**Внимание!!! Виды интернет-мошенничества.**

Схемы мошенничества в сети давно называют классическими, о них регулярно предупреждают и кажется, все уже в курсе происходящего. Но даже такая огласка злоумышленникам не помеха. Запущенные когда-то механизмы обмана совершенствуются, адаптируются и продолжают работать. Проблема в том, что ключевым здесь остаётся фактор человеческий и, к сожалению, сотрудникам милиции неподконтрольный: доверчивость людей – именно в этом кроется причина большинства киберпреступлений.

По-прежнему не теряет позиций вишинг. Так называемый разговорный жанр: когда с человеком беседуют напрямую. Мошенник звонит в один из мессенджеров и представляется, специалистом службы безопасности банка либо сотрудников правоохранительных органов. Цель - получить от владельца платёжной карты конфиденциальную информацию, а вместе с тем и доступ к управлению счётом. Или же мотивировать человека лишиться денег самостоятельно: перевести их на счёт злоумышленника либо оформить кредит. Сегодня об этом не слышал разве что ленивый, но как показывает практика, знание не всегда гарантия защиты.

Практически все, кто становится жертвой мошенников, осведомлены. Однако, конкретно в момент общения с преступником: разволновались, растерялись, поверили. Многие объясняют своё поведение тем, что c толку сбивает доброжелательность и «компетентность» злоумышленников. Разговаривая с приятным и вежливым человеком, который оперирует терминами и даже некоторыми личными данными, обращается по имени и отчеству – они не замечают подвоха.

Со слов пострадавших, по телефону всё звучит очень правдоподобно. Вот и думают, что на этот раз их точно не обманывают, а наоборот, хотят помочь. Например, якобы остановить списание денег со счёта. То есть мошенники предлагают «спасти» от мошенников – сегодня весьма распространённая ситуация. Пользуясь тем, что люди переживают за свои сбережения, на них и делают акцент. Человека застают врасплох и пугают: рассказывают о подозрительных банковских транзакциях, о том, что с его карты снимают деньги или оформляют кредит – и предлагают срочно это прекратить.

Скорость, кстати, тоже имеет значение и является одной из уловок. Всё происходит быстро, сразу много вопросов, поток информации - анализировать некогда, сделать паузу не выходит, как и положить трубку, отказавшись от любого рода услуг. И человек начинает следовать инструкциям. Предоставляет реквизиты карты, пароли, которые направляются системой дистанционного банковского обслуживания в смс-сообщениях, паспортные данные. А уже имея такие сведения, злоумышленник может не только украсть деньги, но и оформить онлайн-кредит.

Но и это не предел. Особые методы срабатывают и офлайн. Когда люди идут в банк самостоятельно и по «рекомендации» аферистов берут кредит. Причём, и банков и кредитов может быть несколько. Два-три дня «клиента» держат на крючке, постоянно поддерживая связь и координируя действия. В итоге круглая сумма ложится на счёт мошенников: наличные обманутые должники переводят через инфокиоск. Доходит до того, что ради займа в город приезжают даже из сельской местности.

 Такая схема актуальна сейчас для лжемилиционеров. Звонят, представляются сотрудниками правоохранительных органов и призывают совместными усилиями, опять же, разоблачить интернет-мошенников, поучаствовать в «спецоперации». Иногда просят жертву никому о секретном задании не сообщать, угрожая при этом уголовной ответственностью.

В качестве подтверждения отправляют фото поддельного удостоверения в мессенджер, используют профессиональную лексику или какие-то данные о реальных сотрудниках милиции, которые можно найти в открытом доступе. Как правило, в разговоре участвуют несколько аферистов, раздают указания друг за другом. Такая цепочка даёт больший эффект, как бы придаёт важности разговору, убеждает в правдивости, да и в целом не даёт человеку опомниться и отойти от телефона.

**Представители банка и правоохранительных органов не используют мессенджеры для общения с гражданами!**

**Если вам поступил подобный звонок – прекратите разговор и сообщите об этом в милицию.**

Перейти по вредоносной ссылке, ввести данные карты на поддельном сайте или поучаствовать в фейковом розыгрыше – ещё не полный список того, на что может попасться любой интернет-пользователь. Востребованность онлайн-решений сегодня – преимущество для мошенников. Доступность платежей в сети теперь популярна не только с точки зрения удобства, но и как инструмент обмана и краж.

Злоумышленники хорошо изучили рынок и быстро подстраиваются под изменения. Один из способов – эксплуатация известности и в целом надёжности некоторых маркетплейсов, порталов или сайтов различных магазинов: «Куфар», «21vek.by», «Остров чистоты».

В мессенджере предлагают купон с дополнительной скидкой, расширенную программу лояльности, участие в акции и т.п. Всё, что для этого нужно – перейти по ссылке и ввести данные карты, в том числе CVV/CVC код. После чего все средства скорее всего исчезнут со счёта.

Имитацию действительно очень сложно отличить от настоящего ресурса: всё сходится, кроме пары символов в адресе сайта - вот здесь требуется повышенное внимание. Именно в связи с такой обстановкой необходимо иметь отдельную карту для оплаты товаров и услуг, чтобы крупные суммы на ней не хранились. Ведь изначально мошенники работают вслепую, и пока не проделают ряд манипуляций, баланс они проверить не могут.

Хотя сейчас даже условные пять копеек на карте не всегда являются сдерживающим фактором. Например, имея удалённый доступ к управлению гаджетом и владея реквизитами карты, злоумышленники могут оформить кредит уже без участия владельца. То есть даже не придётся озвучивать пароли, которые придут от банка: мошенник увидит их благодаря удалённому доступу. Чтобы получить его, подставной специалист банка предложит установить «приложение безопасности», оно и позволит ему дистанционно управлять рабочим столом вашего телефона или компьютера.

Бывает, мошенники предлагают воспользоваться службой доставки. Отправляют продавцу ссылку на фишинговый сайт, допустим, «Европочты», и когда тот вводит реквизиты карты – деньги уходят.

**Рекомендуем:**

используйте специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещение сомнительных сайтов;

не реагируйте на сообщения от неизвестных отправителей: высока вероятность того, что это спам или мошенники;

не переходите по подозрительным ссылкам и не открывайте вложения;

при покупке/продаже товара общайтесь в личных сообщениях непосредственно на сайте. Не ведите переписку в мессенджерах и не переходите по ссылкам, если вам их прислал потенциальный продавец/покупатель;

не сообщайте третьим лицам паспортные данные, коды из СМС-сообщений банка или ресурса, где Вы осуществляете продажу или покупку, CVV/CVCкод на обратной стороне банковской карточки.

*Старший оперуполномоченный группы по противодействию кибер преступности криминальной милиции Могилевского РОВД* ***Фурманов Владислав Владимирович***