

Направление функциональной
грамотности
Финансовая грамотность

Тема проекта
Как не стать жертвой мошенников

Тип проекта
Творческий

Выполнил:
Сухоплюев Константин, 7 «Г» класс
Наставник:
Фёдорова С.Ю., учитель информатики



Мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. За последние годы мошенничество в сети Интернет приобрело популярность. Подобная преступная деятельность преследуется законом независимо от места совершения - в реальной или виртуальной среде. Этим и обусловлена актуальность темы проекта.

Цель работы рассмотрение основных видов мошенничеств в сети Интернет, составление рекомендаций безопасного пользования ресурсами сети Интернет.

Задачи:

Изучить виды мошенничества в сети Интернет.

Изучить меры предосторожности от действий мошенников.

Ознакомиться с определенными мерами безопасности в сети Интернет





Своё начало мошенничество берёт ещё с Древнего Рима, в правовой системе которого изначально не было такого понятия, поэтому оно приравнивалось к обману.

Появление мошенничества в Древней Руси связано с торговлей. Торговцы обожали приукрашивать продаваемый товар покупателю, завышать цену на него и обсчитывать со сдачей. Позже, упоминание о мошенничестве появилось в Судебнике 1550 года. Это преступление приравнивалось к краже чужого имущества.

Виды мошенничества

1. «Фишинговые сайты»

Фишинговые сайты — это поддельные сайты, которые маскируются под настоящие. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Пытаясь зайти на популярный сайт, пользователь попадает на сайт-подделку, очень похожий на оригинал. Все данные, введенные на таком сайте (пароли, номера банковских карт, паспортные данные и т. д.), окажутся у злоумышленников.

2. «Нигерийские письма»

Жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки. Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взятки чиновникам и т.п.

3. «Приобретение товаров и услуг посредством сети Интернет»

Это оплата покупки полностью или предоплата до получения. После того как вы перечислите деньги на счет мошенника, он просто исчезает и не выходит на связь.

4. «Крик о помощи»

В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

5. «Брокерские конторы»

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам-трейдерам.

6. «Заражение вирусом-вымогателем»

Вирусы-вымогатели, которые попадают на компьютер «жертвы» и зашифровывают все файлы, что ставит под угрозу всю хранившуюся информацию и парализует работу. Чтобы вернуть все ваши документы, вирус выдает сообщение с требованием перевести средства на криптовалютный кошелек, чтобы их невозможно было отследить.

7. «Установка приложения на смартфон»

Практически каждый современный человек пользуется смартфоном. Это еще одно поле деятельности для кибермошенников. Одним из вариантов хищения ваших личных данных является установка зловредных приложений под видом обычных программ.

8. «Фальшивые интернет-аукционы»

Интернет-аукцион является хорошей возможностью купить товар по более низкой цене, но и здесь можно попасться «на удочку».

Совет: прежде чем делать ставки на лот, проверьте рейтинг и отзывы о продавце. На аукционах – это важнейшие показатели честности. Не рекомендуется делать ставки на товары продавцов с маленьким количеством отзывов и сделок или нулевым рейтингом.

9. «Мошенничество с любителями онлайн-игр»

Многие дети и даже люди старшего поколения обожают игры. Желание быть лучшим порождает зависимость, которая проявляется в растрате денег на своих игровых персонажей для покупки виртуальных улучшений и предметов. Чтобы сэкономить, многие ищут, где это можно сделать подешевле, наталкиваясь на аферистов, которые берут предоплату, но не предоставляют виртуальные ценности

10. «Мошенничество на бесконтактных платежах»

Современные банковские карточки оснащаются чипом, позволяющим совершать быструю оплату, поднося карту к терминалу, который считывает информацию и списывает соответствующую сумму со счета. Теперь подобными устройствами считывания пользуются не только магазины, но и мошенники. Они носят в сумке самодельные портативные терминалы и прислоняются к «жертвам», чтобы украсть деньги с карты.



Как не стать жертвой мошенников

Автор Сухоплюев Константин

Правила использования Интернета



- ✓ Когда ты регистрируешься на сайтах, старайся не указывать личную информацию (номер мобильного телефона, адрес электронной почты, свое фото).
Используй веб-камеру только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор, так как он может быть записан.
Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- ✓ Ты должен знать, что если ты публикуешь фото или видео в Интернете — каждый может посмотреть их.
- ✓ Нежелательные письма от незнакомых людей называются «Спам». Если ты получил такое письмо, не отвечай на него. Если ты ответишь на подобное письмо, отправитель будет знать, что ты пользуешься своим электронным почтовым ящиком, и будет продолжать посылать тебе спам.
- ✓ Не добавляй незнакомых людей в свой контакт лист в IM (VK, Instagram, Watsup, и т.д.)
- ✓ Если тебе приходят письма с неприятным и оскорбляющим тебя содержанием, если кто-то ведет себя в твоём отношении неподобающим образом, сообщи об этом взрослому.
- ✓ Если рядом с тобой нет взрослых, не встречайся в реальной жизни с людьми, которыми ты познакомился в Интернете. Если твой виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к твоей заботе о собственной безопасности!

Виды мошенничества:

- Фишинг
- Нигерийские письмо
- Приобретение товаров и услуг в сети Интернет
- Крик о помощи
- Мошенничество на бесконтактных платежах
- Мошенничество с любителями онлайн-игр
- Брокерские конторы
- Заражение вирусом-вымогателем
- Фальшивые интернет-аукционы

Заключение

Мошенничество, неискоренимо. И на просторах интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной. Не стоит думать, что Интернет – это безопасное место, в котором можно чувствовать себя полностью защищенным. Чтобы максимально обезопасить себя и своих близких от опасностей сети Интернет, нужно постоянно совершенствовать свои знания и навыки в области информационной безопасности в сети Интернет.

Для помощи в этом вопросе мною был подготовлен буклет с основными рекомендациями.

Список использованной литературы:

1. Мошенничество в сети – Общие вопросы. Справка https://yandex.ru/support/common/security/phishing.html?utm_source=facts/ (дата обращения 31.01.2022)
2. Интернет – мошенничество. Памятка для граждан <https://мвд.рф/document/1910260/> (дата обращения 31.01.2022)
3. Десять схем кибер-мошенничества, о которых вам следует знать <https://club.dns-shop.ru/blog/t-57-tehnologii/20007-desyat-shem-kiber-moshennichestva-o-kotoryih-vam-sleduet-znat/> (дата обращения 01.02.2022)
4. Статья Исследовательский проект <https://multiurok.ru/files/issliedovatel-skii-proiekt-moshiennichiestvo-v-si.html> (дата обращения 01.02.2022)
5. Образовательная социальная сеть <https://nsportal.ru/shkola/informatika-i-ikt/library/2012/04/27/vidy-moshennichestv-i-kak-zashchititsya-ot-moshennikov-v/> (дата обращения 03.02.2022)

Направление функциональной грамотности
Финансовая грамотность

Тема проекта
Как не стать жертвой мошенников

Тип проекта
Творческий

Выполнил:
Сухоплюев Константин, 7 «Г» класс
Наставник:
Фёдорова С.Ю., учитель информатики