С какими мошенническими схемами можно столкнуться в 2024 году?

Схема 1. Операторы сотовой связи

Под видом специалистов известных телекоммуникационных копаний мошенники стараются получить доступ к аккаунту пользователя «Госуслуги».

Они звонят жертве и утверждают, что договор заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет злоумышленник. достаточно продиктовать код из смс. Следующий шаг – перейти по ссылке, где нужно ввести ещё один код.

Таким образом, человек не продлевает договор, который на самом деле является бессрочным, а предоставляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе, которая хранится на этом ресурсе.

Есть и другая цель, которую преследуют мошенники, представляясь оператором связи.

Жертве также поступает звонок с предложением по смене тарифного плана, подключением опций, замены sim-карты. Чтобы реализовать любое из действий абоненту необходимо продиктовать код из смс, который придет на его номер. С помощью этого кода злоумышленник получает доступ к личному кабинет пользователя на официальном сайте оператора. а уже там он настраивает переадресацию сообщений и звонков с номера телефона жертвы на свой.

Это делается для того, чтобы в дальнейшем подтвердить разного рода операции: вывод средств с банковских карт абонента, оформление на него кредита.

ВАЖНО!

Вы можете обновить персональные данные обратившись за услугой лично – в офисе оператора связи или в личном кабинете на его официальном портале (но не по ссылке из смс).

Не называйте никаких данных незнакомым по телефону. Если сомневаетесь, позвоните оператору связи по номеру, который размещен на его официальном сайте.

Схема 2. Предложения от лжеброкеров

Злоумышленники связываются с потенциальными инвесторами через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое – нужно лишь открыть «брокерский» счет и инвестировать от 10 000 рублей. Доход – не меньше миллиона.

Для открытия такого счета мошенники требуют установить приложение.

Далее программа имитирует якобы рост доходов от инвестиций, в том числе в криптовалюту. Как только у «инвестора» возникает желание вывести деньги со счета – начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счет еще раз на определенную сумму, оплатить «страховку» или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя, чтобы можно было «обналичить» средства. В итоге инвестор теряет свои деньги, а заодно и надежду на будущие миллионы.

Вариант этой мошеннической схемы – участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают потенциальных жертв при помощи писем на электронную почту. Злоумышленники, оформляя сообщение, копируют визуальный стиль финансовой организации и далее для убедительности используют те же корпоративные цвета, логотип и другие элементы. Для участия в «выгодной» кампании предлагается перейти по ссылке из письма.

После жертве предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи с представителем организации, а также дадут доступ к специальному приложению. А уже там понадобится ввести данные своей банковской карты – с нее аферисты потом и спишут деньги.

ВАЖНО!

Проверьте сайт инвестиционной компании или брокера. Обратите внимание на реквизиты и наличие лицензии Банка России.

Откажитесь от услуг компании или ее представителей, если они просят перевести деньги за услуги на карту физического лица (либо через электронный кошелек).

Обязательно заключите договор и запрашивайте отчет об оказании брокерских услуг.

Не ведитесь на обещания гарантированного высокого дохода в короткие сроки.

Схема 3. Общение с работодателем

Собеседование с будущим работодателем – волнительная процедура. Порой мошенники пользуются растерянностью соискателей и крадут личные данные прямо во время онлайн-встречи.

Под видом будущего работодателя мошенники проводят собеседование, где они просят кандидата заполнить анкету прямо во время зума. Один из ее пунктов – номер карты и другие ее данные. На нее злоумышленники обещают производить оплату. Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия.

Вместо пополнений с банковской карты соискателя в будущем происходят списания, а на работу его так и не устраивают.

Находясь в поиске работы, можно не только потерять деньги, но и нарушить закон, став дроппером.

В последнее время именно этот мошеннический сценарий становится популярным, а его жертвами становятся студенты и пенсионеры.

Дропперы или дропы (от английского drop — бросать, капать) – подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт.

Часто жертва не осознает, что вовлечена в преступную схему. Ведь объявление о работе, на которую она устраивается, не выглядит подозрительно. А будущий работодатель после собеседования предоставляет договор, оговаривает условия труда, сроки выполнения работы и другие нюансы.

ВАЖНО!

Внимательно изучайте предложение от будущего работодателя и отзывы о нем.

Не ведитесь на обещания легкого заработка с минимальной затратой собственного времени.

При общении сохраняйте холодную голову, не поддавайтесь эмоциям, а главное – следите за данными, доступ к которым предлагается предоставить.

Схема 4. Звонки или сообщения от знакомых

Еще одна тактика злоумышленников – рассылка сообщений с просьбой одолжить денег близким или друзьям. Порой в своих сценариях мошенники заходят и дальше – играют на чувствах жертвы и сообщают, что ее родственник попал в беду. Если раньше аферистам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за них это делает искусственный интеллект.

Злоумышленники взламывают аккаунт пользователя, скачивают голосовые сообщения и на их основе генерируют монолог для дальнейшего обмана.

