Мой безопасный интернет

Правила безопасного поведения в сети

Универсум
АНО Центр НИОКР

ПРИ ПОДДЕРЖКЕ
ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Остерегайся вирусов/вредоносных программ

Что делают вирусы?

- мешают работе компьютера/телефона,
- стирают файлы,
- крадут личные данные и пароли
- вымогают деньги

Как можно заразить компьютер/телефон?

- при установке «пиратского» ПО
- скачивание и открытие вирусных файлов
- через зараженные флешки
- переход по непроверенной ссылке
- посещение незащищенных сайтов

Как уберечься от интернет-вирусов:

- устанавливай лицензионное ПО;
- проверяй файлы и флешки антивирусами;
- не переходи по ссылкам в сообщениях от незнакомых адресатов;
- посещайте только защищенные сайты, адресная строка которых начинается с https://, а не с http://

Береги личные данные в интернете

Какие личные данные могут украсть мошенники?

- адес электронной почты;
- пароли от твоих аккаунтов в социальных сетях;
- номер банковской карты;
- личные фотографии;

Как мошенники могут использовать украденные данные?

- рассылать от твоего имени спам;
- взломать твои социальные сети и вымогать у твоих знакомых деньги;
- красть деньги с твоей банковской карты или карты твоих родителей;

Как защитить личные данные в интернете?

- храни в секрете свои пароли;
- придумывай для своих аккаунтов сложные пароли, чтобы их трудно было подобрать;
- используй двойную защиту при входе в свой аккауни (через смс на телефон);
- будь осторожен при вводе своих данных в сетях wi-fi общего пользования (например, в кафе школе, метро)

Совершай безопасные платежи в интернете

Как мошенники могут украсть ваши деньги?

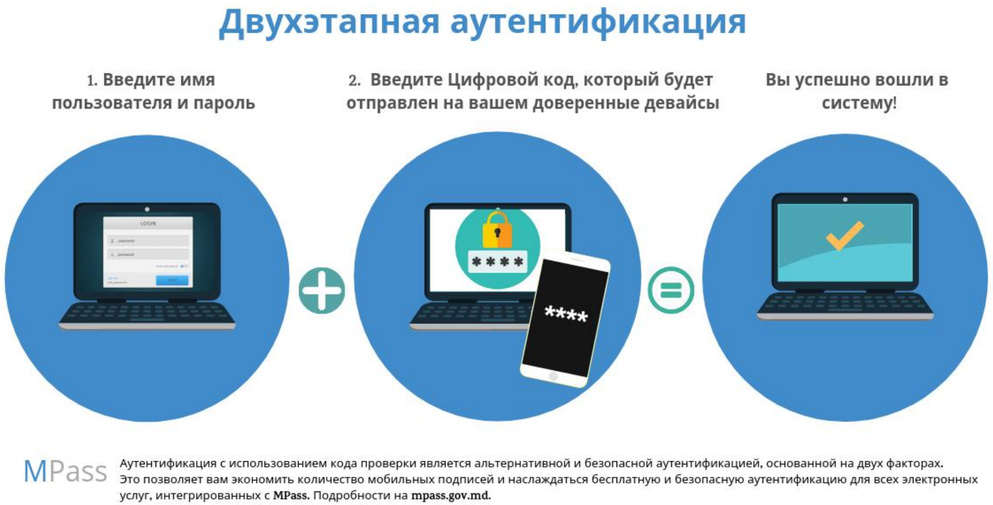
- с помощью поддельных сайтов банков, которые выглядят как настоящие;
- могут позвонить, представиться сотрудником банка и запросить данные счета или смс код для якобы проверки данных;
- могут написать сообщение со взломанной страницы твоего друга и попросить о помощи - перевести деньги;
- организовать в интернете розыгрыш призов, объявить вас победителм и предлжить перевести небольшую сумму за доставку приза;
- скопировать данные вашей карты через незащищенные интернет-магазины;

Как защитить ваши деньги в интернете?

- Никому не сообщайте коды из смс, которые приходят вам от банков и платежных сервисов;
- Держите в тайне пин-коды и пароли, необходимые для платежа;
- Помните: настоящие сотрудники банка никогда не будут просить у вас паролей и пин-кодов от счета, просить оправить им смс с подтверждением;
- Прежде чем броситься выручать товарища, вспомните о том, что писать вам может вовсе и не он. Лучше всего сначала перезвонить человеку. Наверняка выяснится, что никакой беды нет, а просто взломали аккаунт;
- Проверяйте адрес сайта, на котором вводите данные карты. У мошеннических сайтов в нём будут ошибки и опечатки. Например, вместо money.yandex.ru фальшивая страница может использовать адрес money.yanex.ru.
- Обращайте внимание на безопасность соединения — ищите в строке браузера заветный набор букв https.

Что делать, если...

- Компьютер или телефон был заражен вирусом → Запустите проверку антивирусником
- Взломали вашу социальную сеть или почту → Срочно смените пароль и установите двойную защиту через смс на телефон
- Украли данные банковской карты или вы по неосторожности ввели её данные на сайте мошенников → Не ждите, пока мошенники доберутся до денег — сразу идите в банк и заблокируте карту. С виртуальной картой проще — её вы можете заблокировать сами, в личном кабинете на сайте платежного сервиса, и тут же перевыпустить



Как обезопасить свой телефон при потере?

- Настройте пароль на разблокировку или пользуйтесь разблокировкой по отпечатку пальца;
- Установите на телефоне программу «Найти устройство», или активируйте ее на телефоне. Тогда телефон можно будет найти легче;
- Не храните на телефоне фотографии паспорта и других личных документов, чтобы они не попали к мошенникам;
- Все денежные приложения должны открываться по коду доступа, который отличается от кода доступа к телефону.

Что делать, если телефон все-таки потерян и вы боитесь, что важная информация попадет злоумышленникам?

- Заблокируйте ваш номер телефона через оператора.

  Ваша задача сделать так, чтоб сим карта была неактивной. Сделать это нужно как можно быстрее. Это затруднит возможность пользования вашими данными;
- Удаленно заблокируйте свой телефон (для этого потребуется на компьютере зайти в ваш аккаунт Google или Apple ID.

Подведем итог!

Соблюдай эти несложные правила

01

Не публикуй в интернете личную информацию (она может быть использована против тебя)

02

Посещай только безопасные сайты и не переходи по ссылкам с неизвестных адресов

03

Установи антивирусные программы на свои устройства, чтобы предупредить попадание вирусов

04

Создавай сложные пароли на свои аккаунты и не храни их в доступном месте

05

Не поддавайся на заманчивым предложениям в интернете, которые просят у тебя поделиться личными данными или отправить деньги

Универсум

АНО Центр НИОКР

Спасибо за внимание
и безопасного интернета!

ПРИ ПОДДЕРЖКЕ
ФОНДА
ПРЕЗИДЕНТСКИХ
ГРАНТОВ