DOI 10.37539/2949-1991.2024.22.11.016
УДК 343.8

Селезнёва Елена Викторовна,
к.п.н., доцент СибАДИ, г. Омск
Selezneva E.V., Ph.D., Associate Professor of SibADI

Соловьев Анатолий Алексеевич,
профессор СибАДИ, г. Омск
Soloviev A.A. – Professor of SibADI

Филимонова Ольга Алексеевна,
ст.преподаватель СибАДИ, г. Омск
Filimonova O.A. – senior lecturer of SibADI

Бисембаева Зарина Нурболовна,
студент СибАДИ, г. Омск
Bisembaeva Z.N. – student of SibADI

ПРОТИВОДЕЙСТВИЕ ТЕЛЕФОННЫМ МОШЕННИКАМ
OF COUNTERING TELEPHONE SCAMS

Аннотация: Сегодня фактически каждое второе имущественное преступление совершается с использованием сети Интернет и телекоммуникационных технологий. Злоумышленники идут на все и постоянно совершенствуют методы обмана. Потери омичей от действий телефонных мошенников за 2024 год превышает 1 миллиард рублей. Главным методом борьбы с дистанционным обманом по-прежнему остается профилактика.

Abstract: Today, virtually every second property crime is committed using the Internet and telecommunications technologies. Attackers go to great lengths and constantly improve their methods of deception. Criminals have already written their own criminal scenarios for each audience. The losses of Omsk residents from the actions of telephone scammers in 2024 exceed 1 billion rubles. Prevention is still the main method of combating remote deception.

Ключевые слова: Интернет, злоумышленники, телефонные мошенники, обман.

Keyword: The Internet, attackers, telephone scammers, deception.

Ежедневно полицейские сводки переполнены сообщениями людях, которые лишились своих сбережений. Мошеннические кол-центры за несколько лет стали криминальной индустрией, в которой «трудятся» сотни тысячи людей. Преступники научились похищать миллионы рублей, используя мобильный телефон, вредоносное программное обеспечение и чью-то доверчивость. *Сегодня фактически каждое второе имущественное преступление совершается с использованием сети Интернет и телекоммуникационных технологий.* Схемы обмана самые разные: потерпевшие переводят миллионы рублей на несуществующие «безопасные счета», делятся с мошенниками кодами для подтверждения переадресации звонков и SMS, верят на слово псевдосотрудникам банков или правоохранительных органов. В первые десять месяцев 2024 года мошенники чаще всего пользовались тремя схемами: притворялись сотрудниками «Госуслуг», работниками Омскводоканала или лжепокупателями с сервисов объявлений. Они обманом заставляли жертву установить программы для доступа к счетам

Для каждой аудитории у преступников уже написаны свои криминальные сценарии: пенсионерам звонят под видом энергокомпаний и сотрудников Пенсионного фонда, молодым

женщинам присылают в мессенджерах ссылки на фишинговые страницы с узнаваемым дизайном косметики. Главным методом борьбы с дистанционным обманом по-прежнему остается профилактика. Ведомством также налажен оперативный обмен информацией с банками, микрофинсовыми организациями, пресекаются факты незаконной реализации sim-карт, блокируются абонентские номера, которые аферисты использовали для обмана. Чтобы поставить заслон кибератакам, правоохранительными органами проводятся мероприятия по выявлению на территории Омской области нелегальных GSM-шлюзов, которые позволяют преобразовывать междугородние звонки во внутрисетевые, что значительно снижает расходы на международные телефонные. Снизить количество кибератак поможет законодательный запрет использования виртуальных номеров и виртуальных АТС, обязательную идентификацию покупателей телекоммуникационного оборудования, принятие мер по ужесточению продажи SIM-карт. Сравнительно новым направлением в борьбе с мошенничеством в полиции назвали и показательные уголовные дела в отношении дропов – людей, которые сознательно или случайно предоставляет свои банковские реквизиты мошенникам для проведения банковских операций в интересах преступников. Рассмотрим основные приемы мошенников и как с этим бороться. У многих людей дома есть возможность подключаться к беспроводному интернету и иметь возможность потреблять огромное количество трафика. Но постоянно включенный Wi-Fi на смартфоне имеет ряд существенных недостатков. Основная причина, по которой стоит переключаться на мобильный интернет в общественных местах, – это безопасность данных. Когда Wi-Fi включен, то телефон автоматически ищет доступные сети для подключения. Как правило, вам необходимо вбить пароль и логин. Но если вы ранее подключались к какой-либо сети, гаджет автоматически соединяется с ней, когда вы снова входите в зону ее действия. Если у этой сети нет высокого уровня безопасности, вы становитесь легкой целью перехвата данных, которые передаются между вашим смартфоном и общедоступной точкой доступа. Личные данные, данные банковских карт и доступ к основным сервисам могут попасть к хакерам, что может привести не только к слежке за вашей активностью в сети, но и финансовым потерям. Второй момент: включенный поиск Wi-Fi дополнительно расходует заряд батареи. Так что при отключении поиска ваше устройство будет работать быстрее и эффективнее. Существуют способы снизить риски, связанные с Wi-Fi на вашем гаджете. Первый – отключать Wi-Fi, когда выходите из дома. Для этого достаточно зайти в настройки смартфона и выбрать параметры сети. Также вы можете отключить эту функцию прямо из меню, раскрыв панель быстрого доступа. Второй вариант – постоянно очищать список сохраненных сетей Wi-Fi, к которым вы подключались ранее. Это следует делать систематически, когда вам больше не нужно пользоваться общедоступной сетью. Также в настройках можно изменить правила использования общедоступных сетей, чтобы они автоматически «забывались». Кроме того, следует отключать Bluetooth и VPN, когда они не требуются, поскольку они также влияют на безопасность, снижают время автономной работы, а VPN еще и снижает скорость мобильного интернета. Согласно статистике, 85% хищений средств приходятся на социальную инженерию. Банки совершенствуют системы противодействия мошенникам, которые позволяет моментально отвязать все устройства с доступом к мобильному приложению. После сброса сессий доступ злоумышленникам будет заблокирован. Если мошенники получают доступ к личному кабинету клиента в онлайн-банке, то они могут, либо попытаться как можно быстрее вывести все средства, либо длительное время наблюдать за движением средств на счетах потенциальной жертвы, чтобы, например, дождаться поступления крупной суммы.

