Удочка для легковерных

Продолжаем цикл публикаций о том, как максимально обезопасить себя и свой кошелек. По мере совершенствования системы кибербезопасности растут и возможности аферистов, которые придумывают все новые способы обмана.

Минобрнауки России предупреждает о продолжающихся атаках телефонных мошенников на сотрудников научных и образовательных организаций. В зоне риска – старшее поколение. И хотя злоумышленникам практически не удается ввести людей в заблуждение, даже единичные случаи заставляют серьезно отнестись к данной проблеме.

Телефонные мошенники непрерывно меняют стратегию: отправляют вредоносные ссылки, звонят якобы из банка с просьбой назвать код из СМС, используют для звонков мессенджеры (Телеграм, WhatsApp и др.), применяют шантаж, давят на жертву от имени ректора, представителя ФСБ или МВД. Могут применяться технологии подмены номеров и подделки голосов, упоминаться личные сведения о человеке, побуждающие снизить порог критического восприятия.

Что делать, если вам поступил звонок, в подлинности которого вы не уверены? Незамедлительно завершить беседу. Проинформировать своего непосредственного руководителя о факте подозрительного обращения. Попробовать проверить личность контакта – если звонящий или пишущий с неизвестного номера представился вашим знакомым, свяжитесь с ним по актуальному номеру.

Практически ни одна мошенническая схема не обходится без применения социальной инженерии. Методы игры на слабостях и страхах обычного человека позволяют преступникам найти беспроигрышный подход, чтобы добиться желаемого - похитить деньги, персональные данные, продать бесполезное, ввести в заблуждение относительно истинного умысла своих действий.

Давайте подробнее определим, на какие уловки мошенников можно попасться сейчас?

Сгустить краски. Мошенник убеждает, что все деньги обесценятся/заморозятся "из-за обвала рубля и западных санкций". Любые предложения "спасти" накопления - обман. Если внезапно возникший "финансовый аналитик", знакомый со связями или лжегосслужащий уговаривают немедленно перевести деньги на якобы безопасный счет, поменять деньги на новые, обменять валюту по старому курсу - это мошенник, ваши "спасенные" деньги окажутся у него.

Подобные предложения часто транслируются через соцсети, мессенджеры или электронную почту. В заманчивых сообщениях нередко используют имена известных людей, якобы цитаты из законодательства, мошенники нагнетают ситуацию и пугают последним вагоном (сейчас или завтра будет поздно).

Все это - элементы социальной инженерии, нацеленные на то, чтобы потенциальная жертва поддалась панике и не имела возможности и времени оценить такое предложение здраво, собрать дополнительную информацию. Спасение одно - бежать подальше и помнить, что любые финансовые решения нельзя принимать под сторонним эмоциональным давлением, в спешке, поддавшись панике.

"Близкие в беде". Беженцы, больные дети, голодные животные - все те, кому необходима помощь, не оставляют равнодушными многих людей. И это нормально. Но именно на этих чувствах построен лжефандрайзинг. Как обезопасить себя от удочки "на жалость"? Помогать лишь в том случае, если информация достоверна: личное знакомство с нуждающимся в помощи или наличие официального подтверждения беды.

Нельзя доверять смазанным фото неких документов или душещипательным историям в соцсетях. Лучше оказывать помощь тем, кого знаешь лично, или официальным благотворительным организациям.

Еще одна схема - звонок или сообщение "из органов" или от "родственника" о том, что близкий человек совершил административное или уголовное правонарушение (сбил пешехода, участвовал в несанкционированном митинге и т.п.) и нужно заплатить, чтобы не заводили дело. Этот старый способ, известный многим.

Аферисты чаще выбирают для таких новостей пожилых людей. Желание спасти близкого человека, страх и растерянность - все это может лишить здравомыслия и не дать критически оценить ситуацию. Нужно объяснять своим пожилым родственникам, что любую информацию необходимо сначала проверять.

Эффект халявы. Не следует верить сообщениям о срочной распродаже товаров в связи с закрытием магазина или ликвидацией. Часто такие предложения поступают в форме рассылки, в которой содержится ссылка для перехода на фейковый ресурс. В надежде купить телефон или компьютер по "выгодной" цене можно вовсе остаться без денег на счете. Помните, никто не будет торговать себе в убыток.

Никогда не нужно переходить по присланным ссылкам - именно так можно занести на свой девайс вирус, похищающий личные данные. Ссылка также может выглядеть как картинка или кнопка.

К подобным схемам часто прибегают мошенники на таких популярных сайтах, как "Avito": например, продавец срочно и дешево продает квартиру, потому что "уезжает из страны". Находится такой человек, как правило, не в городе покупателя, а в командировке, в больнице и т.п. Документы в наличии, но нужен аванс, обычно не слишком значительный - 1-3% от стоимости, чтобы "я уже не предлагал никому".

Отправив аванс, можно попрощаться с деньгами. Все сделки купли-продажи заключаются очно, требуют письменного оформления, в том числе подтверждения внесения аванса.

