**ОСТОРОЖНО - МОШЕННИКИ!**

**Внезапный звонок телефонного мошенника - это прекрасная возможность застать человека врасплох, не оставить ему время подумать и выманить данные карты или побудить жертву самостоятельно перевести деньги. Телефонное мошенничество - целая индустрия со своими колл-центрами, четким разделением труда и отшлифованными методами социальной инженерии.**

**"СОТРУДНИК БАНКА"**

Представляясь специалистом банка (как правило, службы безопасности), для убедительности мошенник называет вас по имени, говорит, что у вас есть вклад или карта представляемого им банка. В последнем им помогает теория вероятности: у многих имеются карты крупнейших банков, можно легко угадать и "попасть в цель".

Распространены звонки из "службы безопасности" банков. Незнакомец сообщает, что с вашей карты пытались снять деньги в другой части России или что кто-то вошел в ваш личный кабинет. Далее есть несколько сценариев: мошенник может попросить вас сообщить данные карты, код из СМС или установить приложение на ваш смартфон по присланной им ссылке. Все эти сценарии ведут к одному исходу - злоумышленники похитят ваши средства. Сразу бросайте трубку. Мошенники играют на нашем страхе потерять деньги: в минуты стресса мы делаем быстрые и необдуманные решения.

Если раньше такие звонки поступали с незнакомых номеров, то теперь мошенники могут звонить и с номера банка, подделывая его с помощью IP-телефонии. Эта технология позволяет подставить любой номер во время звонка. "Разрешить свои сомнения о том, кто звонит, достаточно просто - перезвоните. Ведь IP-телефония работает только в одну сторону. Если вы перезвоните, то точно попадете в банк. Просто помните, что сотрудники банка никогда не звонят вам с просьбой передать данные банковской карты и других кодов, а также установить на ваш телефон какие-либо программы".

**"ДРУГ или РОДСТВЕННИК"**

Эта схема почти такая же старая, как мир: вам приходит СМС с просьбой о помощи: "Я попал в беду, переведи деньги на этот номер…" Деньги близкому человеку нужно перевести именно срочно - задача мошенников в том, чтобы у жертвы не было возможности подумать или посоветоваться. Такой способ уже кажется примитивным, но сегодня эта схема усложняется использованием IP-телефонии. "Позвонить могут и с номера друга или родственника, если он стал известен мошенникам. В основном мошенники осуществляют звонки на стационарные номера телефонов и тихим голосом общаются с жертвой, при этом в телефонной беседе мошенник поясняет, что попал в ДТП и у него имеются повреждение лица и поэтому речь у него тихая и невнятная. Каким бы ни было сообщение, нужно взять себя в руки и перезвонить близкому человеку.

**"БЕСПЛАТНЫЙ ПОМОШНИК"**

Мошенник представляется сотрудником какой-либо финансовой или правозащитной организации и предлагает проверить кредитную историю, составить кредитный рейтинг. "Консультация" бесплатна, а вот за конкретную услугу мошенник может запросить приличную сумму. Нужно помнить, что два раза в год проверить свою кредитную историю можно бесплатно. "Рекомендация, когда вам предлагают "бесплатную" помощь, может быть одна: возьмите паузу, проверьте информацию или посоветуйтесь с близкими".

*Если сегодня в новостях говорят о социальных выплатах или компенсациях, то уже завтра мошенники могут ссылаться на эти виды поддержки.*

Такие мошенники могут сообщить, что ваша кредитная история ухудшилась, и предложить услуги по ее "улучшению". "Бывает, что в кредитной истории появляются долги по ошибке, но в таком случае внесение изменений бесплатно. Если же это действительно ваши долги, то улучшить историю можно, погасив их".

**"ПОКУПАТЕЛЬ по ОБЪЯВЛЕНИЮ"**

Онлайн-объявления стали для мошенников прекрасным предлогом для развода. Они могут позвонить и сообщить о готовности приобрести ваш товар, а для этого запросить данные вашей карты, включая CVV-код (трехзначный код на оборотной стороне) или даже проверочный код из СМС. Расчет в том, что вы не знаете, что для перевода денег на карту достаточно только ее номера. Такие мошенники могут также прислать ссылку для ввода данных из СМС, ссылаясь на сервисы доставки или оплаты сайтов онлайн-объявлений. Ссылка может быть похожа на официальную и содержать название этого агрегатора объявлений.

**Важно знать**

Ключевые правила безопасности.

Соблюдая элементарные правила, можно обезопасить себя от потерь, ненужных разбирательств с банком и плохого настроения:

1. Никогда и никому не сообщайте ваши персональные данные, а также данные карты, CVV-кода (трехзначный код на оборотной стороне) или проверочный код из СМС.

2. Если вам звонят с предложением перечислить денег (субсидию, пенсию, государственную поддержку), не торопитесь радоваться. Лучше проверьте сами, положена ли вам такая выплата, и оставьте заявку на официальных ресурсах.

3. Никогда не торопитесь с ответом и не бойтесь положить трубку, ведь второпях вами правят эмоции, а не разум! Перезвоните сами в банк или родственникам/друзьям, чтобы убедиться, что все в порядке.