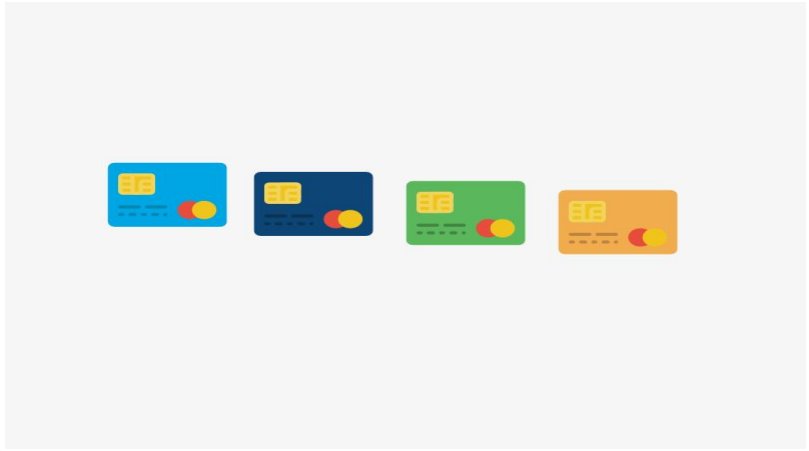


Проект на тему:

«Защити себя и близких от мошенников»

Актуальность проблемы

- В 21 веке в современном мире насчитывается свыше миллиарда банковских карточек. Карточки постоянно совершенствуются, растет сфера их применения, расширяется поле оказываемых услуг по их использованию. Однако банковские пластиковые карточки, как всякий высокодоходный бизнес (особенно в сфере денежного обращения), давно стали мишенью для противоправных посягательств.

Цели проекта:

- Расширение знаний о банковских картах и безопасности их использования;
- Раскрытие технических способов мошенничества.

Задачи:

- Способствовать просвещению учащихся школ и их родителей по безопасному использованию банковских карт;
- Распространять сведения о видах мошенничества и какие действия необходимо предпринимать обманутым пользователям банковских карт.

Операция «Пин-код»

В прошлом году мошенники украли с банковских карт россиян 961 миллион рублей. Это на 114 миллионов (или 10,6%) меньше, чем годом ранее. Всего за год было совершено 317 178 краж: именно такое число приводится в обзоре Центра мониторинга и реагирования на компьютерные атаки FinCert, опубликованном на сайте Центробанка России. Отметим, что, помимо безналичной оплаты покупок в интернет-магазинах, злоумышленники физически опустошают чужие карточки в банкоматах. Для этого им часто достаточно одного лишь пин-кода.

Мошенники-максималисты

Надо сказать, что пин-код интересует не всех мошенников: некоторым из них нужна сама карта. Для ее получения в картоприемник банкомата устанавливается специальный конверт из пленки, в котором карта застревает. Смирившийся со своей участью владелец карточки уходит, а злоумышленник извлекает конверт. Этот способ называется «ливанская петля».

Если банкомат не отдает карту, немедленно позвоните в банк и заблокируйте кредитку. Если к вам подойдут «помощники», ни в коем случае не вводите при них пин-код.

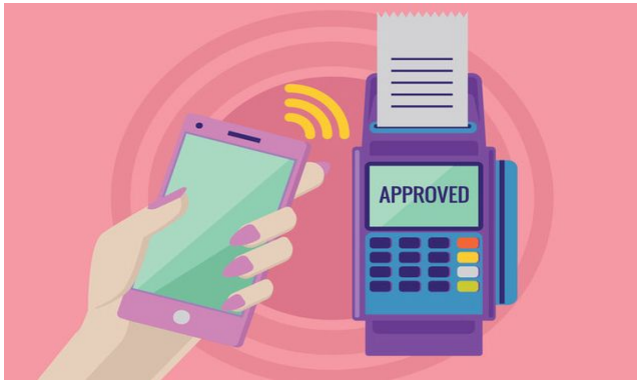
Эволюция пирато.

Последние изобретения мошенников, ворующих деньги с карт

Прогресс в области кражи средств с банковских карт не стоит на месте: охотники за чужими финансами регулярно придумывают новые способы наживы. Несмотря на то, что в прошлом году объём несанкционированных операций с карточками россиян сократился (с 1,15 млрд рублей в 2015 году до 1,08 млрд в 2016), количество таких транзакций, по данным Центробанка, растёт.

СМС-Мошенники

- **По данным Центробанка, в нашей стране продолжает процветать мошенничество с помощью SMS-сообщений.**



В минувшем году также эволюционировали способы мошенничества с помощью SMS-рассылок. Приходит SMS с текстом: «По вашей карте совершена покупка и заблокирована определённая сумма, позвоните по такому-то номеру» После того, как владелец карты связывается со злоумышленниками, они пытаются выяснить номер его карточки, счёта, CVC-код и прочие данные. Как правило, SMS-рассылками занимаются лица, находящиеся в местах лишения свободы, что мешает расследованию преступлений.

