.

Прежде всего, интернет-сайт представляет собой «совокупность страниц, в основном объединенных общей темой, которые принадлежат одной компании или владельцу» [5]. Данный ресурс оформляется в одной тематике, размещается по уникальному сетевому адресу (домену) и в восприятии пользователей сети Интернет представляется как единое целое. Страницы веб-ресурса являются до-

кументами текстового формата, кроме текстов на сайте могут размещаться изображения, звуковые и видеофайлы.

Существуют различные типы сайтов, такие как: визитка, квест, просайт, интернет-магазин, каталог товаров, корпоративный ресурс.

Однако работоспособность любого интернет-сайта включает в себя регистрацию доменного имени и аренду хостинга, зная данные особенности, сотрудник правоохранительных органов может получить значимую информацию для раскрытия и расследования преступлений подобной категории.

Сайты размещаются по одному адресу и имеют одно доменное имя. Но случается, что несколько ресурсов могут иметь общий домен или один ресурс можно разместить по нескольким адресам. Местом хранения любого сайта выступает веб-сервер (системный блок большого размера).

Виртуальный хостинг — это услуга по размещению сайта в Интернете, так как интернет-сайт должен иметь свое место для хранения на физическом носителе. Для хранения информации используется специальное оборудование — серверы, подключенные круглосуточно к сети Интернет. Аренда хостинга представляет аренду части пространства на данном сервере и для того, чтобы арендовать хостинг, необходимо составить соответствующий договор и оплатить предоставляемые услуги.

Сотрудник правоохранительных органов может направить запрос лицу, организующему аренду хостинга, и установить: данные о лице, арендовавшем хостинг, какие банковские карты и счета для оплаты аренды им используются, IP-адреса, электронные почты, абонентские номера и т. д.

Доменное имя — это «легко запоминающееся название сайта, связанное с определенным IP-адресом в Интернете. Оно указывается в адресе сайта после “www” и в адресе электронной почты после символа “@”. Приобрести доменное имя может любой желающий. Для этого необходимо перейти на сайт регистратора доменов, выбрать свободное имя и ежегодно платить небольшой взнос за его использование» [6].

Направив запрос в адрес регистратора доменного имени, сотрудник правоохранительных органов может получить информацию, аналогичную информации, предоставляемой хостинг-арендодателем.

В связи с тем, что существует огромное множество организаций-арендодателей хостинга и организаций-регистраторов, сотрудник правоохранительных органов при подготовке подобного запроса может использовать интернет-ресурс www.reg.ru. При этом необходимо зайти на указанный сайт, ввести доменное имя сайта, сведения о котором нужно установить, и нажать кнопку Whois, после чего на сайте будет представлена информация об организации, где зарегистрировано доменное имя. Указанному юридическому

лицу следует направлять соответствующий запрос. С помощью данного интернет-ресурса также устанавливаются сведения организации, предоставляющей хостинг для сайта. Полученные сведения могут быть представлены в виде справки, приобщены сотрудником правоохранительных органов к материалам уголовного дела либо материалам процессуальной проверки и играть доказательственное значение при раскрытии и расследовании мошенничеств, совершенных с использованием интернет-сайта.

---

1. Число киберпреступлений в России [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 03.04.2022). Перейти к источнику Вернуться к статье

2. Как определить мошеннический сайт [Электронный ресурс]. URL: https://www.nic.ru/info/blog/scammer/ (дата обращения: 03.04.2022). Перейти к источнику Вернуться к статье

3. Что такое кейлоггеры [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/chto-takoe-keylogger/700/ (дата обращения: 01.04.2022). Перейти к источнику Вернуться к статье

4. Что такое SSL-сертификат и определение и описание [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-a-ssl-certificate (дата обращения: 01.04.2022). Перейти к источнику Вернуться к статье

5. Интернет-сайт [Электронный ресурс]. URL: https://blog.ingate.ru/seo-wikipedia/internet-site/ (дата обращения: 03.04.2022). Перейти к источнику Вернуться к статье

6. Основные сведения о доменных именах [Электронный ресурс]. URL: https://support.google.com/a/answer/2573637?hl=ru (дата обращения: 02.04.2022). Перейти к источнику Вернуться к статье