НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.

Телефонный номер-«грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

Простой код от оператора связи: предложение услуги или другой выгоды - достаточно ввести код, который на самом деле спишет средства с Вашего счёта.

Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.

Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

ТУЙМАЗИНСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА

НАПОМИНАЕТ:

В СЛУЧАЕ, ЕСЛИ ИМЕЮТСЯ ОСНОВАНИЯ ПОЛАГАТЬ, ЧТО В ОТНОШЕНИИ ВАС ПЕРДПРИНИМАЮТСЯ МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ, ЛИБО ВЫ УЖЕ СТАЛИ ЖЕРТВОЙ МОШЕННИЧЕСТВА НЕОБХОДИМО НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАТЬСЯ В ОТДЕЛ МВД РОССИИ ПО ТУЙМАЗИНСКОМУ РАЙОНУ ПО АДРЕСУ г. ТУЙМАЗЫ, ул. МИЧУРИНА 3, А ТАКЖЕ В ТЕРРИТОРИАЛЬНЫЕ ПРЕДСТАВИТЕЛЬСТВА КРЕДИТЫХ ОРГАНИЗАЦИИ, ЕСЛИ БЫЛИ ИСПОЛЬЗОВАНЫ БАНКОВСКИЕ КАРТЫ

О ФАКТАХ МОШЕННИЧЕСТВА СООБЩАЙТЕ ПО ТЕЛЕФОНАМ

8 (34782) 7-21-02

ДЕЖУРНАЯ ЧАСТЬ ОМВД РОССИИ ПО ТУЙМАЗИНСКОМУ РАЙОНУ РБ

ПРОКУРАТУРА ИНФОРМИРУЕТ

Телефонное мошенничество известно давно - оно возникло вскоре после массового распространения домашних телефонов.

В настоящее время, когда личный номер мобильного телефона может быть у любого члена семьи, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества множатся с каждым годом.

В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях.

Мошенники разбираются в психологии и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении.

Списание денег со счета без ведома владельца, кража паролей и ПИН-кодов, легкий заработок в интернете и вклады под невероятные проценты, онлайн-казино — все это виды финансового мошенничества. Преступники будут спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или государственные организации, чтобы выманить деньги.

И всё-таки как распознать мошенника?

Рассмотрим мошенничество с банковскими картами и кибермошенничество.

Мошенничество с банковскими картами

Одна из самых распространенных сфер деятельности мошенников связана с банковскими картами. Это объясняется, прежде всего, их широким распространением.

Пример: Галина Н. зашла на сайт своего банка, чтобы совершить платеж за коммунальные услуги по кредитной карте. По неизвестной причине программа выдавала ошибку. Через несколько минут на мобильный телефон раздался звонок. Звонивший представился сотрудником банка, сообщил, что на сервере ведутся профилактические работы, и попросил ввести в окошко сайта данные карты, чтобы вручную открыть доступ к личному кабинету. Галина честно выполнила все указания, но войти на сайт так и не получилось. «Сотрудник банка» порекомендовал войти на сайт через два часа. Через два часа зайдя в личный кабинет, Галина обнаружила, что с ее кредитного счета произведено несколько переводов в пользу неизвестного частного лица в том же банке. Банк заблокировал карту, но при этом Галина должна была вернуть «взятые» деньги с кредитной карты.

Для того чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV. Они могут установить скиммер на банкомат (специальное устройство, которое накладывают на приемник карты в банкомате) и видеокамеру над клавиатурой.

Номер CVC или CVV — три цифры, расположенные на поле для подписи владельца карты или рядом с ним. Это проверочный код подлинности, дополнительные цифры которого нанесены на банковскую карту.

Достаточно один раз воспользоваться таким банкоматом и не прикрыть рукой клавиатуру в момент набора ПИН-кода — и ваши деньги могут снять, перевести на несколько счетов и обналичить. Украсть данные вашей карты могут даже в кафе или магазине. Злоумышленником может оказаться продавец, который получит доступ к вашей карте хотя бы на пять секунд. Сфотографировав вашу карту, он сможет воспользоваться ей для расчетов в интернете.

Меры безопасности

- Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
- Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.
- Подключите мобильный банк и СМС-уведомления.
- Если совершаете покупки через интернет, никому не сообщайте секретный код для подтверждения операций, который приходит вам по СМС.
- Старайтесь никогда не терять из виду вашу карту.

Кибермошенничество

Допустим, вы всегда снимаете деньги только в кассе банка, а картой и вовсе не рассчитываетесь. Вы чувствуете себя в безопасности. Вдруг вам приходит СМС или письмо якобы от банка со ссылкой, просьбой перезвонить по неизвестному номеру или с уведомлением о неожиданном крупном выигрыше. Или звонят от имени банка и просят сообщить личные данные, ПИН-код от карты или номер СМС-подтверждения. Или пишут в социальных сетях от имени родственников или друзей, которые внезапно попали в беду (угодили в полицию, сбила машина, украли сумку) и просят перевести энную сумму денег на неизвестный счет. В 99,9% случаев вы имеете дело с мошенниками. За ссылками, скорее всего, таятся вирусы, на другом конце провода — специалисты по обману, которые всеми правдами и неправдами хотят выманить необходимые им данные, а по ту сторону экрана — злоумышленники, которые играют на ваших желаниях, чувствах и заботе о близких.

Основные каналы, по которым мошенники могут взаимодействовать со своей жертвой:

- Электронная почта.
- Сайты.
- Соцсети и мессенджеры.
- Программы и приложения.
- Телефонный звонок и СМС.

Меры безопасности

- Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.
- Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили,