Появились новые виды телефонного мошенничества

На удочку анонимных преступников попался уже каждый десятый россиянин!

О том, как защититься от телефонных мошенников и какие самые распространенные уловки они используют, в интервью KP.ru рассказал директор Научно-исследовательского финансового института при Минфине России Владимир Назаров.

«НЕСТАРЕЮЩАЯ» КЛАССИКА РАЗВОДОВ

- Владимир Станиславович, похоже, телефонные мошенники снова активизировались — мне во всяком случае звонить стали чаще, причем не только «сотрудники банков», но и «полицейские»...

- Мы постоянно обращаем внимание на рост атак и, скажем так, на их оригинальность и изворотливость. Действительно, если раньше мошенники прикидывались работниками банков, то сейчас большинство звонков – это от якобы сотрудников МВД. Просим не верить им на слово, не сообщать номера карточек, а уж тем более CVV-код и уж, конечно, не переводить деньги — даже если вас будут убеждать, что вы участвуете в спецоперации.

По данным ВЦИОМ, в последние полгода половина россиян сталкивалась с телефонными мошенниками, а каждый десятый перевел им деньги. За первые четыре месяца этого года число кибермошеничеств выросло больше, чем на четверть. Средний «чек» в прошлом году составил 13,9 тысячи рублей. А самым крупным было хищение 400 млн рублей, это была целая операция, которую преступники вели несколько дней.

- На какие «сюжеты» люди попадаются чаще всего?

- Один из самых популярных - звонок якобы из службы безопасности банка. Клиенту сообщают о подозрительной операции и предлагают быстро решить проблему: перевести деньги на якобы безопасный счет, либо назвать конфиденциальную информацию – пароли из СМС и push-уведомлений, CVC\CVV-коды.

Сейчас у мошенников стала популярна новая версия этой схемы: они представляются сотрудниками правоохранительных органов и предупреждают граждан, что на их имя собираются оформить кредит. Цель преступников не меняется: либо выведать личные данные, либо заставить перевести деньги на мошеннический счет.

Не устаревает схема «крика о помощи» в соцсетях. Мошенники получают доступ к чужому аккаунту и от имени этого человека начинают рассылать сообщения вроде «срочно, помоги, попал в аварию!» или «очень некогда, мама в реанимации, кинь немного денег» и прочие истории. Люди часто не могут отказать, когда близкий человек в беде, к тому же в этом случае просят небольшую сумму. Если вы получаете такое сообщение, то необходимо связаться с человеком другим способом – лучше всего позвонить и спросить, правда ли то, что случилось. И уже тогда принимать решение о помощи. Но, как показывает статистика, в большинстве случаев якобы попавший в аварию человек спокойно сидит дома.

Практически всегда «в тренде» фишинговые сайты — двойники популярных интернет-магазинов или порталов по оказанию услуг. Для совершения покупки посетителей просят ввести данные карты или провести платеж с помощью электронного кошелька или прямого перевода. Распознать обман непросто, ведь подобные сайты практически полностью копируют оригинал. Как правило, подобные ресурсы существуют недолго, поэтому создаются за несколько дней или недель до использования. Обратите внимание на дату создания и, если она вызывает подозрение, стоит проверить подлинность ресурса, на котором вы собираетесь совершить платежную операцию.

Еще одна прибыльная для мошенников история – это выманивание денег на инвестиции. Навязчивая реклама, обещание сверхдоходности, высокотехнологичный и малопрозрачный бизнес, который якобы совсем скоро взорвет рынок – вот основные признаки обмана.

НЕ ВЕРЬ, НЕ БОЙСЯ, НЕ ПЛАТИ

- А есть ли новые способы мошенничества?

- Мошенники практикуют все более сложные и часто гибридные схемы дистанционного хищения. Например, сейчас в соцсетях набирает обороты целый мошеннический проект, в котором на первом этапе запускается фальшивое видео, так называемый дипфейк, с призывом от известной персоны получить подарок или совершить выгодную покупку. А затем пользователям дается ссылка на фишигновый сайт, где введенные ими платежные данные становятся собственностью злоумышленников.

В преступных целях активно эксплуатируется тема коронавируса. Мошенники предлагают доверчивым гражданам на особых условиях получить медицинскую помощь, материальную поддержку, различные виды компенсации.

Для этого рассылают соответствующие электронные письма с применением государственной символики и названиями крупных российских банков. При переходе по ссылке на фальшивый сайт, человек заполняет заявление, вводит необходимые личные данные и реквизиты карты, включая код CVC. Располагая необходимой платежной информацией, мошенники спокойно списывают чужие средства.

Активно отрабатываются схемы обмана на площадках интернет-сервисов с объявлениями о продаже товаров и услуг. Мошенники используют разные варианты с оплатой перед покупкой, внесением аванса, запросами платежных данных.

