Основные способы мошенничества злоумышленников посредством IT-технологий:

Схема 1. Операторы сотовой связи

Под видом специалистов известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту человека на «Госуслугах».

- 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.

Предупреждение: помните, что 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

Обещание легких денег многих привлекает. 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 и даже зарегистрировать его в Минфине России, 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.

Под удар попадают не только будущие инвесторы, но и те, кто уже давно в этой области. Мошенники под видом финансовых организаций предлагают «разблокировать» активы, замороженные иностранными учетными институтами. Именно об этом сценарии недавно рассказал Банк России. Для того чтобы вернуть средства, злоумышленники просят перевести оплату на счет компании, якобы оказывающей такие услуги. Цена помощи – сумма, равная стоимости замороженных активов. Далее аферисты обещают, что инвестор сможет получить эти деньги на свой банковский счет в двойном размере.

Предупреждение: помните о простых правилах, которые помогут не попасться на удочку инвестиционных мошенников:
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.

Стоит ли говорить, что 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. Варианты работы могут быть разные. Например, будущему дропперу могут предложить вывести деньги с якобы замороженных счетов банков, попавших под санкции, на свой. Жертва

соглашается, ей переводят ранее уже похищенные средства, она снимает их в банкомате. Небольшой процент оставляет себе в виде ежемесячного дохода, остальное – как и договаривались – отдает. А после становится звеном преступной цепи и будет привлечена к уголовной ответственности.

Предупреждение: 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 «безобидный» 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.

Предупреждение: 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.

Предупреждение: оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Схема 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 и новые сценарии. Мошенники под видом специалистов техподдержки финансовых организаций предлагают

установить на смартфон приложение для поиска вирусов. Существует ли оно на самом деле? Нет. 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 жертве о том, что кто-то пытается похитить деньги с ее 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. Для убедительности жертве отправляют смс с подтверждением записи с официального номера регулятора – 300. За сентябрь 2023 года с жалобами на потерю средств в результате такой мошеннической схемы обратилось несколько десятков пострадавших, отмечает регулятор.

Предупреждение: 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 найти ссылки на официальные банковские приложения и скачать их.

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.

Предупреждение: 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.