Как обезопасить себя в интернете

Немного статистики

22%
сталкивались с кражей аккаунтов в социальных сетях или играх

15%
теряли данные из-за компьютерного вируса

14%
отметили, что им писали странные сообщения взрослые

10%
сталкивались с мошенничеством с использованием фальшивых сайтов и писем

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 простых правил.

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.

Изучение политики конфиденциальности

Прежде чем установить приложение или браузерное расширение, воспользоваться онлайн-сервисом или зарегистрироваться в социальной сети, обязательно изучите политику конфиденциальности. Убедитесь, что приложение или сайт не получает права распоряжаться вашими личными данными — фотографиями, электронным адресом или номером телефона.

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.

Настройки браузера

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.

Чистка cookies

Файлы cookies — это временные файлы интернета, которые хранятся на вашем устройстве и содержат информацию о сайтах, которые вы посещаете. Благодаря cookies сайты помнят ваши логины, пароли, электронную почту, историю интернет-заказов или состав корзины в интернет-магазине. С их помощью также можно отслеживать вашу активность в интернете, ваши интересы и предпочтения. Кроме того, с помощью cookies можно взломать ваш почтовый ящик и получить доступ к личной информации. Время от времени удаляйте файлы cookies на компьютере и в смартфоне. Сделать это можно в настройках браузера.

Блокировка рекламы

Специальные программы, блокирующие рекламу, одновременно отслеживают попытки посторонних программ получить информацию с вашего компьютера, поэтому для защиты личных данных полезно скачать и установить такой блокировщик.

Пройти бесплатный курс по кибербезопасности

Защищённое соединение

Сайты, содержащие конфиденциальную информацию пользователей (сайты банков, государственных учреждений, онлайн-магазинов), обычно используют специальные протоколы передачи данных. При защищённом соединении данные шифруются с помощью технологии SSL, после чего информация становится недоступна для третьих лиц. Если в адресной строке браузера перед адресом сайта https:// вы видите зелёный замочек, значит, сайт использует защищённое соединение. Обращайте на это внимание,

когда вводите на сайте логин, пароль, номер банковской карты или другие личные данные.

Домашний Wi-Fi

Пользоваться открытыми сетями Wi-Fi в кафе или торговом центре небезопасно, злоумышленники могут использовать их для взлома компьютера или смартфона и кражи паролей. В общественном месте не заходите на сайты, которые требуют ввода паролей и личных данных, делайте это по мобильной сети или через домашний Wi-Fi.

Безопасное общение

Одна из главных функций интернета в современном обществе — общение. Люди не только вводят личные данные на сайтах, но и взаимодействуют с другими пользователями: обмениваются информацией, ведут переписку, заводят друзей.

И здесь пользователя подстерегают новые опасности — травля в сети, мошенничество или угроза личной безопасности.

Кибербуллинг

Травля по интернету — это угрозы и оскорбления от агрессивно настроенных пользователей в адрес другого пользователя. Заниматься кибербуллингом в ваш адрес может один или несколько человек. Чтобы не пострадать от подобной травли, соблюдайте несколько правил:

1. Не отвечайте на агрессивные сообщения — обидчики только и ждут вашей ответной реакции.
2. Занесите пользователей в чёрный список.
3. Сообщите о происходящем технической поддержке социальной сети. Вам помогут заблокировать пользователя или же написать на него жалобу.
4. Делайте скриншоты переписки, содержащей оскорбления и угрозы, чтобы в случае необходимости использовать её как доказательство травли против вас. На скриншотах должен быть виден текст сообщения и имя отправителя. Не полагайтесь на хранение переписки — в некоторых соцсетях и мессенджерах можно удалить отправленные сообщения.
5. Сообщите о происходящем взрослым. Если угрозы направлены на жизнь и здоровье, то имеет смысл обратиться в правоохранительные органы.

Онлайн-груминг

Грумингом называют различные виды мошенничества в сети, когда преступники обманом втираются в доверие к пользователям и получают от них личные данные или деньги за несуществующие товары и услуги. Часто мошенники пользуются уже взломанными аккаунтами пользователей для рассылки сообщений по списку контактов.

Если ваш друг или знакомый присылает сообщение с просьбой перечислить ему денег на банковскую карту, обязательно уточните у него другим способом (лично, по телефону или в другой социальной сети или мессенджере), что это действительно он.

Мошенники расспрашивают пользователей, особенно детей и подростков, о финансовом положении семьи, о работе родителей, о поездках и других перемещениях, выясняют адреса, телефоны, номера машин. Вся эта информация может быть использована для совершения преступления.

Для защиты от интернет-мошенничества соблюдайте несколько правил:

1. Регистрируясь в социальной сети, закрывайте свой аккаунт от посторонних, а посты с личной информацией публикуйте в режиме «для друзей».
2. Ограничьте контакты в сети с незнакомыми людьми. Никогда не сообщайте им личных данных. Если незнакомый человек хочет встретиться лично, сообщите об этом родителям. Ни в коем случае не ходите на такие встречи в одиночестве.
3. Не публикуйте в открытом доступе личные данные: адрес, номера документов, банковских карт, билетов и так далее.
4. Не переходите по подозрительным ссылкам, даже если получили их по почте или в сообщении от знакомого пользователя.
5. Не скачивайте файлы на подозрительных или ненадёжных сайтах.

Что нужно запомнить

☺ Внимательно отнеситесь к созданию и хранению паролей.

 Изучите политику конфиденциальности сайтов и приложений, запретите вашему браузеру автоматически сохранять пароли, регулярно удаляйте cookies.

 Пользуйтесь блокировщиками рекламы.

☺ Оставляйте личные данные только на сайтах с защищённым соединением. Не пользуйтесь общественными сетями Wi-Fi для передачи конфиденциальной информации.

😖 Если вы столкнулись с травлей в сети, блокируйте пользователя, который отправляет вам агрессивные сообщения. Обратитесь в службу поддержки сайта или социальной сети, сообщите родителям. Не вступайте в дискуссии с агрессивно настроенными пользователями.

 Чтобы не стать жертвой интернет-мошенников, перепроверяйте всю информацию, полученную по электронной почте или в сообщениях социальных сетей и мессенджеров, не сообщайте незнакомым людям и не публикуйте в открытом доступе личные данные.