Киберпреступность. Новые виды.

**Схема 1. Ваш номер нужно подтвердить.**

Простейший обман, который чаще все срабатывает. Идет звонок якобы от оператора сотовой связи. Мошенники пугают, что действующий договор на оказание услуг вязи 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 представляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе, которая там храниться.

Есть и другая цель, которую преследуют мошенники, представляясь оператором связи. Тот же звонок, но теперь с предложением по смене тарифного плана, подключения новых опций либо замены cim –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 в таком случае советуют 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.

**Схема2. 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 инвестиционных компаний. Предложение заманчивое: нужно лишь открыть «Брокерский» счет и инвестировать от 10 т. р. 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» возникней желание вывести деньг со счета, начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счет еще раз на определенную сумму, оплатив «страховку». Или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя, чтобы можно было «обналичить» средства. В итоги инвестор теряет свои деньги, а заодно и надежду на будущие миллионы.

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

После вам предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи, а также дадут доступ к специальному предложению. А уже там понадобиться ввести данные своей банковской карты – с нее аферисты потом спишут деньги.

Как отличить мошенников от реальных брокеров. Проверьте сайт инвестиционной кампании ил брокера. Обратите внимание на реквизиты и наличие лицензии Банка России. Откажитесь от услуг, если 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 типа «Авито». Зарплата привлекательная, условия заманчивые. Но нужно пройти собеседование с будущим работодателем, и вам предлагают сделать это онлайн по видеозвонку.

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

Понятно, что вместо пополнения 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.

Дропперы (от английского drop – бросать, капать)- подставные лица, которые задействованы 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.

Чего нельзя делать при трудоустройстве онлайн. Внимательно изучайте предложение от будущего работодателя и отзывы о нем. Не ведитесь на обещания быстрого заработка с минимальной тратой собственного времени. Главное следите за данными, доступ к которым предлагает предоставить работодатель.

**Схема 4. Друг просить помощи.**

Еще одна тактика кибермошенников- рассылка сообщений с просьбой одолжить денег близким или друзьям. Порой в своих сценариях мошенники заходят дальше -играют на чувствах человека и сообщают, что его родственники попал в беду. Если раньше аферистам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за это делает искусственный интеллект. Аферисты взламывают аккаунт пользователя. Скачивают голосовые сообщения и на них основе н-генерируют монолог для дальнейшего обмана.

Как понять, что родственник фальшивый. Не переходите по неизвестным ссылкам., даже если получили их от знакомых. Договоритесь с родственниками пароле или секретном вопросе, который нужно назвать, если разговор покажется подозрительным.

Прокурор Мантуровского района О.В. Праведников