Существует и другой сценарий – просьба проголосовать за детей или племянников в детском конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

ВАЖНО

Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых.

Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным. Такой шаг поможет раскусить намерения мошенника.

Схема 5. Оплата услуг по фейковому QR-коду

Сегодня, чтобы получить какую-либо услугу или оплатить товар, достаточно навести камеру на QR-код. Например, им можно воспользоваться, чтобы взять в аренду самокат или портативное зарядное устройство для гаджета. Правда, вместо прогулки с ветерком и заряженного аккумулятора телефона можно получить пустой банковский счет.

Дело в том, что такой QR-код ведет не на официальный сайт сервиса, а на поддельный ресурс, через который аферисты крадут деньги и данные карты.

ВАЖНО

Оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Схема 6. Звонки и сообщения из банка

#1 Мошенник создаёт в мессенджере аккаунт, якобы принадлежащий Сберу, — с названием, имитирующим номер 900 и логотип банка. С этого профиля злоумышленник делает первый звонок, представляясь сотрудником банка, и спрашивает человека, обновлял ли он мобильное приложение в последнее время.

#2 Если ответ отрицательный, «работник» сообщает, что необходимо дождаться звонка от профильного специалиста банка, который поможет обновить приложение.

Сообщник мошенника звонит с другого аккаунта или даже в другом мессенджере, где есть функция трансляции экрана во время видеозвонка. Такая путаница с разными «специалистами» нужна, чтобы дезориентировать человека и заставить действовать по указке.

#3 Второй «сотрудник» объясняет, что звонит по видеосвязи для идентификации клиента по биометрии. А потом просит включить режим демонстрации экрана. Благодаря этому, по словам мошенника, подключается некая «роботизированная система для диагностики счёта».

#4 После этого человека просят зайти в мобильное приложение банка. Мошенник уверяет, что это абсолютно безопасно, так как экран будет видеть только робот, а сам сотрудник — нет.

На самом деле трансляция экрана позволяет злоумышленнику увидеть номера карт, суммы на счетах, коды в СМС от банка. Эта и другая информация помогает мошеннику заполучить доступ к личному кабинету клиента в приложении на своём устройстве и украсть его деньги — или убедить его перевести их на «безопасный счёт»

ВАЖНО

Сотрудники банков не связываются с клиентами в мессенджерах.

Нельзя демонстрировать по видеосвязи экран своего устройства незнакомцам, кем бы они ни представлялись.

Роботизированная система для диагностики счёта — это выдумка мошенников.

Схема 7. Звонки и сообщения от государственных ведомств.

Часто мошенники звонят или пишут человеку якобы от лица сотрудников ФСБ, Росфинмониторинга, ФНС, Социального фонда России, портала «Госуслуги».

Самая распространенная уловка – предложение получить какую-либо государственную выплату. Схема классическая: вы нам данные карты, мы вам – деньги. Есть и другой сценарий. Например, звонок от представителей следственных органов или Росфинмониторинга с угрозой блокировки счета, по которому якобы зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф. Для убедительности они могут даже прислать квитанцию на официальном бланке ведомства.

ВАЖНО

Помните, что подобные ведомства не наделены полномочиями по аресту денежных средств, не оказывают платных услуг по оформлению документов, а также не рассылают подобные письма и не звонят по телефону или в мессенджерах. Если вы получили подобные сообщения – проигнорируйте их и обратитесь напрямую в государственную организацию.

Внимание!

Совсем недавно мошенники начали осваивать схемы обмана с использованием **ДИПФЕЙКОВ** — аудиосообщений, которые имитируют голос знакомого вам человека, и вводят в заблуждение.

Вот несколько форм обращений к пользователям сети, основанных на технологиях искусственного интеллекта, которыми аферисты пользуются наиболее часто.

- Сообщения от «босса». Злоумышленники выдают себя за руководителей компаний и требуют связаться «с сотрудником службы безопасности». Задача последнего — убедить жертву перевести деньги на некий «безопасный счет».

Фейковые свидания. Мошенники используют аудиосообщения со сгенерированным женским голосом и привлекательным фото, чтобы обманывать пользователей на онлайн-площадках знакомств.

- Привет от родственника. Телефонные аферисты, моделируя голос близкого человека, заставляют детей отдавать подставным курьерам сбережения родителей.

ВАЖНО:

Будьте бдительны в ходе телефонных разговоров, не спешите принимать решения и всегда перепроверяйте информацию — особенно, если речь идет о деньгах.

В официальном телеграмм-канале мессенджера «Telegram» «Вестник киберполиции России» Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации размещены информационные материалы по профилактике дистанционных хищений, содержащие сведения о схемах мошеннических действий, применяемых преступниками на территории Российской Федерации, здесь же можно оперативно получать информацию о новых схемах мошенничества (ссылка: https://t.me/cyberpolice_rus/1072).

Официальная страница отдела общественной безопасности и профилактики правонарушений администрации Советского района:

Официальная страница Отдела Министерства внутренних дел Российской Федерации по Советскому району в социальной сети «ВКонтакте»: