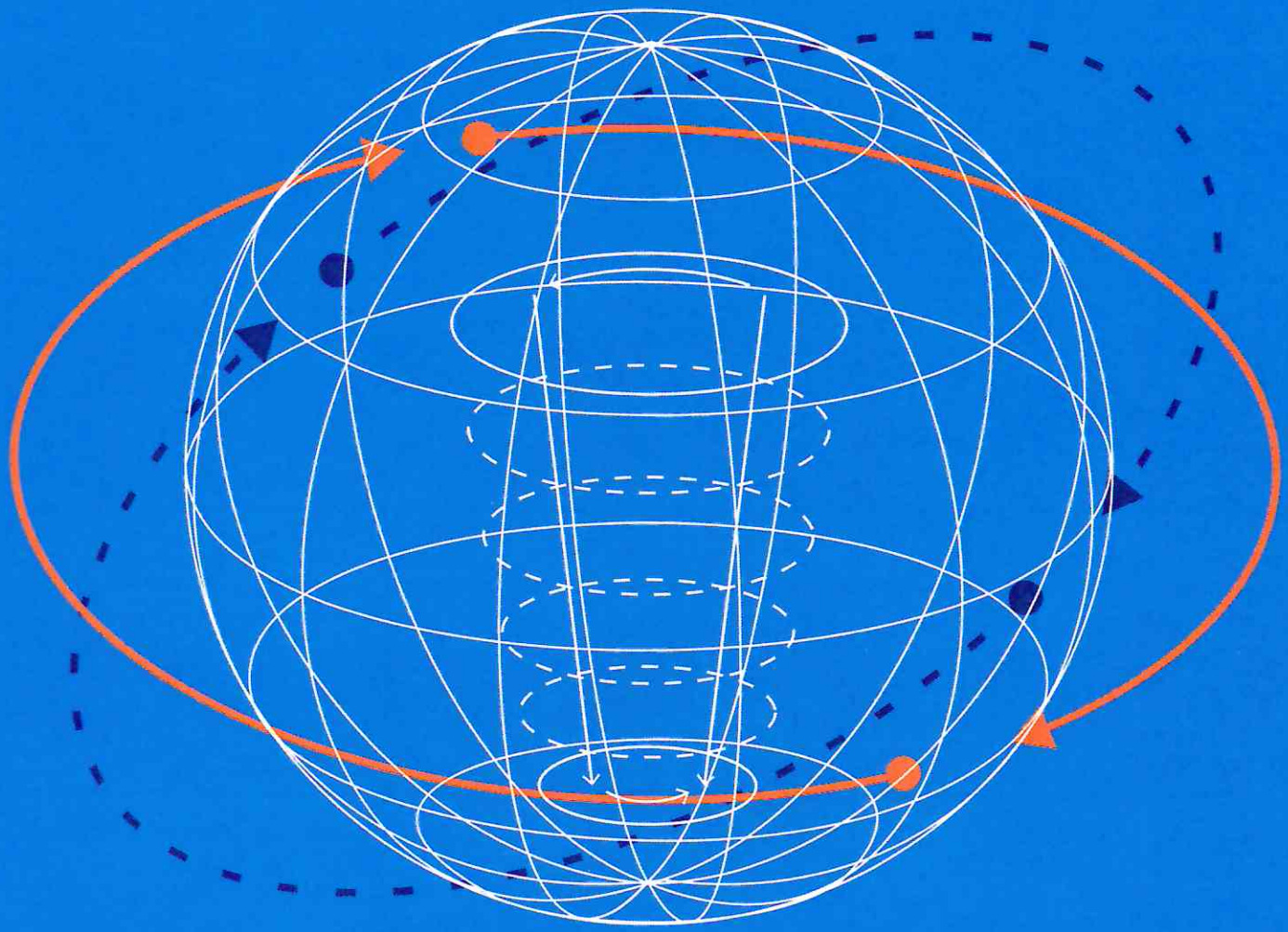


КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

ЭТО БЕЗОПАСНОСТЬ ДЕЙСТВИЙ И ТРАНЗАКЦИЙ, СОВЕРШАЕМЫХ В ИНТЕРНЕТЕ, ВКЛЮЧАЕТ БЕЗОПАСНОСТЬ БРАУЗЕРА И СЕТИ, А ТАКЖЕ ПРАВИЛЬНОЕ ПОВЕДЕНИЕ В СЕТИ.

