Кибербезопасность: как защитить личные данные в сети

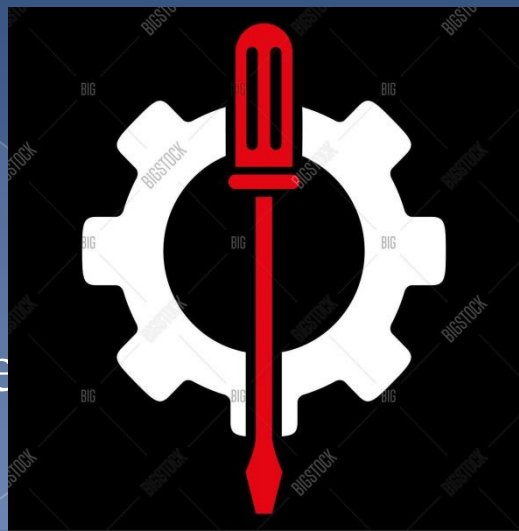
Над презентацией работал
Морозов Ян гр.113

Защита информации

- Сайты, приложения, социальные сети и поисковые системы постоянно занимаются тем, что собирают информацию о пользователях. Полученные данные используются для анализа интересов посетителей страниц, их покупательной активности и спроса, для изучения целевой аудитории и настроек рекламы.
- На первый взгляд, это выглядит удобным — браузеры запоминают пароли, хранят данные о поисковых запросах и страницах, которые вы посетили. С другой стороны, этими данными легко могут воспользоваться злоумышленники. Ваш аккаунт могут взломать, а личные данные — передать третьим лицам, которые используют их в мошеннических или других преступных целях. Чтобы этого не произошло, соблюдайте несколько

Настройки браузер

- Не разрешайте браузеру автоматически запоминать пароли к личным сайтам и страницам, а лучше отключите эту опцию в настройках. Особенно это касается сайтов, где необходимо вводить номера документов или банковской карты. Автосохранение паролей увеличивает риск взлома личных страниц: если злоумышленник получит доступ к вашему компьютеру, ему не составит никакого труда извлечь эти данные из памяти браузера.
- Отключите синхронизацию браузера на компьютере и в смартфоне. Если этого не сделать, при утере телефона все личные страницы и аккаунты станут доступны для посторонних.



Пароли

- Это основной способ защиты ваших личных данных в интернете, поэтому к нему нужно отнестись с особым вниманием.
- Не храните информацию о паролях на компьютере, который используется для выхода в интернет. Конечно, лучше всего держать пароли в голове. Если же пароль слишком сложный, лучше запишите его отдельно на лист бумаги или в блокнот, и храните в надёжном месте.
- Пользуйтесь двухэтапной аутентификацией — так ваши аккаунты будут надёжно защищены. Регулярно проверяйте почту и SMS-сообщения — если вам приходят подозрительные уведомления, вы всегда сможете пресечь попытки злоумышленников.
- Не используйте для паролей информацию, которую злоумышленники могут найти самостоятельно: дату рождения, номера документов, телефонов, имена ваших друзей и родственников, адрес и так далее.
- Придумывайте сложные пароли длиной не менее 8 символов с использованием заглавных и строчных букв, цифр, специальных значков %$#.
- Не используйте одинаковые пароли на разных сайтах.
- Регулярно меняйте пароли.

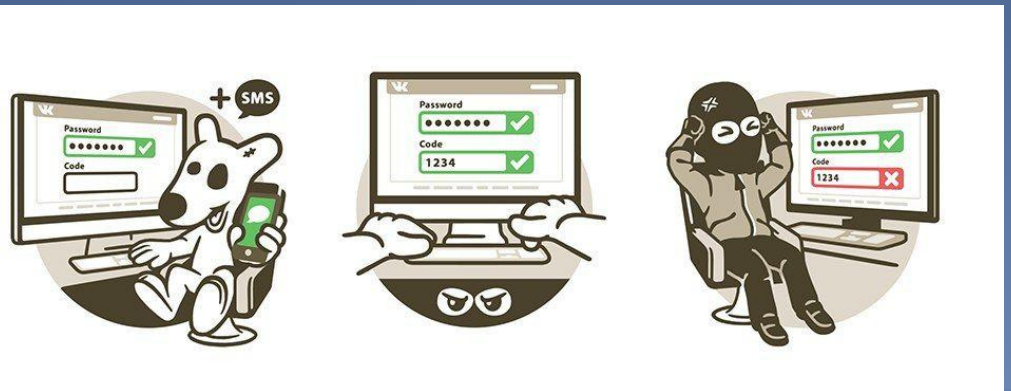
Безопасность страницы

Разрешения для приложений

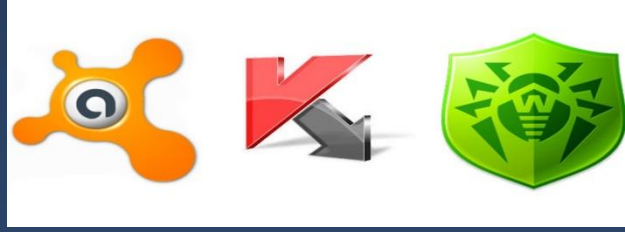
- Многие приложения запрашивают данные об электронной почте или доступ к камере, фотогалерее и микрофону. Не выдавайте разрешений автоматически, следите за тем, какую информацию запрашивает приложение. В некоторых случаях разумнее вообще отказаться от его использования, чтобы не передавать личные данные о себе неизвестным лицам.

МЕТОДЫ ЗАЩИТЫ ОТ ВЗЛОМА

- Внимание и осторожность во время серфинга в интернете – первый пункт. Даже самое лучшее ПО для защиты компьютера не поможет, если вы будете бездумно кликать и скачивать.



АНТИВИРУС



- Антивирусная защита должна быть всегда включена, библиотеки обновлены до актуальной версии, а профилактическую диагностику нужно проводить не реже, чем раз в месяц. Считайте, что это аксиома, которая не требует доказательств и не слушайте тех, кто говорит, что такое ПО «садит»

VPN

- Virtual Private Network – особый метод организации доступа. С помощью сложных алгоритмов специальное ПО создает запутанную сеть узлов, а также шифрует трафик. В результате отследить местоположение компьютера, узнать историю посещений и другую информацию о пользователе невозможно. Точнее, это настолько трудоемкая и затратная по

НАСТРОЙКА ФАЙЕРВОЛА И ЗАКРЫТИЕ ЛИШНИХ ПОРТОВ

- Многие пользователи не догадываются, что злоумышленники могут получить контроль над ПК даже без вашего участия. Соединение с Интернет – это двусторонний канал, поэтому важно заблокировать все виды доступа к вашем компьютеру, кроме служебных и защищенных. Лучше обратиться для этого к системному администратору – процедура займет пару минут.


Спасибо за
внимание

- https://yandex.ru/turbo?text=https%3A%2F%2Fmedia.foxford.ru%2Fcybersecurity%2F
- https://proxy.am/ru/articles/bezopasnost-v-seti-kak-zashhitit-svoj-kompyuter-ot-vzloma