Информация
об основных схемах мошеннических действий, используемых преступниками на территории Ханты-Мансийского автономного округа – Югры

Перечень и основные характеристики дистанционных хищений:

1. Звонок сотрудника банка либо правоохранительных органов, рекомендующего под предлогом пресечения несанкционированного оформления кредита, хищения денежных средств с банковских счетов гражданина, оформить встречный кредит (зеркальная заявка) и направить средства на указанный мошенником счет.

2. Под предлогом заработка путем инвестиционных вложений предлагается перевести денежные средства с личных счетов на указанный мошенником счет.

3. Внесение предоплаты при совершении сделки по приобретению товаров (услуг) на сайте «Авито», в социальной сети «ВКонтакте», в группах мессенджеров «WhatsApp», «Viber», «Telegram».

4. Заем денежных средств «родственнику, знакомому» посредством отправления сообщений или осуществления звонков с известных потерпевшему номеров в мессенджерах «WhatsApp», «Viber», «Telegram».

5. Передача или перечисление денежных средств третьим лицам как способ помощи родным или близким, «попавшим в беду», или же как способ помочь им «избежать уголовного преследования».

6. Когда участниками преступления используется механизм поэтапного обмана потерпевшего, где на первом этапе «работник» сотового оператора под предлогом необходимости продления срока договора предоставления услуг мобильной связи предлагает гражданину сообщить ему смс-коды доступа к личному кабинету на сайте «Госуслуги», после чего уже «сотрудники» сайта «Госуслуги» и Центрального банка Российской Федерации под предлогом пресечения противоправных действий и сохранения денежных средств потерпевшего от несанкционированного перевода либо хищения убеждают его перевести личные сбережения либо кредитные средства на «безопасный банковский счет».

7. Когда гражданину от лица руководителя сообщается о рекомендованном (обязательном) выполнении предложений сотрудников правоохранительных органов или работников банковских структур по перечислению личных сбережений либо оформлению встречной (зеркальной) заявки на кредит и последующего перечисления кредитных средств, якобы направляемых на пресечение несанкционированного оформления кредита, попытки хищения денежных средств с банковских счетов потерпевшего.

8. Когда в мошеннических схемах злоумышленники, используя доверчивость несовершеннолетних, их заинтересованность в получении легких доходов, их желание защитить родителей либо близких им людей от преступников, получив реквизиты банковских карт, совершают хищение личных сбережений либо кредитных средств.

Для оказания большего давления на потерпевших зачастую перечисленные схемы дополняются информацией, что средства с их счетов несанкционированно переводятся на поддержку вооруженных сил Украины, в связи с чем, чтобы избежать уголовной ответственности за финансирование террористических организаций, требуется незамедлительное выполнение рекомендуемых действий.

С какими мошенническими схемами можно столкнуться в 2024 году (данные МВД России)

Операторы сотовой связи

Под видом специалистов известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту пользователя «Госуслуги». Они звонят жертве и утверждают, что действующий 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 еще 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 кабинету пользователя на официальном сайте оператора. А уже там он настраивает переадресацию сообщений и звонков с номера жертвы на свой.

Это делается для того, чтобы в дальнейшем подтверждать 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.

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.

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.

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.

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.

10 правил, как не стать жертвой одной из мошеннических схем при дистанционной покупке товаров

1. Старайтесь не переходить по ссылкам из рекламных писем на сайты магазинов. Это может быть мошенническая копия, на которой получится только оплатить товар (перевести деньги мошеннику), но, конечно, не получить его. Вводите адрес известного магазина в строке браузера самостоятельно и проверяйте, действительно ли в нем есть акция, о которой идет речь в письме.

2. Всегда обращайте внимание на доменное имя сайта: мошеннические ресурсы имеют схожие с известными магазинами имена, но написанные с ошибками или замененными символами.

3. Проверьте дату создания сайта с помощью Whois-сервисов. Если странице пара недель или месяц, то она с высокой долей вероятности фейковая, созданная к праздничной дате в целях наживы.

4. Удостоверьтесь, что сайт использует протокол https и имеет действующий сертификат безопасности (символы https и изображение замочка в адресной строке). В противном случае никогда не вводите на сайте свои персональные и платежные данные.

5. Проверьте отзывы о товарах и магазине. Если их нет или они исключительно положительные и написанные примерно в одно и то же время, перед вами, скорее всего, фейк. Отзывы об интернет-магазине читайте не на сайте самого интернет-магазина, а на сторонних ресурсах.

6. Обратите внимание на косвенные индикаторы фейка: требование обязательной предоплаты, недоступность самовывоза и отсутствие возможности оплатить покупку при получении. Эти три фактора должны насторожить вас и предупредить о том, что перед вами, возможно, мошеннический сайт.

7. Сравнивайте цены. Перед покупкой обращайте внимание на цену на товар в сравнении с предложениями других магазинов. Если цена сильно ниже рыночной, особенно в период высокого спроса, то велика вероятность, что вы получите товар сомнительного качества или не получите его вовсе.

8. Проверяйте реквизиты интернет-магазина перед покупкой. На мошеннических сайтах чаще всего это реквизиты физического лица, номер карты или электронного кошелька. Таким сайтам доверять нельзя.

9. Не ведитесь на манипуляции, к которым относятся: всплывающие заманивающие баннеры, акции с таймерами оставшегося времени, надпись «этот товар вместе с вами смотрят N человек» и многое другое. Все эти приемы не должны подгонять вас совершить покупку – сначала убедитесь, что сайту можно доверять.

10. Всегда держите включенным антивирус на компьютере и телефоне – это поможет защититься от заражения троянской программой, позволяющей злоумышленникам обчистить ваш банковский счет.