Схемы мошенничества, это:

1. Внедрение на компьютер жертвы вредоносной троянской программы либо манипулирование по телефону методами социальной инженерии
2. Получение информации о персональных данных, номерах счетов и карт
3. Получение дубликата sim карты в офисе оператора по поддельному паспорту, водительскому удостоверению, нотариальной доверенности
4. Мониторинг финансовых потоков жертвы, выбор момента совершения преступления
5. Использование дубликата sim карты в телефоне мошенников, перехват сообщений
6. Хищение средств и перевод их на банковские счета, карты, счета мобильных телефонов или электронные кошельки, контролируемые мошенниками
7. Снятие наличных денежных средств либо покупка товаров и услуг для последующей перепродажи. Также представлен пример sms, e-mail-фишинга.

Мошенники используют широковещательные рассылки, зачастую от имени банка

С электронных счетов и карт у россиян уводят по 1 млрд. рублей в год! И часто преступникам помогают сами держатели банковских карт. Ведь большинству кажется, что с ними такого произойти не может. Еще как может.

Молодёжная модельная библиотека «25 квартал»
г. Орёл, ул. Рощинская,25
тел. 33-04-86,
E-mail: orel_lib8@orel-region.ru

Как обезопасить свою банковскую карту : памятка / МКУК ЦБС г. Орла, Молодёжная модельная библиотека «25 квартал» ; сост. : О. А. Черниговцева ; ред. Е. В. Семенихина, Л. В. Демичева, Г. М. Соковых. – Орел, 2022. – 2 с.

Муниципальное казённое учреждение культуры «Централизованная библиотечная система города Орла»
Молодёжная модельная библиотека «25 квартал»

Как обезопасить свою банковскую карту

ПАМЯТКА

16+

Орёл 2022

1. Не сообщайте никому постороннему секретные данные вашей карты: CVV (три цифры на обороте) и пин-код

Единственное, что могут спрашивать у вас сотрудники колл-центра, - это кодовое слово. Но это происходит лишь в том случае, если вы звоните в банк, а не наоборот.

2. Оставляйте как можно меньше личной финансовой информации в интернете

Не публикуйте в социальных сетях фото банковской карты или сканы документов. Желательно даже не упоминать, клиентом какого банка вы являетесь.

3. Установите двухфакторную идентификацию

Чтобы при заходе в онлайн-банк и проведении операций нужно было не только ввести постоянный пароль, но и подтвердить свое решение одноразовым паролем, который приходит по смс.

4. Используйте для покупок в интернете отдельную банковскую карту

5. Не переходите по подозрительным ссылкам

Иначе можно скачать себе вирус, который передаст все финансовые сведения мошенникам. Скачивайте только официальные приложения банков в AppStore и Google Play. Их легко определить по общему числу скачиваний. У официального приложения крупного банка не может быть несколько сотен скачиваний. Обычно речь идет о десятках тысяч.

6. Используйте сложные пароли

Желательно, чтобы они были разными для разных устройств и ресурсов. Плюс желательно время от времени менять их.

7. Если вам стали приходить странные смс, похожие на банковские, сразу же звоните в банк

Сообщение может выглядеть так: «Подтвердите перевод на 1000 рублей. Код доступа - 56854». Если вы не инициировали эту операцию, значит, кто-то подобрал пароль к онлайн-банку и пытается вывести деньги с вашего счета. Главное – звонить по официальному номеру банка, указанному на оборотной стороне карты, а не по тому номеру, который указан в сообщении.

8. Если вы поняли, что потеряли карту или что данные вашей карты могли попасть к мошенникам, лучше не искушать судьбу и заблокировать карту

Это можно сделать либо в мобильном приложении банка, либо позвонив в колл-центр. Если через полчаса вы найдете карту в кармане пальто, можно так же быстро ее разблокировать и отменить перевыпуск новой карты.