КАК МНОГО ВРЕМЕНИ ТЫ ПРОВОДИШЬ, ИЗУЧАЯ СТРАНИЦЫ ДРУЗЕЙ «ВКОНТАКТЕ»?

НАВЕРНЯКА ТЫ В КУРСЕ ВСЕХ ЧЕКИНОВ, ПОСТОВ И ПОСЛЕДНИХ СЕЛФИ, ОПУБЛИКОВАННЫХ ПРИЯТЕЛЯМИ, И ЗНАЕШЬ, КАК ОНИ РАЗВЛЕКАЮТСЯ И ЧЕМ УВЛЕКАЮТСЯ.?

НА САМОМ ДЕЛЕ ТО ЖЕ САМОЕ МОЖЕТ СДЕЛАТЬ КТО УГОДНО, НО В СВОИХ КОРЫСТНЫХ ИНТЕРЕСАХ: ЧТОБЫ ВЗЛОМАТЬ ТВОЮ УЧЕТНУЮ ЗАПИСЬ, ЗАРАЗИТЬ ТВОЙ ПК ВИРУСАМИ И ЗЛОВРЕДНЫМ ПО ИЛИ ЖЕ УКРАСТЬ ЦЕННЫЕ ДАННЫЕ, ТАКИЕ КАК ИГРОВЫЕ АККАУНТЫ.

ПОЧЕМУ КИБЕРБЕЗОПАСНОСТЬ ТАК ВАЖНА?

ВСЕ БЕЗ ИСКЛЮЧЕНИЯ ПОЛЬЗОВАТЕЛИ ИНТЕРНЕТА ПОДВЕРЖЕНЫ РИСКУ БЫТЬ ВЗЛОМАННЫМИ, ВЕРНЕЕ — ИХ КОМПЬЮТЕРЫ, СМАРТФОНЫ И ДРУГИЕ УСТРОЙСТВА С ВЫХОДОМ В ГЛОБАЛЬНУЮ СЕТЬ. ДЛЯ ПРЕДОТВРАЩЕНИЯ ПОПЫТОК ЗЛОУМЫШЛЕННИКОВ УКРАСТЬ

ЛИЧНЫЕ ДАННЫЕ

ПОВРЕДИТЬ/УДАЛИТЬ ФАЙЛЫ С ЦЕЛЬЮ ШАНТАЖА

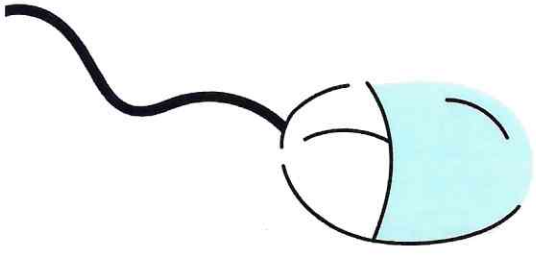
КАКИЕ УГРОЗЫ ПОДСТЕРЕГАЮТ НАС НА КАЖДОМ ШАГУ?

