

МОУ ИРМО «Марковская средняя
общеобразовательная школа»
Интернет мошенничество



Работа ученика 9 «А» класса

Демьяненко Станислава

Руководитель проекта

Боровская Нина Константиновна

- Цель: Охарактеризовать основные виды мошенничества, с которыми могут столкнуться подростки.
- Задачи: 1.. Изучить и разобраться в видах мошенничества и их методов.
- 2. Поиск и анализ статистики.
- 3. Выяснить . какие правила необходимо соблюдать, чтобы не попасться на уловки мошенников в Интернете?
- Гипотеза: избежать обмана в сети Интернет возможно в случае хорошей информированности пользователей сети Интернет.

Мошенничество

Мошенничество — хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Под обманом понимается как сознательное искажение истины (активный обман), так и умолчание об истине...

Лицо, занимающееся мошенничеством, называется мошенник или мошенница.



Основные виды интернет мошенничества.

- Кража карты и обнуление счета
- Кража PIN – кода
- Мошенничество на SMS
- Заказ товаров и услуг по интернету



СКИММИНГ

Это кража данных карты при помощи специального считывающего устройства (скиммера).



Вишинг

- Телефонные мошенничества с банковскими картам считаются одними из наиболее распространенных преступлений.
- Мошенники представляются работниками банка.



Статья 159 УК РФ. Мошенничество

Наказывается штрафом в размере от ста двадцати тысяч рублей до 500 тысяч рублей, или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.

Фишинг

- С его помощью кибермошенники пытаются выманить у человека конфиденциальные данные или вынудить его на какие-либо нежелательные действия. С этой целью злоумышленники используют мгновенные и почтовые сообщения и специально созданные поддельные веб-сайты.

Официальные домены Steam – steamcommunity.com и steampowered.com. Мошенники регистрируют очень похожие домены для усыпления бдительности жертвы.

К примеру:

steam.stearncommunity.click
steamcammunnitty.com
steamsteamcammunity.ml
camrnunnitty.com
steamcommunnitty.ml



Одна из организаций занимающиеся борьбой с мошенничеством - «Лига безопасного интернета»

Лига безопасного интернета» поможет поймать киберпреступника
Если вы стали жертвой фишинга, сайта с вирусами, злоупотребления персональными данными, вам поможет «Лига безопасного интернета». Организация уже несколько лет успешно борется с вредоносным контентом в вебпространстве. В своей области она пользуется авторитетом и представляет серьёзную угрозу для мошенников.



ЛИГА
БЕЗОПАСНОГО
ИНТЕРНЕТА

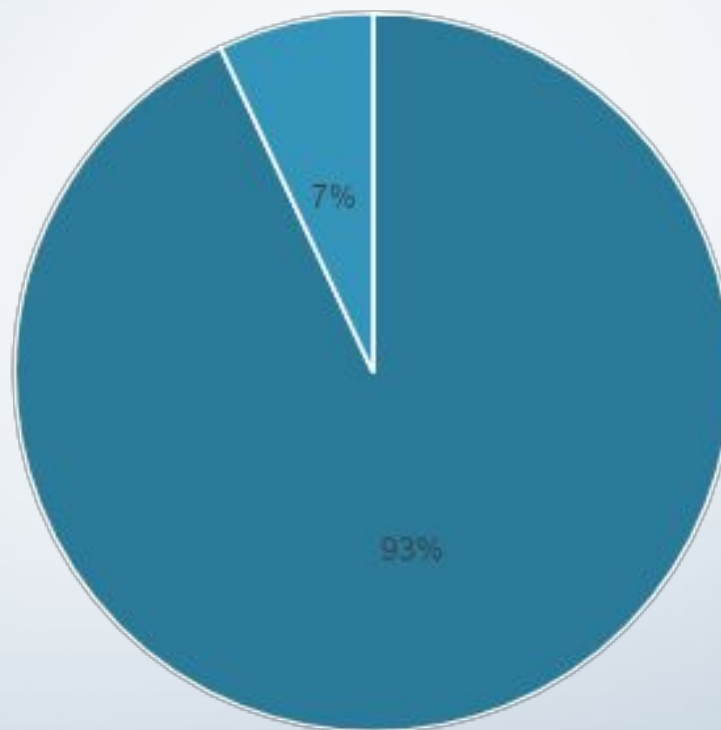
Как защититься от мошенничества.

- Необходимо следовать принципам безопасного поведения в интернете и не переходить по ссылкам, присланным в подозрительных или непонятных сообщениях электронной почты или через мессенджеры.
- Не загружать вложенные файлы из сообщений электронной почты, которых вы не ожидали.
- Обеспечить надежной защитой свои пароли и не сообщать их никому.
- Не сообщать никому свои персональные данные - будь то по телефону, лично или в сообщении эл. почты.
- Внимательно анализировать адрес сайта (URL), на который была переадресация. В большинстве случаев фишинга, несмотря на то, что сайт выглядит идентично настоящему, URL-адрес может отличаться от оригинального (например, заканчиваться на .com вместо .gov).

Поддерживать свой браузер обновленным и своевременно устанавливать обновления интернет безопасности программ.

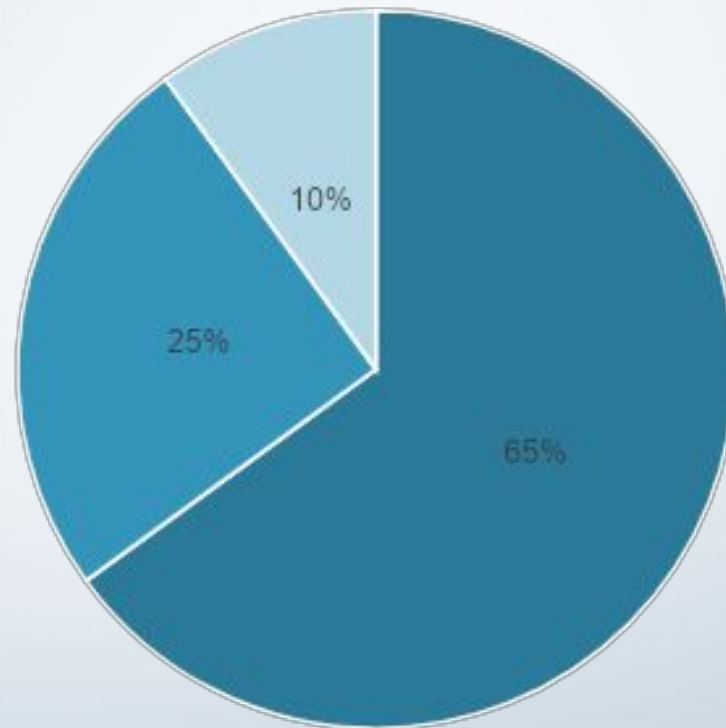
Знаете ли вы что такое мошенничество.

- Знаю
- Не знаю



Анализ данных предоставленных сотрудниками Находкинской полиции.

Вы сталкивались с мошенниками



- Да
- Нет
- Не знаю