Совсем недавно была раскрыта крупная мошенническая схема. Злоумышленники размещали на популярных интернет-площадках объявления о продаже объектов

недвижимости, премиальных автомобилей или товаров повышенного спроса. Заинтересовавшихся просили перед сделкой подтвердить платежеспособность. Для этого им нужно было совершить денежный перевод своему родственнику или знакомому с помощью определенной системы платежей, а потом отправить квитанцию о финансовой операции преступникам. Таким образом мошенники собрали личные данные граждан, изготовили на их имена поддельные паспорта, а затем посещали кредитные организации и снимали деньги со счетов ничего не подозревающих граждан. Сейчас преступники задержаны, но сама схема может получить распространение.

- Сейчас полным ходом идет отпускной сезон. Можно ли наскочить на мошенника при покупке путевок, билетов? Что должно насторожить?

- Да, можно. И потому мы всегда призываем быть очень бдительными, когда люди покупают билеты и путевки через сайты, а это фактически 90% населения. Наибольшую активность такие мошенники проявляют в период праздников или отпусков. Например, в этом году только перед майскими праздниками злоумышленниками было создано порядка пятидесяти фишинг-сайтов с возможностью онлайн-покупки туристических продуктов и авиабилетов.

Обычно такие ресурсы либо маскируются под всем известные туристические компании и агрегаторы, либо позиционируют себя как только что вышедшие на рынок турфирмы.

Клиентов заманивают ценами ниже рынка, различными акциями для раннего бронирования, подарками, скидками и даже кэшбэком. В реальности же у них крадут деньги или личную информацию.

Защититься поможет простая внимательность. Проверьте, входит ли компания, у которой вы хотите купить турпродукт, в единый федеральный реестр туроператоров. Вбейте ее название в поисковик. Проверьте, действительно ли вы находитесь на ее официальном сайте. Различия между оригинальным ресурсом и подделкой могут заключаться в одной букве или символе в адресной строке. Обратите внимание на дату создания сайта. Как правило, сайты-призраки появляются незадолго до наступления туристического сезона.

Если вы путешествуете самостоятельно, всегда проявляйте осторожность при аренде недвижимости или транспорта, особенно если наткнулись на крайне выгодные предложения на сайтах объявлений и форумах. Очень часто злоумышленники просят перевести им аванс, а затем просто перестают выходить на связь.

ЗЛОУМЫШЛЕННИКИ ОСВОИЛИ QR-КОДЫ

- Сейчас широкое распространение получили QR-коды. Мошенники уже используют их в своих схемах?

- Конечно. Нередко злоумышленники распространяют ложные рекламные материалы, к которым прикреплен заведомо опасный QR-код. Обычно это предложения скидок, каких-то щедрых акций или товаров по очень низким ценам.

Иногда мошенники просто клеят поверх настоящих QR-кодов свои. Например, это может произойти в кафе или ресторанах. Вы думаете, что сейчас подключите бесплатный wi-fi или

перейдете на раздел с меню, а в реальности попадаете на поддельный сайт, где происходит передача платежных данных клиента преступникам, либо производится платежная операция, в результате которой деньги пользователя уходят в карман злоумышленников. Надо признать, что автоматическое списание средств по QR-коду происходит довольно редко. Обычно вы попадаете в форму оплаты услуги, где вместо реквизитов реальной организации вводятся реквизиты мошенников. Поэтому перед тем как согласиться с операцией всегда проверяйте эту информацию и при сомнениях запрашивайте у получателя дополнительные данные. Кроме того, сейчас есть мобильные приложения, с помощью которых можно проверить безопасность QR-кода.

- *Как не стать жертвой мошенника?*

- Соблюдать принципы финансовой гигиены. Первый - регулярно обновляйте операционную систему вашего компьютера или телефона, скачивайте приложения только из официальных магазинов, проверяйте состояние гаджета с помощью антивируса.

Второй - не размещайте финансовую информацию о себе в открытых источниках. Настройте двухфакторную аутентификацию в приложениях, к которым привязана ваша карта. Кстати, для покупок в интернете, лучше использовать отдельный «пластик». Можно, например, завести виртуальный. Старайтесь пользоваться проверенными и защищенными сайтами. Не переходите по ссылкам из рассылок в почте, на которые вы не подписывались. При финансовых операциях используйте мобильный интернет, а не открытые общественные сети wi-fi. Будьте внимательны, если для оплаты используются ссылки и QR -коды. Обязательно обратите внимание на реквизиты получателя, особенно если они заполняются автоматически.

Третий принцип, наверное, наиболее сложный. Это привычка критически мыслить, когда вы рассматриваете финансовые предложения или когда вам поступают какие-либо звонки. Чаще всего мошенники используют нашу жадность, страх потерять деньги, невнимательность, оказывают моральное давление. Никогда не принимайте важных финансовых решений поспешно. Если от вас просят что-то сделать с вашими деньгами «срочно!», то скажите, что вам надо подумать или просто повесьте трубку. Перезвоните по официальному номеру в банк или государственную организацию, сотрудником которой вам представились, и узнайте все там спокойно и без спешки.

Автор: Владимир ПЕРЕКРЕСТ