Обеспечение личной кибербезопасности

Жданов Даниил 9А МБОУ СОШ С УИОП 58

Содержание

- Актуальность
- Цель и задачи
- Основной этап
- Итог
- Используемая литература

Актуальность

Цель

Научится **предостерегать и устранять угрозы** для своих данных в сети интернет.

Задачи

- Узнать методы киберпреступлений
- Найти способ противостоять угрозам из сети интернет

Угроза заражения виртуальным вирусом

Одним из самых **распространенных** способом кражи или уничтожения данных являются **вирусы**. Для того, чтобы начать действовать им необходимо оказаться на жёстком диске жертвы, а иногда требуется ручной запуск.

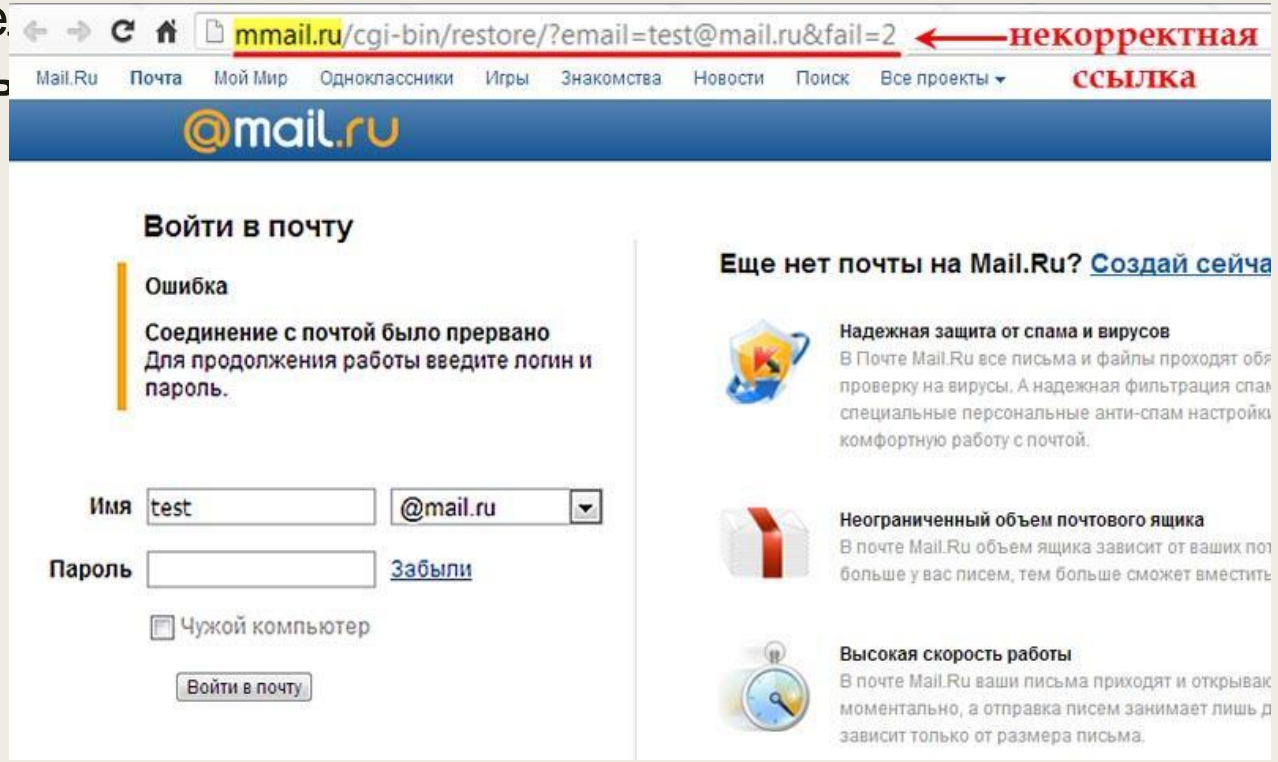
Для защиты от вирусов нужно:

- Установить **проверенный** антивирус с **официального сайта**
- Не загружать *подозрительные* файлы, не открывать *неизвестные* ссылки
- Не использовать *неизвестные* флеш накопители

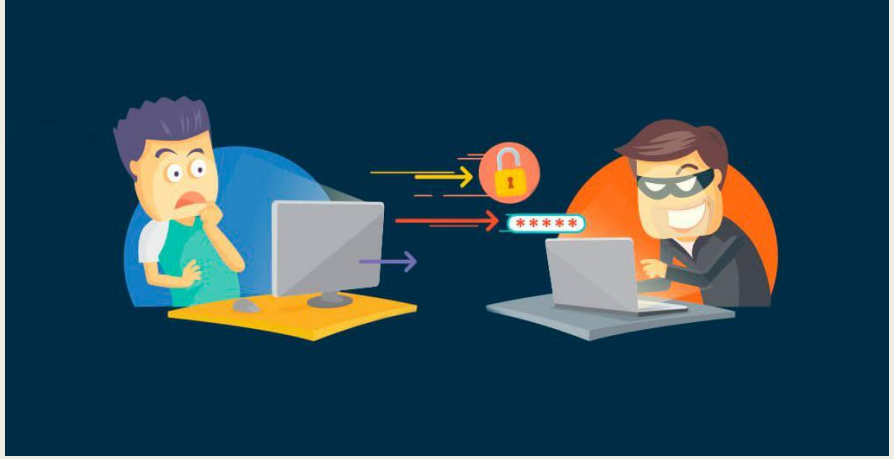
Мошеничество

В интернете могут представлять угрозу не только неизвестные файлы и ссылки, но и реальные люди. Они используют различные техники обмана, но их можно избежать.

- Фишинг: мошенники могут дать ссылку на поддельный сайт для заполнения личных данных, с индетичным дизайном и похожим доменом. Для избежания этого необходимо внимате
собираетесь ввести **личны**



Мошеничество



- Просьба скачать неизвестный файл: из прошлых слайдов мы сделали вывод о том, что **не стоить скачивать неизвестные файлы** .
- Знакомый резко отправляет **странное** сообщение с просьбой перейти по ссылке или отправит денег: спросите у знакомого(желательно не через интернет, но если таковой возможности нет, то через другую сеть общения) взломали ли его.
- Оповещение о крупном выигрыше: в таких случаях не пытаются украсть данные, но пытаются обманом забрать деньги. Обычно вас просят перевести небольшую сумму денег для отправки выигрыша, а после получения просят выполнить ещё один перевод и так далее. Для защиты от этого вида мошенников требуется знать то, что **в лотереях/прочих условиях «выигрыша» оплату за транзакцию берёт на себя сторона, устроившая розыгрыш.**

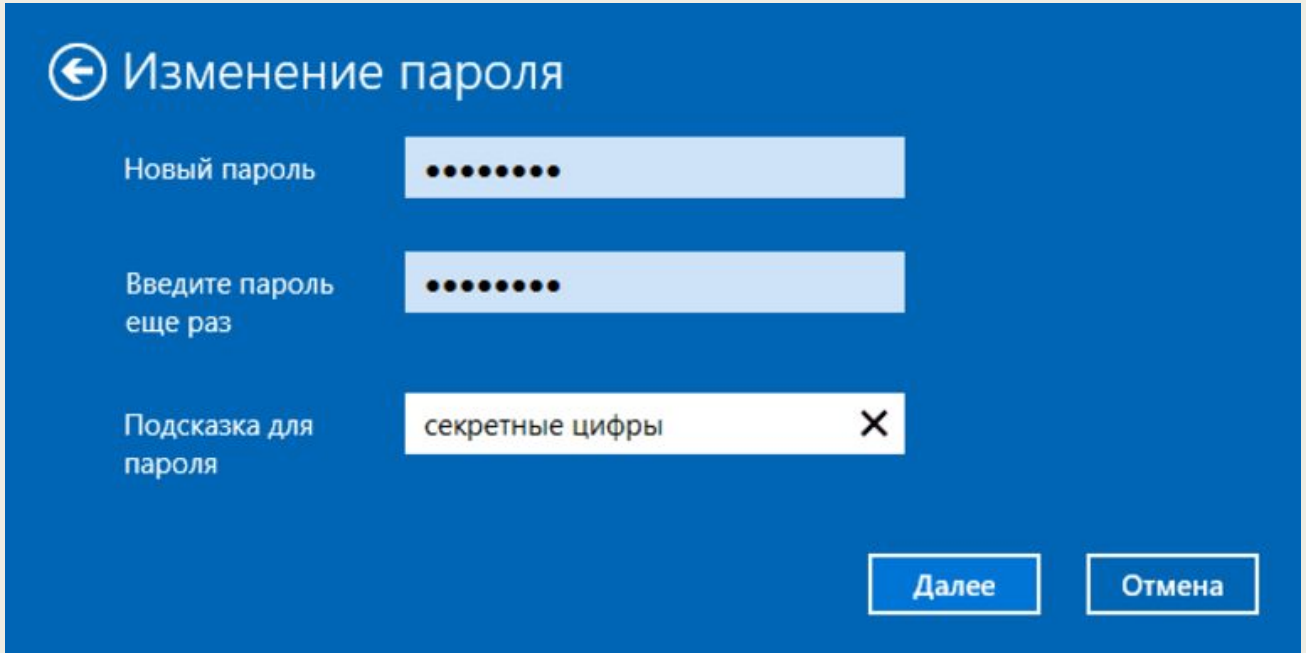
Мошенничество

Угрозы: вас могут заставить отправлять деньги для того, чтобы расшифровать данные данные на заражённом устройстве, или же угрожать личным данным. В данном случаев **не нужно ничего не переводить**, а в случае беспокойство обратится в **полицию**.

- Также, никогда не вводите личные данные в **общественных точках доступа**. Через них мошенники могут перехвать ваши данные.

Что делать, если киберпреступление уже совершено?

- Если оно мешает работе устройства, то стоит «прочистить» его антивирусом, но если такой возможности нет, то полностью переустановить систему.
- Если ваши данные были украдены, то стоит обратится в полицию и поменять пароли/перевыпустить карту в зависимости от ситуации.



Итог

Эта презентация должна помочь вам находить и вовремя обходить стороной киберугрозы, а также дать совет о том, какие действия надо предпринимать в случае киберпреступления.

Источники

- https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/
- https://kaspersky-ru.turbopages.org/turbo/kaspersky.ru/s/resource-center/definitions/what-is-cyber-security
- https://proglib-io.turbopages.org/turbo/proglib.io/s/p/kiberbezopasnost-v-2021-godu-otvety-na-glavnye-voprosy-novichkov-2021-07-09
- https://habr.com/ru/company/sberbank/blog/592275/
- https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html