Нередко предлагают быстро разбогатеть. Сценарий обычно такой: в "Телеграме" создается канал, в котором сначала размещаются успешные схемы заработка, отчеты о баснословных доходах, лайфхаки. После привлечения подписчиков объявляется набор на "курс обучения", но мест ограниченное количество, разумеется, надо срочно записываться.

В стремлении обладать эксклюзивной информацией о заработке, люди переводят деньги, но получают либо бесполезные и общедоступные сведения, либо просто прощаются со своими средствами, потому что курс так и не состоялся.

Помните, "секретные" способы заработка не продаются (зачем о них рассказывать всем, если можно так хорошо зарабатывать). Более того, можно не только потерять деньги, но и свободу, если деятельность незаконна.

Преступники, как правило, примерно понимают, какие люди поддадутся влиянию, а какие - нет. К сожалению, сегодня практически невозможно не попасть в списки к таким мошенникам - мы сами нередко оставляем в открытом доступе информацию о себе: об имущественном положении, семье, отдыхе, заработке, заполняем анкеты в магазинах и точках продаж и многое другое.

Кроме того, злоумышленники постоянно придумывают новые уловки, меняют схемы обмана, а иногда возвращаются к старым, хорошо забытым способам. Предусмотреть их все невозможно, но это и не нужно. Абсолютное большинство методов преступников разобьются о банальную внимательность, осторожность, критическое мышление, базовые принципы финансовой безопасности и понимание, на каких чувствах и слабостях обычно играют мошенники.

Счета в "надежных банках". Такое мошенничество появилось не сегодня, сменились лишь аргументация - теперь жертве предлагают таким образом скрыть доходы и накопления в "далеких валютных офшорах".

Схема обмана: мошенники запускают страницу веб сайта якобы "банка", организовывают горячую линию кредитной организации. Открыть счет предлагается только удаленно и жертву убеждают в надежности тем, что находятся вне контроля мегарегулятора - Банка России, ИФНС и прочих надзорных органов.

Результат "открытия" таких счетов - гарантированное похищение личных и персональных данных (в том числе - реальных банковских) плюс кража денежных средств.

Какую информацию требуют аферисты? Данные паспорта - по словам "представителя банка" эта информация необходима для присвоения индивидуального кода счета (без имени), данные существующих банковских счетов/карт). Мошенники предупреждают, что для безопасности деньги на новый "счет" будут поступать через посредника.

Вводя в заблуждения клиента в процессе переговоров, они говорят, что могут потребоваться смс или пуш-уведомления (для "подтверждения транзакции" на созданный "счет"). Каждый раз мошенники могут придумывать новые уловки с одной целью - добраться до сбережений жертвы. Однако далее наступает череда проблем: что-то идет не так, "нужно немного подождать", сложности с переводом ввиду санкций, проверка платежа, необходимость открыть еще один "резервный счет" и т.д.

Правила финансовой безопасности

Цифровые финансовые услуги включают методы электронного хранения и перевода средств, осуществления и получения платежей, займа, сбережения, страхования и инвестирования средств, а также управления финансами дистанционно. Это удобно, но при использовании данных инструментов существенно возрастает риск финансового мошенничества. Для безопасного использования цифровых финансовых услуг необходимо придерживаться следующих рекомендаций.

- Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах.
- Желательно подключить СМС-уведомления по используемой банковской карте и электронному кошельку и отслеживать движение и остаток средств.
- Не допускайте посторонних к банковской карте, электронному кошельку, мобильному телефону и компьютеру.
- ПИН-код нужно помнить, не записывать нигде в явном виде, никому не говорить, никогда не вводить в интернете, прикрывать рукой при вводе в терминале.
- При пользовании банкоматом проявляйте осторожность, обращайте внимание на посторонних вокруг и на подозрительные устройства и накладки в местах ввода ПИН-кода и карты.
- Используйте сложные и разные пароли, регулярно меняйте их, никому не сообщайте и не пересылайте по электронной почте и в СМС.
- Не сохранять пароли и личные данные в интернет-сервисах.
- Желательно использовать режим "инкогнито" (приватный) при совершении покупок через интернет. Удаляйте информацию о платежах с помощью очистки буфера файлов (cache) и файлов сохранения данных (cookies).
- Избегайте смс-платежей на короткие номера для оплаты интернет-услуг и переводов непроверенным получателям.
- Не реагируйте на сообщения якобы от банка или платежной организации, предлагающие перерегистрироваться, повторно ввести данные, перезвонить и т.п.
- Незамедлительно сообщайте в платежную организацию, если кошелек "взломан", карта потерялась, данные карты стали известны посторонним или с нее без согласия держателя списаны деньги.
- Не передавайте банковскую карту посторонним - ее реквизиты (номер карты, срок действия, имя владельца, CVV/CVC-код) могут быть использованы для чужого интернет-платежа или оплаты покупок в магазине.
- Запомните, ни один сотрудник банка не имеет право запрашивать номер вашей карты, трехзначный номер с обратной стороны карты или код-подтверждения из СМС. Всеми этими данными банк располагает.
- Помните, что на любой банковской карте указан телефон горячей линии банка, куда можно обратиться.