Новые схемы киберпреступлений

В настоящее время растет киберприступность и существует несколько основных мошеннических схем.

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 одно- 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 операций 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 там уже он настраивает переадресацию звонков с номера жертвы на свой. Это делается для того, чтобы в дальнейшем подтвердить разного рода операции: вывод средств с банковских карт абонента, оформление на него кредита.

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 что сложно. Нужно пополнить счет еще раз на определенную сумму, оплатить «страховку».

Как отличить мошенников от реальных брокеров? Проверьте сайт инвесткомпании или 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 якобы нужна 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.

Вместе с тем, при таких операциях можно нарушить закон, став дроппером. Дропперы – 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.

Чего нельзя делать при трудоустройстве онлайн. Внимательно изучайте предложения от будущего работодателя. Не видитесь на обещания большого заработка с минимальной затратой собственного времени. И главное, следите за данными, доступ к которым предлагает предоставить работодатель.

Прокурор Фатежского района А.Н. Минаков