Поэтому важно не только оперативно реагировать на подозрительные ситуации, но и предпринимать профилактические меры и периодически проверять, какие устройства подключены к онлайн-банку. Технология работает следующим образом: клиент звонит в

контакт-центр или обращается в отделение для ограничения доступа к личному кабинету. В этом случае у него будет на выбор две опции: «Заблокировать» или «Отвязать все устройства». Опция «Отвязать все устройства» позволит завершить все сессии в личном кабинете, начатые на разных устройствах. При этом не нужно посещать офис или банкомат, а повторный вход онлайн займет не более минуты. В то же время, если клиент предпочтет заблокировать доступ, он может сделать это с последующей разблокировкой в отделении или через банкомат. При звонке в контакт-центр можно активировать опцию с помощью бота или при поддержке оператора в среднем менее чем за 1 минуту. Не всегда пользователи могут оперативно обратиться в отделение или воспользоваться банкоматом. Новая функция может пригодиться клиенту в любой точке мира – звонок в поддержку доступен круглосуточно. Другой способ обмана, когда злоумышленники от имени сотрудников пенсионного фонда обзванивают людей и узнают пароль из СМС для входа в личный кабинет на портале госуслуг. Получив к нему доступ, мошенники могут оформлять кредиты на сайтах для микрозаймов. Жертвами чаще выбирают людей старшего поколения, но жулики могут позвонить любому гражданину. По сути, схема не является совсем новой: мошенники и раньше пытались под тем или иным предлогом получить доступ к личным кабинетам граждан на сайте госуслуг. Сейчас просто легенда изменилась. Злоумышленники действуют так: они звонят по телефону человеку и сообщают о необходимости скорректировать начисление пенсии. Якобы в данных нашли ошибку и ее нужно исправить. Жертве предлагают приехать в центральный офис пенсионного фонда, предварительно записавшись на конкретную дату и время. Для записи рекомендуют использовать портал «Госуслуги». Мошенники инициируют вход на портал, человеку в этот момент приходит СМС для подтверждения доступа. Если человек называет цифры из сообщения, злоумышленники получают доступ к его личному кабинету. Получив доступ, мошенники, действуя от имени жертвы, регистрируются на сайтах микрофинансовых организаций, используя функцию «Войти с помощью госуслуг». Они оформляют кредит и быстро обналичивают полученные деньги. Жертве остаются долговые обязательства с огромными процентными ставками. Кроме того, персональные данные из личного кабинета госуслуг пострадавшего могут использоваться в других схемах мошенничества. Антифрод-система Сбера зафиксировала рост мошеннической активности по данной схеме. Сбер автоматически выявляет и пресекает операции по ней, однако люди должны знать об опасности и сохранять бдительность. Нельзя сообщать код подтверждения доступа из СМС неизвестным лицам, кем бы они ни представлялись. Если во время общения возникли сомнения, говорит ли с вами мошенник, то лучше положите трубку и сами перезвоните в Социальный фонд России (злоумышленники по старой памяти называют пенсионным фондом). Звонить следует по официальному номеру. Ответившему сотруднику опишите ситуацию – вам подскажут, что делать. Также рекомендуется никогда не предпринимать поспешных действий на основании указаний звонящих – посоветуйтесь с родственниками, друзьями. Если мошенники все-таки завладели вашим личным кабинетом, постарайтесь как можно быстрее восстановить доступ к нему. Максимально оперативно это можно сделать в мобильном приложении СберБанк Онлайн: в строке поиска достаточно ввести слово “Госуслуги”, выбрать действие “Регистрация на госуслугах”, а затем подтвердить учетную запись и восстановить пароль.

Надо обратить внимание на новую набирающую популярность схему мошенников – вам звонят и сообщают о скором снятии номера телефона. Итак, вам поступает звонок, «Сотрудник» вежливо поинтересуется, все ли вас устраивает в обслуживании, есть ли жалобы, пожелания и внезапно сообщает, что у вашего номера есть срок действия. Да, вы что, не читали пункт 12.6 на 7 странице договора 5 лет назад? Так вот этот срок якобы есть, и он подходит к концу, а ваш номер скоро отключат. Вы, конечно, немного в шоке, но оператор быстро успокаивает. Никуда бежать не надо. Договор быстро переоформят. На какой срок вы

хотите? Год? Пять? Десять? Чтобы вы ничего не заподозрили (или успокоились, если уже заподозрили), псевдосотрудник обязательно подчеркнет, что никаких данных сообщать не надо, все это бесплатно, и номер карты никто не попросит. Наша бдительность усыплена, подвоха не видим, согласны на продление договора по телефону. Для большей правдоподобности лжеоператор сообщает, что копию нового договора можно получить в любом салоне связи. Также он придет на почту, которая указана на Госуслугах. И вот здесь начинается самое интересное. Но жертва уже так рада, что все легко решилось, что угрозы может и не заметить. Нам говорят, что для завершения процедуры оформления оператору необходимо проверить адрес электронной почты, который указан на Госуслугах. А для этого их хитрая база, соединенная с базой сервиса, запросит у вас пароль подтверждения, который вот прямо сейчас уже пришел вам в виде СМС. СМСка приходит действительно от Госуслуг, что подтверждает легенду. Как только вы сообщите звонившему код, вы рискуете потерять свою учетку на Госуслугах. Смысл всей схемы – угнать ваш аккаунт. На самом деле во время разговора мошенники просто пытались «восстановить» пароль к вашему кабинету через отправку вам СМС-сообщения. Зачем мошенникам ваш личный кабинет на Госуслугах. На первый взгляд, вроде ничего особо страшного, кроме мелких и крупных неудобств, нет. Ведь там нет данных карт. Но потеря своей учетной записи (доступа в личный кабинет) на самом распространенном сервисе страны сулит, большие неприятности. На вас оформят кредит или микрозайм. Мошенники, действуя от имени жертвы, регистрируются на сайтах микрофинансовых организаций, используя функцию «Войти с помощью Госуслуг». Они оформляют кредит и быстро обналичивают полученные деньги. Вам останутся долговые обязательства и бешеные проценты. На вас оформят налоговый вычет. Через Госуслуги злоумышленники получают доступ к аккаунту человека на сайте налоговой. Если налоги уплачены и человек имеет право на налоговый вычет, мошенники оформляют его сами и указывают свой банковский счет, который открыли специально для этой цели. Если не зайти в раздел «Вычеты» на сайте налоговой, не заметить заявку и не отменить ее, деньги уйдут мошенникам. Персональные данные из личного кабинета Госуслуг пострадавшего могут использоваться в других схемах мошенничества, а фантазия у таких преступников богатая и постоянно развивается. Что делать, если вас предупреждают об окончании срока действия вашего номера. Первое, что надо понимать: это никакие не операторы. Сотрудники никогда не звонят с подобными предложениями, не вступайте в беседы с подозрительными лицами, ни в коем случае не называйте коды СМС. Новый сервис «Защитник» на основе анализа больших данных надежно ограждает от мошеннических и спам-звонков, а также предупреждает о возможных утечках персональных данных от третьих лиц и попытках оформления на абонента кредита. И помните главное: никогда и не при каких обстоятельствах не сообщайте никому никаких кодов! Неважно, кем представляется звонящий.

Список литературы:

1. Гарафутдинова Н.Я., Селезнева Е.В., Соловьев А.А. Методы кибермошенничества и технологии противодействие им // Известия Омского регионального отделения Всероссийского общества охраны природы. Выпуск 16. Омск: ОРО ВООП, 2024. 111 с.

2. Уберечься от мошенников / Дзен. URL: https://dzen.ru/search?query=уберечься%20от%20мошенников&mt_link_id=kikkq1&utm_source=yandex&utm_medium=cpc&utm_campaign=SEARCH_Category_NoScam&yclid=10814793335844634623