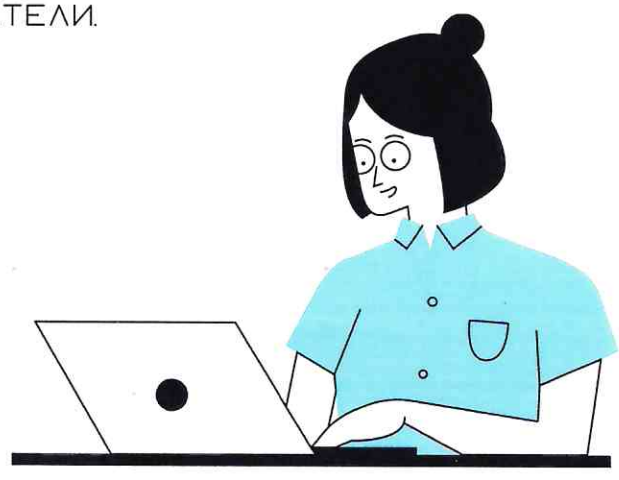
ЗЛОУМЫШЛЕННИКИ ПРИДУМАЛИ БОЛЬШОЕ КОЛИЧЕСТВО СПОСОБОВ ПОЛУЧЕНИЯ ДОСТУПА К ЛИЧНОЙ ИНФОРМАЦИИ, НАРУШЕНИЮ РАБОТЫ КОМПЬЮТЕРНЫХ ПРОГРАММ, УСТРОЙСТВ ИЛИ ЦЕЛЫХ СИСТЕМ, КАК, НАПРИМЕР, ИНТЕРНЕТ-БАНКИНГ. ПРИВЕДЕМ НЕСКОЛЬКО САМЫХ РАСПРОСТРАНЕННЫХ ТИПОВ СЕТЕВЫХ УГРОЗ

ФИШИНГ. ЭТА ТЕХНОЛОГИЯ ВЗЛОМА, ОБЫЧНО ПРИМЕНЯЕМАЯ ДЛЯ КРАЖИ НОМЕРОВ БАНКОВСКИХ КАРТ, ДАННЫХ (ЛОГИНЫ/ПАРОЛИ) НА ТЕХ ИЛИ ИНЫХ САЙТАХ. ЗЛОУМЫШЛЕННИКИ МОГУТ ОТПРАВЛЯТЬ ЭЛЕКТРОННЫЕ ПИСЬМА ИЛИ СООБЩЕНИЯ В ПОПУЛЯРНЫХ МЕССЕНДЖЕРАХ (WHATSAPP, TELEGRAM И Т.Д.), В КОТОРЫХ, К ПРИМЕРУ, СОДЕРЖАТСЯ ПРИЗЫВЫ ПЕРЕЙТИ ПО ССЫЛКЕ ИЛИ СКАЧАТЬ КАКОЕ-ЛИБО ПРИЛОЖЕНИЕ.

ВРЕДОНОСНЫЕ ПРОГРАММЫ. ЭТО КЛАССИЧЕСКАЯ ТЕХНОЛОГИЯ ВЗЛОМА КОМПЬЮТЕРОВ, О КОТОРЫХ ЗНАЮТ ВСЕ. ВИРУСЫ СПОСОБНЫ ВЫПОЛНЯТЬ ВООБЩЕ ЛЮБЫЕ ДЕЙСТВИЯ — ВПЛОТЬ ДО ПРЕДОСТАВЛЕНИЯ ПОЛНОГО ДОСТУПА К КОМПЬЮТЕРУ ЖЕРТВЫ. ВРЕДОНОСНЫЕ ПРОГРАММЫ ЗАЧАСТУЮ ПОПАДАЮТ НА ПК ИЗ ИНТЕРНЕТА ВМЕСТЕ С ДРУГИМИ СКАЧИВАЕМЫМИ ФАЙЛАМИ ЛИБО ВМЕСТО ТОГО, ЧТО НАМЕРЕВАЛСЯ ИЗНАЧАЛЬНО СКАЧАТЬ ПОЛЬЗОВАТЕЛЬ.

КОНЕЧНО, ЭТО ДАЛЕКО НЕ ВЕСЬ ПЕРЕЧЕНЬ СУЩЕСТВУЮЩИХ СЕГОДНЯ СЕТЕВЫХ УГРОЗ, С КОТОРЫМИ МОГУТ СТОЛКНУТЬСЯ ВСЕ — НЕ ТОЛЬКО СПЕЦИАЛИСТЫ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ, НО И ПРОСТЫЕ ПОЛЬЗОВАТЕЛИ.





КАК ПРОТИВОСТОЯТЬ СЕТЕВЫМ УГРОЗАМ?

