

Как СОХРАНИТЬ СВОИ ДЕНЬГИ от МОШЕННИКОВ?

С каждым годом количество методов хищения денежных средств мошенниками увеличивается. Как не попасть «на крючок» злоумышленникам и избежать потерю денежных средств? – расскажем про самые распространенные методы.

Фишинг - это вид интернет-мошенничества, который используют для получения доступа к личной информации пользователя: **логинам, паролям, номерам телефонов, данным банковских карт** и так далее.

Скимминг - технология кражи данных банковской карты для последующего изготовления её копии. Классический скимминг подразумевает взаимодействие устройства злоумышленников с картой жертвы. То есть вы должны вставить её в скомпрометированный банкомат или платёжный терминал.

Интернет – мошенничество – хищение денежных средств с банковских карт часто осуществляется **через интернет**. Способов существует несколько:

- перехват данных банковской карты при совершении крупных покупок в сомнительных интернет-магазинах,
- вирусы-«диверсанты», которые встраиваются в операционную систему компьютера и подменяют данные при совершении оплаты,
- вирус-троян. Действует аналогично предыдущему виду, но в отличие от него изменяет не реквизиты для оплаты, а саму страницу сайта, на которую заходит владелец карты и совершает оплату.

По телефону – злоумышленники представляются должностными лицами: полиции, ФСБ, сотрудниками безопасности банка и т.д.

Данные методы являются основными, но не единственными!

Правила, которые помогут отличить мошенника

Мошенники – всегда представляются:

- **Сотрудниками банка: службой безопасности, технической поддержкой. Информировуют о событиях:**

- Хищения денежных средств,
- «Взломом» личного кабинета,
- Подтверждении перевода,
- Смене номера телефона,
- Просят коды с СМС-уведомлений,
- Уточняют личную информацию и т.д.



Противодействие

Сотрудники банка НИКОГДА не проводят подобных операций и не просят персональные данные и коды из уведомлений! **Рекомендуется НЕ ВЕСТИ РАЗГОВОР И НЕ БРАТЬ ТЕЛЕФОН НА ЗВОНКЕ!**

- **Сотрудниками правоохранительных органов (МВД, ФСБ, Следственный комитет, участковый и т.д.)**

- Сообщают о хищении персональных данных,
- О возбуждении уголовного дела на Вас (как подозреваемого или свидетеля) или на Вашего родного/близкого за совершение преступления,
- Просят сообщить Ваши персональные данные, коды с СМС-уведомлений, заплатить «взятку» и т.д.



Действующие сотрудники правоохранительных структур всегда направят Вам Почтовый ящик с подтверждением. **Рекомендуется СРАЗУ ПРЕКРАТИТЬ РАЗГОВОР И НЕ БРАТЬ ТЕЛЕФОН ПРИ ПОВТОРНОМ ЗВОНКЕ!**

- **Притворяются Вашим родным и близким по телефону, СМС – сообщениям, социальным сетям. Просят:**

- Совершить финансовую операцию (перевести денежные средства, взять кредит и т.д.),
- Проголосовать за участника в конкурсе перейдя по ссылке,
- Помочь финансово (одолжить денежные средства) до заработной платы, прекращения уголовного преследования, на приобретение дорогостоящих покупок,
- Помочь в решении проблемы, так как попал в беду



Рекомендуется СОЗВОНИТЬСЯ С РОДНЫМИ ИЛИ БЛИЗКИМИ ЧЕЛОВЕКОМ ЛИЧНО ДЛЯ ПОДТВЕРЖДЕНИЯ ИНФОРМАЦИИ/ не проходить по ссылкам!

Устанавливайте приложения только с официальных источников

Данные методы являются основными, но не единственными! Будьте бдительны!