

Как защитить личные данные в сети

Чтобы обеспечить безопасность в интернете и защитить свои данные, можно следовать перечисленным ниже рекомендациям.

Используйте многофакторную аутентификацию везде, где возможно

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используется два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация:

Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или адрес электронной почты.

Ответы на личные вопросы безопасности.

Отпечаток пальца или другая биометрическая информация, например голосовые данные или лицо.

Многофакторная аутентификация снижает вероятность кибератаки. Чтобы защитить онлайн-аккаунты, рекомендуется по возможности использовать многофакторную аутентификацию. Для обеспечения безопасности в интернете можно также можете применять сторонние приложения проверки подлинности, такие как Google Authenticator и Authy.

Используйте сетевой экран

Сетевой экран исполняет роль барьера между вашим компьютером и сетью, например интернетом. Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами. Часто сетевой экран входит в состав операционной системы или системы безопасности. Для обеспечения максимальной безопасности в интернете рекомендуется убедиться, что сетевой экран включен и настроено автоматическое обновление.

Внимательно относитесь к выбору браузера

Браузер – это основной инструмент для выхода в интернет, он играет ключевую роль в обеспечении безопасности в интернете. Хороший веб-браузер должен быть безопасным и обеспечивать защиту от утечки данных. Фонд свободы прессы составил подробное руководство, описывающее плюсы и минусы безопасности основных веб-браузеров.

Создавайте надежные пароли и используйте менеджер паролей

Надежный пароль помогает обеспечить безопасность в интернете. Он обладает следующими свойствами: Длинный: минимум 12 символов, в идеале, даже больше.

Содержит заглавные и строчные буквы, а также специальные символы и цифры.

Не очевидный: в пароле не используются комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.

Не содержит запоминающихся сочетаний клавиш.

Замена букв и цифр похожими символами, например, “P@ssw0rd” вместо “password”, сейчас уже не является эффективной мерой – злоумышленники умеют обходить такую замену. Чем сложнее ваш пароль, тем сложнее его взломать. Использование менеджера паролей позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли.

Используйте на устройствах последнюю версию программы безопасности

Антивирус, обеспечивающий защиту в интернете, очень важен для сохранения конфиденциальности и безопасности. Лучшие программы интернет-безопасности защищают от различных видов атак, а также обеспечивают безопасность данных в интернете. Очень важно обновлять антивирусное программное обеспечение. Большинство современных программ обновляются автоматически, что гарантирует защиту от последних угроз интернет-безопасности.