CTRL | 1. СОЦИАЛЬНЫЕ СЕТИ | ALT

ОСНОВНЫЕ СОВЕТЫ ПО БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ:

1. ОГРАНИЧЬ СПИСОК ДРУЗЕЙ. У ТЕБЯ В ДРУЗЬЯХ НЕ ДОЛЖНО БЫТЬ СЛУЧАЙНЫХ И НЕЗНАКОМЫХ ЛЮДЕЙ

2. ЗАЩИЩАЙ СВОЮ ЧАСТНУЮ ЖИЗНЬ. НЕ УКАЗЫВАЙ ПАРОЛИ, ТЕЛЕФОНЫ, АДРЕСА И ДРУГУЮ ЛИЧНУЮ ИНФОРМАЦИЮ. НЕ ОТКРЫВАЙ ДОСТУП К СВОИМ ПОСТАМ И ФОТОГРАФИЯМ В СОЦСЕТЯХ ДЛЯ ВСЕХ

3. ЗАЩИЩАЙ СВОЮ РЕПУТАЦИЮ ПОДУМАЙ, ПРЕЖДЕ ЧЕМ ЧТО-ТО ОПУБЛИКОВАТЬ, НАПИСАТЬ И ЗАГРУЗИТЬ

4. ЕСЛИ ТЫ ГОВОРИШЬ С ЛЮДЬМИ, КОТОРЫХ НЕ ЗНАЕШЬ, НЕ ИСПОЛЬЗУЙ СВОЕ РЕАЛЬНОЕ ИМЯ И ДРУГУЮ ЛИЧНУЮ ИНФОРМАЦИИ: ИМЯ, МЕСТО ЖИТЕЛЬСТВА, МЕСТО УЧЕБЫ И ПРОЧЕЕ

5. НЕ ПЕРЕСЫЛАЙ ВАЖНУЮ ИНФОРМАЦИЮ (НАПРИМЕР, ЛОГИН И ПАРОЛЬ) ПО НЕЗАЩИЩЕННЫМ КАНАЛАМ: В ЧАТЕ ИЛИ НА ФОРУМЕ.

6. ДЛЯ СОЦИАЛЬНОЙ СЕТИ, ПОЧТЫ И ДРУГИХ САЙТОВ НЕОБХОДИМО ИСПОЛЬЗОВАТЬ РАЗНЫЕ ПАРОЛИ. ТОГДА ЕСЛИ ТЕБЯ ВЗЛОМАЮТ, ТО ЗЛОУМЫШЛЕННИКИ ПОЛУЧАТ ДОСТУП ТОЛЬКО К ОДНОМУ МЕСТУ, А НЕ ВО ВСЕ СРАЗУ

2. МОБИЛЬНЫЙ ТЕЛЕФОН

ОСНОВНЫЕ СОВЕТЫ ДЛЯ БЕЗОПАСНОСТИ МОБИЛЬНОГО ТЕЛЕФОНА:

1. НЕ ПОДКЛЮЧАЙСЯ К НЕПРОВЕРЕННОМУ WI-FI, ОСОБЕННО К ОТКРЫТОМУ, ПОТОМУ ЧТО ЕГО МОГУТ ИСПОЛЬЗОВАТЬ ДЛЯ СБОРА ДАННЫХ, КОТОРЫЕ ТЫ ОТПРАВЛЯЕШЬ (НР: ПАРОЛЕЙ)

2. ДУМАЙ, ПРЕЖДЕ ЧЕМ ОТПРАВИТЬ SMS, ФОТО ИЛИ ВИДЕО. ТЫ ТОЧНО ЗНАЕШЬ, ГДЕ ОНИ БУДУТ В ИТОГЕ?

3. НЕОБХОДИМО ОБНОВЛЯТЬ ОПЕРАЦИОННУЮ СИСТЕМУ ТВОЕГО СМАРТФОНА

4. ИСПОЛЬЗУЙ АНТИВИРУСНЫЕ ПРОГРАММЫ ДЛЯ МОБИЛЬНЫХ ТЕЛЕФОНОВ

5. ТЫ МОЖЕШЬ КОНТРОЛИРОВАТЬ СВОЕ УСТРОЙСТВО УДАЛЕННО, ДАЖЕ ЕСЛИ ОНО ПОТЕРЯНО ИЛИ УКРАДЕНО. ДЛЯ ЭТОГО АКТИВИРУЙ ОПЦИИ УДАЛЕННОГО УПРАВЛЕНИЯ И РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ С ПОМОЩЬЮ ВСТРОЕННЫХ ВОЗМОЖНОСТЕЙ ТЕЛЕФОНА (НАПРИМЕР, НАСТРОЙКИ «НАЙТИ МОЙ IPHONE») ИЛИ ИСПОЛЬЗУЙ СПЕЦИАЛЬНОЕ ПРИЛОЖЕНИЕ