Обналичивают чужие карты

- В России также растёт количество операций с использованием банковских карт без согласия их владельцев, о чём предупреждает Банк России. Речь идёт о новом виде мошенничества с банковскими картами.
- «Неизвестные лица размещают объявления о приобретении платёжных карт или обращаются непосредственно к держателям карт с предложением купить у них эти карты. Затем карты используются для осуществления несанкционированных операций», — сообщает регулятор.
- Мошенники, практикующие эту схему, используют чужие пластиковые карты для обналичивания денег, полученных преступных путём, или для вывода средств, украденных в интернет-банке или из электронных кошельков. В ЦБ отмечают, что раскрываемость подобных преступлений низкая.

Признаки потенциально опасного интернет-магазина

1

Низкая цена

Стоимость товаров в магазине мошенников зачастую существенно ниже, чем в других. Не следует поддаваться на слова «акция», «количество ограничено», «спешите купить» и т.д.

2

Отсутствие курьерской доставки и самовывоза:

В этом случае нередко приходится вносить предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара.

3

Отсутствие контактной информации и сведений о продавце:

Если на сайте прописаны только форма обратной связи и мобильный телефон продавца, такой магазин может представлять опасность. Перед обращением сюда следует почитать отзывы в интернете.

4

Подтверждение личности продавца посредством направления покупателю скана его паспорта

Документ, особенно отсканированный, легко подделать.

5

Отсутствие истории у продавца или магазина

Потенциально опасными являются страницы, зарегистрированные пару дней назад

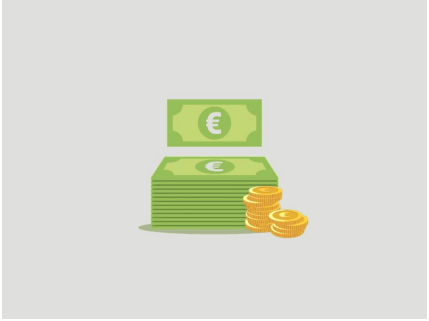
6

Неточности и несоответствия в описании товаров

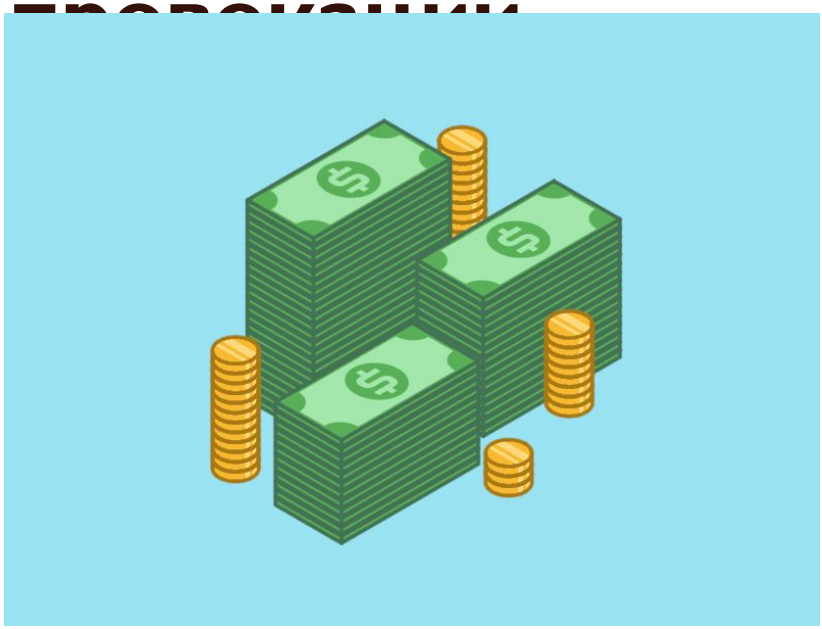
Желательно почитать описания такого же товара на других сайтах.

Заработок мошенников

- Ещё один способ заработка мошенников — округление валюты при использовании интернет-банкинга. Об этом говорится в сообщении компании Positive Technologies. Простые граждане от этого метода не страдают: действия «пиратов» затрагивают банки.
- Схема выглядит следующим образом: банковские правила таковы, что при конвертации валют сумма округляется до двух знаков после запятой. Допустим, владелец счёта переводит в доллары 29 копеек. При курсе американской валюты в 65 рублей сумма в 29 копеек соответствует 0,004461 доллара. При конвертации она округляется до 0,01 доллара. После этого мошенник переводит 1 цент обратно в рубли и получает 0,65 копеек. Получилось, что на одной операции он заработал 36 копеек. Как выяснили эксперты, с помощью этой схемы можно получить до 15 тысяч рублей в месяц.



Методы мошенников постоянно совершенствуются, поэтому будьте бдительны и не поддавайтесь на провокации



Вывод

- Подавляющее большинство мошенничеств с банковскими картами становится возможным благодаря небрежности владельцев или из-за незнания ими основных правил безопасности, поэтому назрела острая необходимость в просвещении людей в мерах предосторожности пользования банковскими картами и алгоритме действий в случаях противоправных посягательств.
-

Спасибо за внимание!

Проект подготовили:
ученики 11 класса
МАОУ СОШ№20 *(2018г)*