***Самые популярные способы мошенничества с банковскими картами***

1. **Мошенники представляются работниками банка - э**то свежая схема обмана, которая набирает большую популярность у мошенников. Человеку изначально поступает СМС с номера 900 (сервисный номер Сбербанка), в котором неизвестное лицо просит перевести ему некоторую сумму денег, которая спишется со счета жертвы, если в ответном сообщении отправить присланный цифровой код, либо операция будет подтверждена автоматически через 600 секунд. Человек естественно ошарашен от такой безвыходной ситуации. И тут начинается самое интересное…

Вдруг раздается телефонный звонок с официального номера Сбербанка (8-800-555-5550), на другом конце провода мужчина, который обращается к жертве по имени и сообщает, что его пытаются обмануть мошенники.  А он, как специалист службы безопасности банка, должен разобраться и помочь в этой проблеме. Далее сотрудник «Сбербанка» говорит, что надо остаться на линии, написать ответ на сообщение — код, который там указан, вставить пробел и слово — «отмена перевода». После этого деньги, вместе со специалистом службы безопасности банка, бесследно исчезают.

P.S. На вопрос, может ли мошенник позвонить, прикрываясь номером Сбербанка, да так, чтобы и при обратном звонке, и в детализациях звонков был указан именно этот номер, представители сотовых компаний не скрывают, что такое технологически сделать можно.

1. **Еще одна распространенная схема - ж**ертва **размещает объявление о продаже какого-либо товара на одном из популярных сайтов объявлений** и становится прицелом для мошенников. Звонит покупатель и говорит, что готов приобрести продаваемую вещь. Далее он сообщает, что находится в другом городе и готов произвести оплату на карту, а за покупкой отправит курьера из транспортной компании. Жертва пересылает мошеннику номер своей банковской карты, а также все паспортные данные, так как они нужны транспортной компании. Через некоторое время поступает звонок с номера, которому все привыкли доверять — 8-800-555-5550 (официальный номер Сбербанка). Голос: «Здравствуйте.
Я сотрудник службы безопасности Сбербанка. На Ваш счет поступил перевод в размере (называет сумму). Так как сумма большая, требуется подтверждение. Вам на телефон была отправлена смс с кодом подтверждения. Если вы мне её назовете, то сумма сейчас зачислится на ваш счет». Жертва верит и предоставляет мошеннику всю информацию, после чего все деньги с карты исчезают.

**3. Мошенничество с помощью беспроводного терминала и бесконтактной технологии PayPass - з**лоумышленники снимают деньги у пассажиров с помощью беспроводного терминала через одежду и стенки сумок. Посредством бесконтактной технологии PayPass с карточки без PIN-кода можно снять до 1000 российских рублей. К несчастью, подобные воришки вполне могут заполонить места массового скопления народа. Чтобы снять деньги со счета, достаточно приложить устройство к карману или сумке, считыватели бесконтактных карт работают на расстоянии до двадцати сантиметров, достать их проблем не составляет.

Уязвимость бесконтактных карт можно снизить с помощью «шапочки из фольги», точнее, кошелька. Условно говоря, если Вы положите карту в фольгированный пакет, специальный радиоэкранированный кошелек или металлическую коробочку, транзакцию провести будет нельзя.

**И не забывайте о методах мошенничества с банковскими картами, которые стали уже классическими. Вот некоторые из них:**

**\*Скимминг - э**то кража данных карты при помощи специального считывающего устройства (скиммера). Злоумышленники копируют всю информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания срока ее действия, CVV- и CVC-код), узнать ПИН-код можно с помощью мини-камеры или накладок на клавиатуру, установленных на банкоматах.

Стать жертвой скимминга можно не только снимая наличные, но и оплачивая покупки в торговых точках.

**\*«Мама, у меня проблемы, не звони, переведи деньги на этот счет» - д**аже если Ваш ребенок сидит на диване рядом с Вами, Вы испугаетесь, получив такое сообщение. Так уж устроены родители: они беспокоятся о своих детях, и реакция на возможную угрозу им очень сильна. А если Ваш ребенок где-то в городе? Простая, эффективная и наглая схема, использующая сильные чувства и базовые, фундаментальные инстинкты.

**\*Фишинг - п**реступники создают сайты, похожие на официальные интернет-страницы кредитных организаций, на которых предлагают клиентам оставить конфиденциальную информацию о себе. Другой вариант — рассылка по почте или с помощью СМС фальшивых сообщений от банков с просьбой предоставить номера карт.

Получив эту информацию, мошенники крадут деньги с карт.

 ***Будьте бдительны! Не дайте себя обмануть!***

***Если Вы стали жертвами мошенников сообщите об этом в правоохранительные органы.***

Заместитель Слободского

межрайонного прокурора И. М. Докучаев