DOI 10.58351/2949-2041.2024.16.11.013

Соловьев Анатолий Алексеевич,
к.ф-м.н, профессор, СибАДИ, Омск

Камшибаев Жанат Жаскайратович,
старший преподаватель,
Торайгыров университет, Павлодар

Егорова Наталья Николаевна,
старший преподаватель, СибАДИ, Омск

Отс Дарья Анатольевна,
преподаватель, СибАДИ, Омск

КАК ЗАЩИТИТЬСЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ
HOW TO PROTECT YOURSELF FROM PHONE SCAMS

Аннотация: В статье рассмотрены разнообразные методы обмана населения телефонными мошенниками и способы защиты от них.

Abstract: The article discusses various methods of deception of the population by telephone scammers and ways to protect against them**.**

Ключевые слова: «Злой близнец», соцсети, аккаунт на «Госуслугах», кибербезопасность, фишинговая ссылка, мессенджер, поддельные профили токенизированным картам Антифрод-системы.

Keywords: «Evil twin», social networks, account on «Public Services» cybersecurity, phishing link, messenger, profiles to tokenized cards of the Anti-fraud system.

Функцию автоматического присоединения к уже известным сетям Wi-Fi на телефоне лучше отключать, чтобы не стать жертвой мошенников, которые могут создавать копии Wi-Fi-точек в общественных местах для кражи данных. Распространена атака на пользователей публичного Wi-Fi, которую называют Evil twin («Злой близнец»). Злоумышленник создает в общественном месте свою Wi-Fi-точку, но называет ее так же или именем, похожим на название заведения, где находится. Параллельно к Wi-Fi-роутеру заведения применяется атака, которая отключает от него пользователей. После этого устройства пользователей подключаются к такому «двойнику» и тем самым дают хакеру доступ ко всему их «интернет-трафику». Особую опасность в этом случае представляют настройки смартфона по автоматическому подключению к известным Wi-Fi-сетям.

Иногда при подключении к такой фейковой Wi-Fi-точке пользователь видит «страницу авторизации», которая предлагает зайти в сеть, например, через соцсети или почту. Человек выбирает соцсеть, вводит данные для входа в аккаунт и таким образом отправляет их злоумышленнику. В первую очередь для защиты нужно отключить опцию автоматического подключения к известным Wi-Fi-сетям на устройстве. Если устройство запрашивает повторную аутентификацию, но пользователь не нажимал кнопку «Забыть сеть», то стоит проверить, нет ли в списке доступных сетей другой точки с таким же названием. Есть и другие мифы о безопасности Wi-Fi. Так, защищенный паролем Wi-Fi не защищает данные пользователя. Пароль, который пользователь вводит, чтобы подключиться к сети, защищает только само заведение от того, чтобы его сервисом не пользовались все, кто оказался в зоне покрытия роутера. Он не обеспечивает защиту от перехвата, идущего через Wi-Fi трафика. Также, используя публичный Wi-Fi, пользователь может получить на смартфон или ноутбук вирус. Так, если хакеру удалось взломать роутер или обманом заставить человека подключиться к фейковой сети, он может перенаправлять пользователя на фишинговую страницу, где сообщается, что ему нужно, например, обновить программное обеспечение. Тогда как в действительности по клику на устройство скачивается вредоносный файл.

Участились случаи фиксирования нового способа обмана граждан. Это звонки из поликлиники. Расчет на то, что здесь подозрений быть не может. Легенда примерно такая: представитель поликлиники якобы жалуется на не пройденную процедуру, на которую была запись, угрожает санкциями в виде аннулирования записей и чем-то еще, что не очень важно, потому что все знают, как бывает сложно куда-то записаться. Все, мысли жертвы уже только о том, как найти флюорографию (это может быть и другая процедура, справка, назначение и т.д.). Далее вам предлагают приехать и показать заключение, желательно – прямо сейчас. Если сделать это проблематично, то «заботливый» оператор предлагает пробить вас по системе. Однако это сделать невозможно без номера СНИЛС. Потом по классике: продиктуйте номер, вам сейчас придет СМС. И ваш аккаунт на «Госуслугах» уже у мошенников. А вот чем грозит потеря «Госуслуг». Например, в некоторых банках и микрофинансовых организациях можно взять кредит с помощью подтвержденного аккаунта на «Госуслугах». Если аккаунт защищен слабо или человек сам передаст персональные данные, например пароль или код из СМС, злоумышленники могут попытаться оформить на его имя кредит или микрозаем. 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. Как же защитить свой аккаунт на «Госуслугах».

Еще раз напоминаем о простых правилах, которые помогут сберечь деньги и нервы: никогда не передавайте личные данные третьим лицам и используйте все опции, помните, что в большинстве случаев жертвы сами отдают аферистам все данные; поставьте надежный пароль. Он должен быть действительным надежным; включите двухфакторную аутентификацию, даже, если мошенники подберут пароль, они не смогут войти в аккаунт, а вам придет сигнал от системы о попытке взлома в виде СМС или письма на почту. Что же делать, если аккаунт взломали. Шаг 1: восстановите доступ к учетной записи. Шаг 2: защитите аккаунт (смена паролей, двойная защита – об этом писали выше). Шаг 3: определите, где использовалась учётная запись. Перейдите в личный кабинет → Безопасность → Действия в системе. Проверьте, не было ли подозрительных действий в учётной записи. Если были и учётная запись использовалась на «Госуслугах», обратитесь в службу поддержки. Если на стороннем ресурсе – в службу поддержки данного ресурса. Выйдите из приложений, в которые вы не заходили: личный кабинет → Безопасность → Моб. приложения. Отзовите разрешения, которые вы не выдавали: личный кабинет → Согласия и доверенности → Разрешения. Проверьте поданные заявления. Это поможет выявить, какие действия хотели совершить мошенники от вашего имени. Шаг 4: подайте заявление в МВД. Берегите себя и свои аккаунты!

Рассмотрим, как работает еще одна новая популярная схема обмана россиян. Злоумышленники начали скрывать фишинговые ссылки за изображениями. Мошенники отправляют письма с картинками в рамках таргетированной фишинговой рассылки. С этой киберугрозой уже столкнулись сотрудники компаний из сферы сетевого ритейла, дистрибуции, перевозок и логистики. Цель мошенников – выманить учетные данные от корпоративной почты потенциальных жертв с помощью подставного изображения. Письма приходят на английском языке. Они якобы направлены от представителей южнокорейской компании. В них мошенники под видом сотрудников этой организации сообщают, что отправили инструкцию своему банку для перевода платежа. Они просят потенциальных жертв проверить детали в отсканированном документе, который добавлен в тело письма. По легенде сделать это нужно быстро, чтобы как можно скорее получить оплату. Изображение видно плохо – на это и рассчитывают злоумышленники. Даже если человек не ожидает письма, ему может быть интересно, посмотреть детали. Однако на самом деле за картинкой скрывается фишинговая ссылка. Если Вы нажмете на скан, то он попадет на поддельный ресурс, который выдает себя за файлообменник от Adobe. Пользователя попросят ввести учетные данные от корпоративного почтового аккаунта, чтобы получить доступ к документу. Но делать этого не

стоит. Все введенные сведения уйдут злоумышленникам. Чтобы не стать жертвой фишинговых атак, эксперты по безопасности рекомендует не доверять письмам с незнакомых ящиков, особенно когда речь идет о конфиденциальных данных, денежных операциях и подозрительных вложениях, даже если визуально похоже, что письмо пришло от организации с хорошей репутацией. Компаниям необходимо пользоваться надежным защитным решением, которое автоматически будет отправлять подобные письма в спам. Также важно рассказывать людям о кибербезопасности и обучать их распознавать техники социальной инженерии.

Ещё пример новой мошеннической схему, в которой телефонные аферисты представляются работниками «Почты России». Схема выглядит так. Жертве поступает звонок якобы от сотрудника почтовой компании. Злоумышленник заявляет о посылке из-за рубежа, которая вот-вот должна поступить в отделение и за нее нужно уплатить таможенный сбор, однако жертва не ждет никаких посылок. Следом мошенник предлагает оформить отказ от посылки, которую человек не заказывал. Чтобы это сделать, якобы нужно назвать СМС-код из пуш-уведомления, которое поступит на номер телефона жертвы. На самом деле это код для входа в банковский клиент. Если человек все же назвал код, то мошенники попадают в личный кабинет, переводят все деньги на свои счета или оформляют кредиты. Подобным образом мошенники получают доступ к аккаунтам на Госуслугах. Как только злоумышленники вошли в личный кабинет, они собирают все данные о жертве, чтобы потом использовать их против человека. Стоит отметить, что на официальном сайте «Почты России» можно посмотреть, какие посылки оформлены на человека. Помните, что настоящие сотрудники банков и любых других организаций никогда не запрашивают СМС-коды авторизации.

В последнее время зафиксированы фейковые рекламные акции от имени банка в популярных мессенджерах. В таких сообщениях пользователям обещают деньги в подарок за переход по ссылке и участие в реферальной программе. Таким способом мошенники рассчитывают получить доступ к персональным данным или личному кабинету человека в онлайн-банке – вне зависимости от того, в каком банке хранятся его деньги. Мошенники регулярно используют схемы с фейковыми рекламными акциями и размещают в популярных мессенджерах и соцсетях лже-объявления от банков или других крупных компаний. При этом используют фирменную символику, имитируют стиль сообщения и даже добавляют детали, например, ИНН, ЕРИД, ссылку на сайт компании. Пользователям обещают приз в несколько тысяч рублей за участие в акции, опросе или присоединение к реферальной программе. На самом деле, после перехода по фишинговой ссылке пользователь попадает на страницу с анкетой для ввода персональной информации. При этом для подтверждения действий опасный сайт запрашивает код из СМС, доступ к которому обеспечит мошенникам управление онлайн-банком жертвы или порталом с госуслугами.

В целом злоумышленники могут использовать разные предлоги, чтобы убедить пользователей нажать на фишинговую ссылку. Мошенники постоянно создают новые схемы, при этом поддерживая старые сценарии и возвращаясь к ним за быстрыми деньгами. Работа фишинговых ссылок не требует от злоумышленников больших усилий или вовлеченности в процесс хищения. Технология работает сама по себе, без внимания, но зато объем возможных хищений может сильно варьироваться, достигая больших сумм. Кроме того, каждый пользователь должен соблюдать личную цифровую «гигиену»: проверять безопасность ссылок на сайты и не указывать свою персональную секретную информацию. Чтобы избежать инцидентов с мошенниками, следуйте простым правилам безопасности при работе в интернете. Например, эксперты банка создали специальный дайджест «ВТБ Онлайн против мошенников», где рассказали о самых популярных видах мошенничества и мерах борьбы с ними. Помимо этого, пользователи банка онлайн могут быстро проверить ссылку через настройки профиля в разделе «Безопасность».

Напоминаем, никогда не указывайте свою персональную информацию, включая паспортные данные и данные банковских карт, на незнакомых сайтах. Также переход по опасной фишинговой ссылке может привести к заражению смартфона вирусом, поэтому следует установить на личное устройство антивирус. Мошенники стали чаще похищать деньги

россиян через призыв обновить банковское приложение. Каждый десятый звонок в мессенджерах злоумышленников был с такой просьбой от злоумышленников. Мошенники в разговоре представляются сотрудниками финансовой организации и предлагают установить «правильную версию» банковского приложения. Преступники настаивают на скорейшем обновлении программы – в противном случае банк якобы заблокирует счета и карты клиента. Жертве высылают ссылку для скачивания программы, однако после перехода по ней экран смартфона блокируется. Мошенники получают доступ к кабинету пользователя в приложении, клиенту приходит СМС-код, с помощью которого злоумышленники выводят деньги со счета. В банке гражданам советуют прекратить разговор, если «сотрудник» призвал обновить приложение. Далее следует обратиться в финансовую организацию и попросить временно заблокировать личный кабинет, чтобы мошенники не могли вывести средства со счета.

