СХЕМЫ, ИСПОЛЬЗУЕМЫЕ МОШЕННИКАМИ ДЛЯ ОБМАНА.

Схема 1. Ваш номер нужно подтвердить

Простейший обман, который чаще всего срабатывает. Идет звонок якобы от оператора сотовой связи. Мошенники пугают, что действующий договор на оказание услуг связи заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет собеседник. Достаточно продиктовать код из смс. На самом деле цель одна - получить доступ к аккаунту человека на Госуслугах.

Следующий шаг - перейти по присланной 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 там хранится.

Есть и другая цель, которую преследуют мошенники, представляясь оператором связи. Тот же звонок, но теперь с предложением по смене тарифного плана, подключением новых опций либо замены sim-карты. Чтобы это сделать, абонента просят продиктовать код из смс. С помощью этого кода злоумышленник получает доступ к личному кабинету пользователя на сайте оператора мобильной связи. 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.

Что делать? 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, размещенном на официальном сайте.

Схема 2. Предложения от лжеброкеров

Аферисты предлагают вам выгодно вложить свои средства, обещая процент гораздо выше, чем у банков. С потенциальными инвесторами они связываются через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое: нужно лишь открыть "брокерский" счет и инвестировать от 10 тысяч 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 криптовалюте. 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.

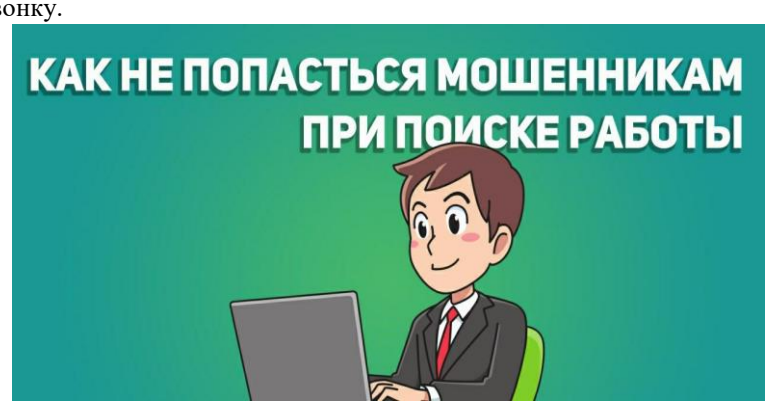
Вариант этой мошеннической схемы - участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают при помощи писем на электронную почту. Мошенники, оформляя сообщение, копируют визуальный стиль банка, для убедительности используя те же корпоративные цвета, логотип и другие элементы. Для участия в "выгодной" кампании предлагается перейти по ссылке.

После вам 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.

Как отличить мошенников от реальных брокеров? Проверьте сайт инвесткомпании 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.

Схема 3. Вам предлагают выгодную работу

Аферисты размещают лжевакансии на популярных сайтах объявлений. Зарплата привлекательная, условия работы заманчивые. Но нужно пройти собеседование с будущим работодателем, и мошенники предлагают сделать это онлайн по видеозвонку.



Либо Вам приходит предложение устроиться на очень интересную, легкую, а главное высокооплачиваемую должность. Получить его вы можете по электронной почте, по смс, а также в личных сообщениях в соц.сетях. Текст, естественно, различается, но суть его сводится к следующему: потенциальный работодатель где-то увидел Вас, и Вы ему настолько понравились, что он хотел бы сам предложить вам работу. Например, если вы где-то в соц.сетях оставляли комментарии, то мошенники могут сослаться на это: «Вижу, вы умеете грамотно и красиво общаться, отстаивать свое мнение», «Я вижу, что вы можете стать отличным кандидатом на эту должность» и т.д.

Чаще всего речь идет о менеджере маркетплейсов, реже – о сотрудниках интернет-магазина. В любом случае – ничего сложного, вы и именно вы прекрасно с этим справитесь вне зависимости от того, кем являетесь. Если вас заинтересовало предложение, то собеседник предложит продолжить общение в одном из популярных мессенджеров и пришлет вам ссылку на диалог.

Далее в дело вступают уже «HR-менеджеры» этой компании «Рога и копыта». На данном этапе Вам расскажут о простых обязанностях, которые отлично при этом оплачиваются, о том, что вы всему научитесь и никакая база не нужна, и, конечно же, о высокой зарплате и прочих плюшках.

Собеседование с будущим работодателем - волнительная процедура.

Во время онлайн-встречи мошенники пользуются растерянностью соискателей и крадут личные данные.

Под видом будущего работодателя они проводят собеседование, где просят кандидата заполнить анкету прямо во время зума.

Один из ее пунктов - номер карты и другие финансовые данные.

Такая информация им нужна якобы для перечисления зарплаты в будущем. Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия.

Также могут попросить внести вступительный взнос в размере, например, 500 рублей за регистрацию на маркетплейсе. Или еще для чего-нибудь – причины и сумма зависят от фантазии и наглости мошенников.

Понятно, что вместо пополнений с банковской карты соискателя в будущем происходят списания, а ни о какой работе естественно речи не идет. 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.

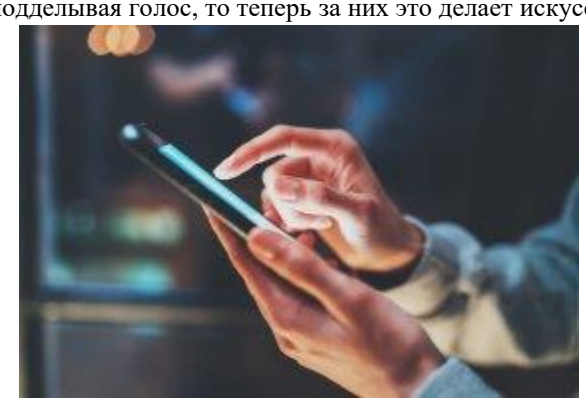
Дропперы (от английского drop - бросать, капать) - подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт. Часто человек даже не осознает, что вовлечен в преступную схему. Ведь объявление о работе, на которую он устраивается, не выглядит подозрительно.

Дропперы (от английского drop - бросать, капать) - подставные лица, задействованные в криминальных схемах по выводу средств с банковских карт жертв

Чего нельзя делать при трудоустройстве онлайн. 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 предлагает предоставить работодатель.

Схема 4. Друг просит о помощи

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



Аферисты взламывают аккаунт пользователя. Скачивают голосовые сообщения и на их основе генерируют монолог для дальнейшего обмана.

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

Как понять, что родственник фальшивый? 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.

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.

Как платить, чтобы не потерять деньги? Оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Схема 6. Звонки из банка

Наряду с лживыми угрозами об оформлении кредита на имя владельца банковской карты другим человеком или подозрительной операции по ней - появились и новые сценарии. Мошенники под видом специалистов техподдержки банков 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. Аферисты под видом сотрудников Банка России сообщают человеку, что кто-то пытается похитить деньги со счета. Чтобы их спасти, надо перевести средства на "безопасный" счет в ЦБ РФ. По легенде это временная мера - на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в приемной Банка России в Москве.

Как проверить звонок из банка? - Пользуйтесь только официальными ресурсами финансовых организаций. Если вам звонят сотрудники банка и разговор с ними кажется подозрительным, перезвоните на официальный номер, размещенный на сайте финансовой организации. Там же вы можете скачать официальные банковские приложения.

Схема 7. Представляются госслужащими

Часто мошенники звонят или пишут человеку якобы от лица сотрудников ФСБ, налоговой, портала "Госуслуги". Самая распространенная уловка - предложение получить какую-либо госвыплату. Схема классическая: вы нам данные карты, мы вам - деньги.

Есть и другой сценарий. Например, звонок от следователя или Росфинмониторинга с угрозой блокировки счета, по которому якобы зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф.

Что следует сделать? -Не верьте таким звонкам вообще. Поскольку ведомства не наделены полномочиями по аресту денежных средств и никогда не оказывают платных услуг по телефону или в мессенджерах.

Схема 8. Звонки сотрудников правоохранительных органов

Звонки фальшивых сотрудников «правоохранительных органов» под предлогом совершения несанкционированных операций со счетами – самая распространенная схема. В свете событий на СВО аферисты активно используют предлог совершения финансовых операций в адрес Украины или сообщают жертве, что ее родственник попал в плен, и для облегчения его участи необходимо совершить какие-либо финансовые операции.

Мошенники требуют действовать быстро, переводить деньги срочно и сохранять все в тайне.

Запомните: сотрудники правоохранительных органов никогда не будут требовать от вас совершить финансовые операции или предлагать по телефону возместить кому-то ущерб. Операции по поимке преступников в дистанционном режиме не проводятся.

Схема 9. Ваш родственник попал в ДТП

Потенциальной жертве звонит неизвестный и представляется сотрудником правоохранительных органов.

Затем следует краткое описание ситуации: ваш внук (или иной родственник) попал в аварию, он сильно пострадал (или ему грозит серьёзный тюремный срок).

Далее жертву ежеминутно держат «на крючке». Городской телефон при этом просят не снимать или вовсе отключить.

На вопрос, как можно уладить ситуацию, поступает мгновенный ответ - перевести существенную денежную сумму на определённый счёт или сами прийти по указанному адресу за деньгами.

Между делом трубка передаётся «внуку/сыну/дочери», который(ая) взволнованным, заплаканным голосом подтверждает своё положение.

Чтобы уберечь себя, не стоит изменять принципу «доверяй, но проверяй». Если некто звонит с неизвестного номера, представляется вашим родственником и утверждает, что попал в серьёзную ситуацию, то стоит сдержать эмоции. Спокойно выясните все нюансы ситуации. Если сомневаетесь, что говорите с родственником, спросите что-то, чего посторонний человек знать не может. Или просто положите трубку и позвоните близкому человеку по его обычному номеру.

Убедившись, что всё в порядке, незамедлительно позвоните в органы внутренних дел.