Информация
об основных схемах мошеннических действий,
используемых преступниками на территории автономного округа
в феврале 2024 года (данные МВД России)

Основные схемы дистанционных хищений:

1. 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. Злоумышленник уверяет, что идти никуда не нужно, все можно сделать по телефону, достаточно продиктовать код из смс-сообщения. Далее гражданину предлагается 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 поступает звонок с предложением по смене тарифного плана, подключением опций или замены «sim-карты». Чтобы реализовать любое из действий, абоненту необходимо продиктовать код из входящего смс на его номер. С помощью данного кода злоумышленник получает доступ к личному кабинету пользователя на официальном сайте оператора, где настраивает переадресацию смс-сообщений и звонков с мобильного номера жертвы на свой номер. Это делается для того, чтобы в дальнейшем подтверждать разного рода операции: вывод средств с банковских карт абонента, оформление кредита на его имя.

Вы можете обновить персональные данные, обратившись лично за услугой в офис оператора связи или в личном кабинете на официальном портале данного оператора связи (но не по ссылке из смс-сообщения). Не называйте никаких данных незнакомым по телефону. Если сомневаетесь, позвоните оператору связи по номеру, который размещен на его официальном сайте.

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 менее миллиона. Для открытия такого счета мошенники требуют установить приложение. Далее программа имитирует рост доходов от инвестиций, в том числе в криптовалюту. При необходимости вывести деньги со счета «инвестором» данная операция оказывается невозможной. «Лжеброкеры» объясняют это сложным процессом и далее предлагают пополнить счет еще раз на определенную сумму, оплатить «страховку» или ежедневное размещение валюты в «европейской ячейке», или 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 жертве предлагается перейти по ссылке из письма, после чего – пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи с представителем организации. Затем жертве предоставят доступ к специальному приложению, где понадобится ввести данные своей банковской карты, с которой мошенники спишут денежные средства.

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 доверяйте обещаниям гарантированного высокого дохода в короткие сроки.

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 просят кандидата заполнить анкету прямо во время онлайн-встречи. Один из пунктов анкеты – номер и другие данные карты, на которую злоумышленники обещают производить оплату. Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, в случае если какую-либо из карт, 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.

Внимательно изучайте предложение от будущего работодателя и отзывы о нем. Не доверяйте обещаниям легкого заработка с минимальной затратой собственного времени. При общении сохраняйте холодную голову, не поддавайтесь эмоциям, и главное – следите за данными, доступ к которым предлагается предоставить.

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 мошенникам 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.

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 раскрыть намерения мошенника.

5. Оплата услуг по поддельному 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 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 мошенники крадут деньги и данные карты.

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

6. Звонки и сообщения из банка.

Наряду с лживыми угрозами об оформлении кредита на имя владельца банковской карты другим человеком или подозрительной операции по ней появились новые сценарии мошеннических действий. Злоумышленники под видом специалистов техподдержки финансовых организаций предлагают установить на смартфон приложение для поиска вирусов. Это вредоносное программное обеспечение, которое дает доступ к телефону жертвы и его данным. Еще один популярный сценарий – помощь в сохранении денежных средств. Мошенники под видом сотрудников Банка России сообщают жертве о том, что кто-то пытается похитить деньги с ее банковского счета. Чтобы этого не допустить, необходимо перевести средства на «безопасный» счет в ЦБ РФ. По легенде это временная мера на период поиска преступников. Затем всю сумму гражданину якобы возместят наличными в приемной Банка России в Москве.

Пользуйтесь только официальными ресурсами финансовых организаций. В случае если вам звонят сотрудники банка и разговор с ними кажется подозрительным, перезвоните на официальный номер, размещенный на сайте финансовой организации. Там же вы можете найти ссылки на скачивание официальных банковских приложений.

7. Звонки и сообщения от государственных ведомств.

Часто мошенники звонят или пишут гражданину 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!». Существует 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.

Помните, что вышеназванные 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, в т.ч. в мессенджерах. Если вы получили подобные сообщения – проигнорируйте их и обратитесь напрямую в государственную организацию.

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 поддельная, 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 отзывов нет или они исключительно положительные и написанные примерно в одно и то же время – перед вами, скорее всего, фальшивая информация. Отзывы об интернет-магазине читайте не на сайте самого интернет-магазина, а на сторонних ресурсах.

6. Обратите внимание на косвенные индикаторы фальшивой информации: требование обязательной предоплаты, недоступность самовывоза и отсутствие возможности оплатить покупку при получении. Три этих фактора должны насторожить вас и предупредить, что перед вами, возможно, мошеннический сайт.

7. Сравните цены перед покупкой. Обращайте внимание на цену товара 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. Проверьте 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 доверяйте «всплывающим» заманивающим баннерам, акциям с таймерами об окончании скидок, надписям «этот товар вместе с вами смотрят N человек» и другой подобной информации. Все эти приемы не должны подталкивать вас совершить покупку – сначала убедитесь, что сайту можно доверять.

10. Всегда держите включенным антивирус на компьютере и телефоне – это поможет избежать «заражения» вирусной троянской программой, позволяющей злоумышленникам обнулить ваш банковский счет.