Около 80% хищений денег происходит с помощью переводов между своими счетами или через мобильные платежные системы для бесконтактной оплаты. По оценкам «Сбера», примерно 50% похищаемых телефонными мошенниками средств выводится через приложение бесконтактной оплаты. Жертву убеждают установить приложение платежной системы и привязать к устройству банковскую карту, которая принадлежит мошенникам. Затем человек вносит наличные деньги через банкомат на карту мошенника, привязанную к приложению бесконтактной оплаты на его телефоне.

Аферисты также начали обманывать пользователей, создавая в мессенджерах поддельные профили популярных сервисов доставки. Чаще всего злоумышленники копируют официальные профили СДЭК, «Сбермаркета», «Яндекс доставки» или Delivery Club в мессенджере WhatsApp, где отправляют сообщение о том, что заказ готов к доставке. Чтобы узнать подробности о доставке или отследить заказ, предлагается перейти по фишинговой ссылке, которая перенаправляет на поддельный сайт, мимикрирующий под официальный сервис. На этом сайте мошенники просят ввести личные данные: номер карты, имя пользователя и пароль от онлайн-банка.

Очередной вид мошенничества, направленный, скорее, на старшее поколение. Здесь главная цель киберпреступников – получить доступ к банковской карте пользователя. Поэтому нельзя переходить ни по каким подозрительным ссылкам, тем более если вы не ожидаете никакой доставки. Злоумышленники заранее заботятся об обходе защитных банковских систем, и уже в половине случаев телефонного мошенничества они маскируют вывод похищенных средств переводом через систему бесконтактной оплаты, установленную на смартфоне самой жертвой.

Злоумышленники используют два механизма вывода похищенных средств: через мобильные платёжные системы (pay-сервисы) для бесконтактной оплаты и переводы между счетами жертвы. Так, по оценкам Сбербанка, примерно половина похищаемых телефонными мошенниками средств сейчас выводится по следующей схеме: злоумышленники убеждают жертву установить на смартфон приложение мобильной платёжной системы (если оно ещё не установлено) и привязать к устройству банковскую карту, которая принадлежит мошенникам. Далее аферисты сообщают жертве данные карты и код подтверждения из СМС, после чего человек самостоятельно вводит их в установленное приложение бесконтактной оплаты. Затем он вносит наличные (как собственные сбережения, в том числе снятые со счетов в разных банках, так и кредитные средства) через банкомат на карту мошенника, привязанную к приложению бесконтактной оплаты на своём телефоне. В итоге внесение денег с такой карты идентифицируется как операция, совершённая владельцем мобильного устройства, хотя фактически доступ к карте имеют злоумышленники. Чтобы «перекрыть кислород» злоумышленникам, необходимо ввести лимиты на операции по токенизированным картам, а также период охлаждения между их установкой на устройствах и активацией.

Помимо этого, деньги выводится с помощью переводов «me2me» (на свой же счёт): жертву убеждают перевести деньги со своего счёта в хорошо защищённом банке на свой же счёт в другом, менее защищённом. Если такого счёта нет – просят его открыть. После этого деньги похищаются в обход «антифрод-системы» (системы противодействия мошенникам)

менее защищённого банка, либо жертва может обналичить их через банкомат, чтобы передать аферистам. Что касается me2me-переводов, они имеют низкий уровень риска, банковские антифрод-системы их пропускают. Поэтому необходимо пересмотреть текущий стандарт риск-индикаторов для переводов между своими счетами. В первую очередь ужесточение стандарта должно касаться банков-получателей – например, они должны строже и внимательнее относиться к операциям по снятию наличных, если клиент недавно перевёл деньги на счёт из другого банка.

Мошенники постоянно совершенствуют актуальность своих схем. Они пытаются получить доступ к счетам россиян, звоня от имени сотрудников «Почты России» рано утром в будни. Для звонка используют аккаунт в мессенджере, контакта «Почта России». Звонящий сообщает, что с ожидаемой посылкой возникла проблема (варианты могут разниться: посылка или потерялась, или ее отправили обратно в сортировочный центр и т. п.), для решения проблемы необходимо установить якобы новое приложение «Почты России». «Злоумышленник «помогает» отключить функции безопасности на телефоне, пострадавший качает вредоносное приложение, которое дает злоумышленнику возможность удаленного доступа к телефону. После этого собеседник просит потенциальную жертву установить в приложении код-пароль, который, как правило, одинаковый для всех сервисов. Пострадавший вводит код-пароль и злоумышленник получает доступ к мобильным банкам, чтобы в дальнейшем удаленно осуществить кражу средств.

Напомним простые правила, которые помогут вам, вашим родным и близким обезопасить себя от подобной мошеннической схемы: Не брать трубку, если вам звонит неизвестный номер, ни по телефону, ни в мессенджере. Не брать трубку, если звонящий в мессенджере номер отображается как «Почта России», любой Банк, государственный орган и т. п. Важно помнить, что официальные представители Банков, социальных и государственных служб никогда не осуществляют звонки через мессенджеры. Не ставить одинаковые код-пароли на приложения, одинаковые пароли к разным аккаунтам. Если вы боитесь забыть пароли – существуют облачные сервисы для хранения паролей (советуем использовать сервисы крупных известных российских компаний). Антифрод-системы не всегда гарантируют безопасность ваших финансов, бдительность – тоже эффективная мера защиты.

Еще одна новая схема взлома профилей на госсервисах. Злоумышленники звонят человеку от имени сотрудников госструктур, сообщают, что ему пришло заказное письмо и предлагают прислать уведомление на почтовый или электронный адрес. Для оформления заявки они просят назвать проверочный код, который присылают на телефон с текстом «код восстановления доступа» к учетной записи. Если на этом этапе человек кладет трубку, заподозрив неладное, через какое-то время ему звонят повторно, также представляясь работниками госструктур. На этот раз собеседники убеждают жертву, что в первый раз она разговаривала с мошенниками, и ее учетная запись взломана. Чтобы защитить данные, они требуют код доступа из СМС-сообщения. В этот момент человек, находясь под психологическим давлением неизвестных и полностью доверяя им, становится жертвой дальнейшего обмана. Такие звонки составляют 30% от общего числа атак, эти схемы особенно распространились в период уплаты налогов. Если вы все же взяли трубку, помните: не бывает ситуаций, в которых вас будут торопить совершать какие-либо действия с вашим устройством, в особенности смысл которых вы не понимаете; не бывает ситуаций, в которых нельзя перезвонить по официальному номеру / обратиться физически в офис банка / на почту / в налоговую и т. п.; если собеседник настаивает на конфиденциальности вашего разговора – помните, что конфиденциальные данные не обсуждаются по открытым каналам связи, в том числе по телефону.

Список литературы:

1. Явинский А.В., Соловьёв А.А. Способы борьбы с телефонными мошенниками // Образование. Транспорт. Инновации. Строительство. Сборник материалов IV Национальной научно-практической конференции. Омск, 2021. С. 828-831.

2. Гарафутдинова Н.Я., Егорова Н.Н., Соловьев А.А. Цифровое мошенничество и методы борьбы с ним // Известия Омского регионального отделения Всероссийского общества охраны природы. Выпуск 16. Омск: ОРО ВООП, 2024. 111 с.

3. Гарафутдинова Н.Я., Поступинских Л.А., Соловьев А.А. О противодействии цифровому мошенничеству // Известия Омского регионального отделения Всероссийского общества охраны природы. Выпуск 16. Омск: ОРО ВООП, 2024. 111 с.

4. 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.