6. ЧИСТИ COOKIES В БРАУЗЕРЕ

7. ПЕРИОДИЧЕСКИ ПРОВЕРЯЙ КАКИЕ ПЛАТНЫЕ УСЛУГИ АКТИВИРОВАНЫ НА ТВОЕМ НОМЕРЕ

8. ДАВАЙ СВОЙ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА ТОЛЬКО ЛЮДЯМ, КОТОРЫХ ТЫ ЗНАЕШЬ И КОМУ ДОВЕРЯЕШЬ

9. BLUETOOTH ДОЛЖЕН БЫТЬ ВЫКЛЮЧЕН, КОГДА ТЫ ИМ НЕ ПОЛЬЗУЕШЬСЯ

3. ЭЛЕКТРОННЫЕ ДЕНЬГИ

ОСНОВНЫЕ СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ С ЭЛЕКТРОННЫМИ ДЕНЬГАМИ:

1. ПРИВЯЖИ К СЧЕТУ МОБИЛЬНЫЙ ТЕЛЕФОН. ЭТО САМЫЙ УДОБНЫЙ И БЫСТРЫЙ СПОСОБ ВОССТАНОВИТЬ ДОСТУП К СЧЕТУ. ПРИВЯЗАННЫЙ ТЕЛЕФОН ПОМОЖЕТ, ЕСЛИ ЗАБУДЕШЬ СВОЙ ПЛАТЕЖНЫЙ ПАРОЛЬ ИЛИ ЗАЙДЕШЬ НА САЙТ С НЕЗНАКОМОГО УСТРОЙСТВА;

2. ИСПОЛЬЗУЙ ОДНОРАЗОВЫЕ ПАРОЛИ. ПОСЛЕ ПЕРЕХОДА НА УСИЛЕННУЮ АВТОРИЗАЦИЮ ТЕБЕ УЖЕ НЕ БУДЕТ УГРОЖАТЬ ОПАСНОСТЬ КРАЖИ ИЛИ ПЕРЕХВАТА ПЛАТЕЖНОГО ПАРОЛЯ;

3. ВЫБЕРИ СЛОЖНЫЙ ПАРОЛЬ. ПРЕСТУПНИКАМ БУДЕТ НЕ ПРОСТО УГАДАТЬ СЛОЖНЫЙ ПАРОЛЬ. НАДЕЖНЫЕ ПАРОЛИ — ЭТО ПАРОЛИ, КОТОРЫЕ СОДЕРЖАТ НЕ МЕНЕЕ 8 ЗНАКОВ И ВКЛЮЧАЮТ В СЕБЯ СТРОЧНЫЕ И ПРОПИСНЫЕ БУКВЫ, ЦИФРЫ И НЕСКОЛЬКО СИМВОЛОВ, ТАКИЕ КАК ЗНАК ДОЛЛАРА, ФУНТА, ВОСКЛИЦАТЕЛЬНЫЙ ЗНАК И Т.П.: НАПРИМЕР, STRONG!;

4. НЕ ВВОДИ СВОИ ЛИЧНЫЕ ДАННЫЕ НА САЙТАХ, КОТОРЫМ НЕ ДОВЕРЯЕШЬ.

