ДИСТАНЦИОННЫЕ МОШЕННИЧЕСТВА:

КАК НЕ СТАТЬ ЖЕРТВОЙ ОБМАНА

УМВД РОССИИ ПО ГОРОДУ ТЮМЕНИ
ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ И БАНКОВСКИХ ТЕХНОЛОГИЙ

Статистика телефонного мошенничества

- В 2023 году в России было зарегистрировано более 15 млн звонков гражданам от телефонных мошенников. Это превратилось в целую отрасль преступного бизнеса, с четкими правилами и хорошо налаженными процессами. Чаще всего мошенники звонят в разгар рабочего дня, когда жертвы заняты и не сосредоточены. Многие такие «колл-центры» работают с территорий стран ближнего зарубежья - Украины (60% звонков), Казахстана, Армении. Другая часть мошенников работает из мест лишения свободы.

Способы телефонного мошенничества

Для обма на мошенники используют один и тот же набор техник и приемов:

- Внезапность информации.
- Срочность выполнения действий («только сейчас»).
- Непрерывность взаимодействия («все время на связи»).

Схема воздействия на человека едина:

1) **Напугать** (шокировать)
2) **Раскачать** на эмоции, дезориентировать
3) **Втереться в доверие**.
4) **Обмануть** - вынудить к желаемым действиям.

Секретные технологии на службе у мошенников

Мошенники используют механизмы манипуляции и обмана в сочетании с психологическими уловками. Нередко мошенников специально обучают использованию техник НЛП (нейролингвистического программирования) и даже трансовым методикам. Это прежде всего речевая подстройка под «клиента» : мошенник подстраивается под ваши темп, громкость, ритм речи, выявляет слова-маркеры, налаживает контакт; создает «якоря» - чувство страха, растерянности.

Психологи или преступники?

Мошенники – чаще всего люди **высокой профессиональной подготовки**, члены организаций, нанимающих профессиональных психологов, которые «натаскивают» их на разговоры с людьми. Часто они используют агрессивные психологические манипуляции, перед которыми сложно устоять. Они говорят **спокойным и ровным голосом**, создают убедительный шумовой фон (имитация работы банка), они **вежливы, тактичны и убедительны**.

1. Шок:«Пугай-спасай»

- Самый распространенный приём мошенников - сразу же повергнуть человека в ШОК сообщаемой информацией, напугать: «На ваше имя взяли кредит в размере миллион рублей», «Ваш сын попал в ДТП», «С вашей карты пытаются снять деньги», и пр. **В этот момент происходит резкий вброс адреналина в кровь, критическое мышление притупляется, человеком руководит СТРАХ. Начинается суета, паника.** Далее Вам предлагается выход из ситуации, «спасение» (дать взятку за непривлечение к ответственности родственника, перевести деньги на безопасный счет, взять кредит и пр.).

2. Авторитет: «Я есть власть!»

Мошенники обращаются к авторитету государственных структур и представляются: сотрудниками банка, сотрудниками службы безопасности, сотрудниками силовых структур (ФСБ, полиции, прокуратуры, налоговой), социальной защиты, опеки, медицины, пенсионного фонда и пр.). Расчет на то, что не поверить представителю власти невозможно!

3. Спешка: почему вас постоянно торопят?

Мошенники задают много коротких вопросов, постоянно торопят вас, чтобы не дать сосредоточиться и подумать. Создают ощущение срочности и спешки, иначе… вот-вот спишут деньги с карты, вот-вот вашего сына посадят в тюрьму , вот-вот на вас уже оформляется кредит….Мошенник торопится создать ЯКОРЬ - ему нужно как можно быстрее вывести вас из психологического равновесия

4. Доверие

Мошенники могут старательно убеждать вас в своей компетентности , называя вас по имени отчеству, называя ваши паспортные данные, место регистрации. **Могут звонить с телефонов, которые похожи на телефоны районных отделов полиции или популярные сервисные номера банка**. Например, номер Сбербанка «900» пишут как 9ОО (9 и две буквы О), выглядит очень похоже. Они могут представляться «важными» должностями, которые точно должны внушить доверие

5. Всё время в контакте: почему вас не отпускают со связи?

Мошенники просят Вас постоянно быть на связи, ехать в банкомат (в банк), не прерывая разговор, выполнять операции в личном кабинете в режиме онлайн - **чтобы постоянно держать вас под контролем**, продолжать психологическое воздействие на вас, не дать возможности опомниться и проанализировать ситуацию.

Попытка всё время держать в вами связь – всегда признак мошенничества!

Итак, обобщим тревожные сигналы:

Что должно Вас насторожить:

1. Чужой незнакомый номер, особенно не вашего города (региона).
2. Спешка, требование незамедлительно принять решение (срочно!).
3. Связь с деньгами (всегда в итоге речь зайдет о деньгах, неважно с какой ситуации начат разговор).

Можно ли победить в схватке с профессиональным мошенником?

Конечно, можно.

Даже несмотря на то, что психологическая подготовка мошенников, как правило, в разы выше, чем знания и умения простого гражданина. **Цель мошенников – завладеть вашими деньгами**. Ваша цель –сохранить ваши деньги и не выполнить требования мошенников. Для этого нужно соблюдать **простые правила**.

Шаг № 1. Замри: делаем паузу

В психологии описываются три известные инстинктивные реакции на стресс: бей, беги, замри. В данной ситуации прежде всего – ЗАМРИТЕ - остановитесь. Что бы вам ни говорили, чем бы вас ни пугали, какие бы советы «срочно принять меры» не давали, СДЕЛАЙТЕ ПАУЗУ. Глубоко подышите, сделайте 5-7 глубоких вдохов и выдохов. Это поможет снять эмоциональное и физическое напряжение и сконцентрироваться. Главное – не принимать никаких решений и не сообщать информацию, которую у вас просят.

Шаг № 2. Беги: уходим от контакта

Прервите разговор на начальном этапе. Можете не быть вежливым и просто отключиться.

Можете сказать: «Я сейчас не могу говорить, перезвоните позже». И отключайтесь.

Не принимаем никаких решений и не сообщаем никакую информацию, которую у вас просят.

Шаг № 3. Действуй: проверяем информацию

Звоните в ваше отделение банка, если вам говорили о сомнительных операциях по вашей карте.

Заходите в личный кабинет банка, смотрите историю операций. При необходимости блокируете карты (звонком в ваш банк либо через приложение). Звоните родственникам, если речь была о ДТП, задержании и пр. с участием якобы ваших близких. Звоните в службы 112 или 02.

Шаг № 4. Поддержка

Если вдруг вы не соблюдали эти правила и поверили якобы сотруднику «ФСБ» или «службы безопасности банка», то, прежде чем бежать в банк за кредитом, или к банкомату , расскажите об этом родственнику, другу, соседу, коллеге. Если вдруг вам мошенники сказали, что еще перезвонят, пригласите кого-нибудь, чтобы присутствовали при разговоре.

На практике нередки случаи, когда именно этот шаг спасал жертв мошенников от преступления!

Не бойтесь опозориться или показаться глупым – уж лучше показаться глупым, чем долгие годы выплачивать многомиллионные кредиты, взятые в пользу мошенников

Самые популярные вопросы

1.Откуда у мошенников мои данные?

У нас слишком много организаций, **где хранятся личные данные граждан в электронном виде**. Начиная с обычных магазинов, где мы оформляем скидочные и накопительные карты, заканчивая банками, сотовыми операторами, государственным фондами. Эти базы, к сожалению, могут оказаться в руках злоумышленников. Часто по номеру мобильного телефона можно узнать, как вас зовут (Сбербанк в приложении покажет имя и отчество, Тинькофф - имя и первую букву фамилии). Номер карты тоже многие сбрасывают по мессенджерам. Начиная от родительских чатов заканчивая сбором денег в социальных сетях.

Самые популярные вопросы

2.Какие способы мошенники используют чаще всего для обмана с картами/счетами?

Самый частый сейчас способ мошенничества: ***позвонить и представиться сотрудником банка/полиции/ФСБ.***
Для вас могут разыграть целый **спектакль по ролям**:
сотрудник банка –сотрудник службы безопасности-сотрудник полиции.
Поводы: «Ваша карта заблокирована», «Нам нужно уточнить ваши данные - была попытка смены номера телефона, привязанного к карте», «Подтвердите перевод с карты», «Вам пришел перевод на 100 тысяч рублей», «На ваше имя оформляется кредит». Количество вариантов зависит от фантазии организаторов схемы.

Самые популярные вопросы

2.Какие способы мошенники используют чаще всего для обмана с картами/счетами?

Мошенники постоянно придумывают все новые и новые способы обмана. В 2024 году наиболее популярными видами дистанционного мошенничества стали следующие схемы:

Самые популярные вопросы

2.Какие способы мошенники используют чаще всего для обмана с картами/счетами?

- *ЗВОНОК ОТ ОПЕРАТОРА СОТОВОЙ СВЯЗИ:*
- *«У ВАС ЗАКОНЧИЛСЯ СРОК ДЕЙСТВИЯ СИМ-КАРТЫ»*

Мошенники звонят жертве и утверждают, что действующий договор заканчивается и надо его продлить, иначе ваш номер отдадут другому абоненту. И все так удобно, что даже ходить никуда не надо, все можно сделать по телефону.