Ч. СЕТИ WI-FI

СОВЕТЫ ПО БЕЗОПАСНОСТИ РАБОТЫ В ОБЩЕДОСТУПНЫХ СЕТЯХ WI-FI

1. НЕ ПЕРЕДАВАЙ СВОЮ ЛИЧНУЮ ИНФОРМАЦИЮ ЧЕРЕЗ ОБЩЕДОСТУПНЫЕ WI-FI СЕТИ. РАБОТАЯ В НИХ, ЖЕЛАТЕЛЬНО НЕ ВВОДИТЬ ПАРОЛИ ДОСТУПА, ЛОГИНЫ И КАКИЕ-ТО НОМЕРА

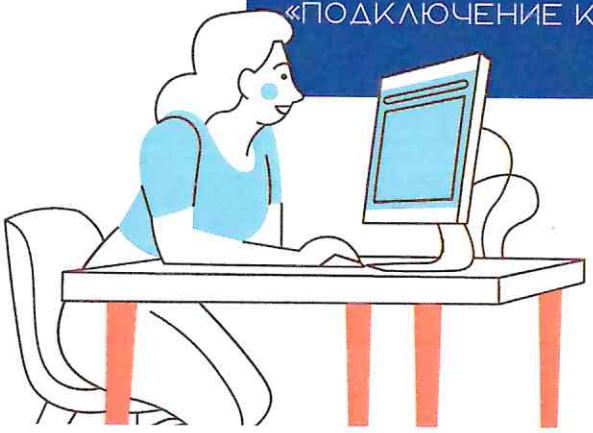
2. ИСПОЛЬЗУЙ И ОБНОВЛЯЙ АНТИВИРУСНЫЕ ПРОГРАММЫ И БРАНДМАУЭР. ТЕМ САМЫМ ТЫ ОБЕЗОПАСИШЬ СЕБЯ ОТ ЗАКАЧКИ ВИРУСА НА ТВОЕ УСТРОЙСТВО

3. ПРИ ИСПОЛЬЗОВАНИИ WI-FI ОТКЛЮЧИ ФУНКЦИЮ «ОБЩИЙ ДОСТУП К ФАЙЛАМ И ПРИНТЕРАМ»

4. НЕ ИСПОЛЬЗУЙ ПУБЛИЧНЫЙ WI-FI ДЛЯ ПЕРЕДАЧИ ЛИЧНЫХ ДАННЫХ, НАПРИМЕР, ДЛЯ ВЫХОДА В СОЦИАЛЬНЫЕ СЕТИ ИЛИ В ЭЛЕКТРОННУЮ ПОЧТУ

5. ИСПОЛЬЗУЙ ТОЛЬКО ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ ЧЕРЕЗ HTTPS, А НЕ HTTP, Т.Е. ПРИ НАБОРЕ ВЕБ-АДРЕСА ВВОДИ ИМЕННО «HTTPS://»

6. В МОБИЛЬНОМ ТЕЛЕФОНЕ ОТКЛЮЧИ ФУНКЦИЮ «ПОДКЛЮЧЕНИЕ К WI-FI АВТОМАТИЧЕСКИ»



5. КОМПЬЮТЕРНЫЕ ВИРУСЫ

МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ:

1. ИСПОЛЬЗУЙ СОВРЕМЕННЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ, ИМЕЮЩИЕ СЕРЬЁЗНЫЙ УРОВЕНЬ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

2. ПОСТОЯННО УСТАНАВЛИВАЙ ПАТЧИ (ЦИФРОВЫЕ ЗАПЛАТКИ, КОТОРЫЕ АВТОМАТИЧЕСКИ УСТАНАВЛИВАЮТСЯ С ЦЕЛЬЮ ДОРАБОТКИ ПРОГРАММЫ) И ДРУГИЕ ОБНОВЛЕНИЯ СВОЕЙ ОПЕРАЦИОННОЙ СИСТЕМЫ. СКАЧИВАЙ ИХ ТОЛЬКО С ОФИЦИАЛЬНОГО САЙТА РАЗРАБОТЧИКА ОС.

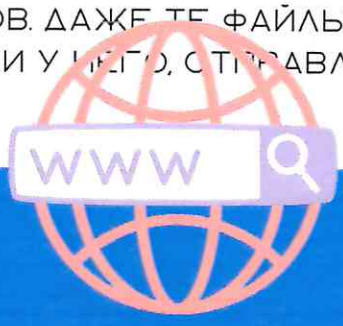
3. РАБОТАЙ НА СВОЕМ КОМПЬЮТЕРЕ ПОД ПРАВАМИ ПОЛЬЗОВАТЕЛЯ, А НЕ АДМИНИСТРАТОРА. ЭТО НЕ ПОЗВОЛИТ БОЛЬШИНСТВУ ВРЕДОНОСНЫХ ПРОГРАММ ПОПАСТЬ НА ТВОЙ КОМПЬЮТЕР

4. ИСПОЛЬЗУЙ АНТИВИРУСНЫЕ ПРОГРАММНЫЕ ПРОДУКТЫ ИЗВЕСТНЫХ ПРОИЗВОДИТЕЛЕЙ, С АВТОМАТИЧЕСКИМ ОБНОВЛЕНИЕМ БАЗ

5. ОГРАНИЧЬ ФИЗИЧЕСКИЙ ДОСТУП К КОМПЬЮТЕРУ ДЛЯ ПОСТОРОННИХ ЛИЦ

6. ИСПОЛЬЗУЙ ВНЕШНИЕ НОСИТЕЛИ ИНФОРМАЦИИ, ТАКИЕ КАК ФЛЕШКА, ДИСК ИЛИ ФАЙЛ ИЗ ИНТЕРНЕТА, ТОЛЬКО ИЗ ПРОВЕРЕННЫХ ИСТОЧНИКОВ

7. НЕ ОТКРЫВАЙ КОМПЬЮТЕРНЫЕ ФАЙЛЫ, ПОЛУЧЕННЫЕ ИЗ НЕНАДЁЖНЫХ ИСТОЧНИКОВ. ДАЖЕ ТЕ ФАЙЛЫ, КОТОРЫЕ ПРИСЛАЛ ТВОЙ ЗНАКОМЫЙ. ЛУЧШЕ УТОЧНИ У НЕГО, ОТПРАВЛЯЛ ЛИ ОН ТЕБЕ ИХ.



ОСНОВНЫЕ СОВЕТЫ

1. СЛЕДИ ЗА СВОИМ АККАУНТОМ. ЕСЛИ ТЫ ПОДОЗРЕВАЕШЬ, ЧТО ТВОЯ АНКЕТА БЫЛА ВЗЛОМАНА, ТО НЕОБХОДИМО ЗАБЛОКИРОВАТЬ ЕЕ И СООБЩИТЬ АДМИНИСТРАТОРАМ

2. ИСПОЛЬЗУЙ БЕЗОПАСНЫЕ ВЕБ-САЙТЫ, В ТОМ ЧИСЛЕ, ИНТЕРНЕТ-МАГАЗИНОВ И ПОИСКОВЫХ СИСТЕМ

3. ИСПОЛЬЗУЙ СЛОЖНЫЕ И РАЗНЫЕ ПАРОЛИ. ТАКИМ ОБРАЗОМ, ЕСЛИ ТЕБЯ ВЗЛОМАЮТ, ТО ЗЛОУМЫШЛЕННИКИ ПОЛУЧАТ ДОСТУП ТОЛЬКО К ОДНОМУ ТВОЕМУ ПРОФИЛЮ

4. ЕСЛИ ТЕБЯ ВЗЛОМАЛИ, ТО НЕОБХОДИМО ПРЕДУПРЕДИТЬ ВСЕХ СВОИХ ЗНАКОМЫХ, КОТОРЫЕ ДОБАВЛЕНЫ У ТЕБЯ В ДРУЗЬЯХ

5. УСТАНОВИ НАДЕЖНЫЙ ПАРОЛЬ (PIN) НА МОБИЛЬНЫЙ ТЕЛЕФОН И ОТКЛЮЧИ СОХРАНЕНИЕ ПАРОЛЯ В БРАУЗЕРЕ

7. НЕ ОТКРЫВАЙ ФАЙЛЫ И ДРУГИЕ ВЛОЖЕНИЯ В ПИСЬМАХ ДАЖЕ ЕСЛИ ОНИ ПРИШЛИ ОТ ТВОИХ ДРУЗЕЙ. ЛУЧШЕ УТОЧНИ У НИХ, ОТПРАВЛЯЛИ ЛИ ОНИ ТЕБЕ ЭТИ ФАЙЛЫ.