Достаточно продиктовать код из СМС!

Этого ни в коем случае делать нельзя – так вы предоставите мошенникам данные для входа в личный кабинет портала ГОСУСЛУГИ

Самые популярные вопросы

2.Какие способы мошенники используют чаще всего для обмана с картами/счетами?

«ЗВОНОК ОТ ОПЕРАТОРА СОТОВОЙ СВЯЗИ»

Не называйте никаких данных по телефону и не отправляйте никакие коды

Обновляйте персональные данные лично в офисе оператора связи или в личном кабинете на ОФИЦИАЛЬНОМ ПОРТАЛЕ ОПЕРАТОРА

Самые популярные вопросы

2.Какие способы мошенники используют чаще всего для обмана с картами/счетами?

«ОПЛАТА УСЛУГ ПО ФЕЙКОВОМУ QR коду»

Такой лже-код, отправленный мошенниками, ведет не на официальный сайт сервиса, а на поддельный ресурс, через который у вас похищают и деньги, и данные карты.

ОПЛАЧИВАЙТЕ УСЛУГИ ТОЛЬКО ЧЕРЕЗ ОФИЦИАЛЬНОЕ ПРИЛОЖЕНИЕ СЕРВИСА, А НЕ ЧЕРЕЗ КАМЕРУ ГАДЖЕТА

Самые популярные вопросы

2.Какие способы мошенники используют чаще всего для обмана с картами/счетами?

«ПРЕДЛОЖЕНИЯ ОТ ЛЖЕБРОКЕРОВ»

Мошенники предлагают открыть брокерский счёт и инвестировать туда деньги. Предлагают установить приложение, в котором как будто бы видно как растет ваш баланс. Это обман. Как только вы захотите «вывести» деньги с этого счета, - возникнут проблемы.

Самые популярные вопросы

3.У меня нет денег, значит я никогда не стану жертвой мошенников?

К сожалению, нет.

На практике имеет место огромное количество случаев, когда жертв обманом склоняют брать многотысячные, а часто и многомиллионные кредиты, которые потом потерпевшие годами вынуждены выплачивать. «На вас кто-то оформляет кредит, поэтому нужно срочно его оформить Вам и перевести на безопасный счет, чтобы вернуть в банк».

Поэтому от мошенников не застрахован никто.

Самые популярные вопросы

4. Могут ли у меня списать деньги, если я никому ничего диктовать не буду?

К сожалению, такие случаи бывают и относятся к случаям интернет-мошенничеств. Но они не происходят сами по себе, а требуют также ваших неправильных действий - в данном случае, это проход по вирусной ссылке.

Это не менее распространенный метод мошенничества, называемый «ФИШИНГ» (от англ. Fish - рыба), обозначающий , что вас «поймали на удочку». Чаще всего этот вид мошенничества встречается при покупке либо продаже товаров на популярных ресурсах АВИТО, ЮЛА (под видом «безопасной сделки»). Не проходите ни по каким незнакомым ссылкам и не вводите там данные своих карт.

Самые популярные вопросы

4. Какие еще есть способы обмана в интернете, без прямого контакта с мошенниками?

Не менее популярный вид мошенничества в интернете - сайты-дублеры. Маскируются под официальные сайты популярных компаний, например: «М-видео», Додо пицца, Авиалинии, РЖД. С первого взгляда не отличишь. Похожее цветовое оформление, реквизиты и даже IP адреса (отличающиеся на одну букву или цифру). Вы сами вводите данные карты, производите оплату, и ваши деньги уходят мошенникам. Здесь очень важно обращать внимание на любые мелочи! Заказывайте через официальное приложение (если вы постоянный покупатель). Если выбрали способ покупки через сайт - сравните несколько ссылок, найдите реальный официальный сайт. Не торопитесь!!!

Самые популярные вопросы

5. Какие еще есть способы обмана в интернете, без прямого контакта с мошенниками?

Наиболее популярный вид **мошенничества в отношении государственных служащих** - создание фейковых (поддельных) аккаунтов в телеграмм, Вотсапп под именем руководителя организации (директора школы, главного врача поликлиники). Человек думает, что общается со своим руководителем, и так или иначе разговор сводится к банковским картам, счетам и переводам денег под разными предлогами.

НЕ ТОРОПИТЕСЬ! Не стесняйтесь перезвонить руководителю на ИЗВЕСТНЫЙ вам номер, либо его заместителям или коллегам.

****

ВСЕГДА ПОМНИТЕ ПРАВИЛА, О КОТОРЫХ МЫ СЕГОДНЯ ГОВОРИЛИ

РССКАЖИТЕ О НИХ СВОИМ БЛИЗКИМ

СПАСИБО ЗА ВНИМАНИЕ !