"Информационная безопасность сети"

Правила безопасности при работе в сети

Вы защитите компьютер от большинства интернет-угроз, если будете соблюдать простые правила безопасности.

Для более безопасной работы в Сети Интернет следует:

Обновляйте операционную систему

Вирусы используют уязвимости операционной системы. Вовремя обновляйте ОС, чтобы защититься от угроз.

Включите автоматическое обновление Windows: Windows 10, Windows 8,Windows 7, Windows XP

Нажмите Пуск → Параметры. На вкладке Центр обновления Windows нажмите ссылку Дополнительные параметры. В спискеВыберите, как устанавливать обновление нажмите пункт Автоматически (рекомендуется).

Нажмите правой кнопкой мыши кнопку Пуск → Панель управления (просмотр по категориям) → Система и безопасность → Включение и отключение автоматического обновления → Важные обновления. В списке выберите пункт Устанавливать обновления автоматически (рекомендуется).

Нажмите Пуск → Панель управления (просмотр по категориям) → Система и безопасность → Включение и отключение автоматического обновления → Важные обновления. В списке выберите пункт Устанавливать обновления автоматически (рекомендуется).

Нажмите Пуск → Панель управления → Центр обеспечения безопасности → Автоматическое обновление → Автоматически.

Примечание. Чем выше версия операционной системы, тем надежнее она защищена. К примеру, Windows 7 безопаснее Windows XP.

Скачайте последнюю версию браузера

Большинство браузеров (например, Яндекс.Браузер, Mozilla Firefox) обновляются автоматически. Если этого почему-то не происходит, скачайте последнюю версию на официальном сайте и установите ее.

Установите антивирус

Из года в год компания AV Comparatives выделяет в числе лучших антивирусы Kaspersky, ESET,Bitdefender, Avast! Free Antivirus, AVIRA, Panda Cloud Antivirus, F-Secure SAFE.

Некоторые антивирусы из списка бесплатны, например Kaspersky, Avast! Free Antivirus и Panda Cloud Antivirus.

Примечание. Если вы подключены к интернету, антивирусы обновляются автоматически.

Пользуйтесь учетной записью с ограниченными правами

Работайте под учетной записью с ограниченными полномочиями. Это безопаснее: вирус не внедрится в систему, даже если проникнет в компьютер. Защитите паролем вход под учетной записью администратора.

Сразу удалять письма подозрительного содержания.

Не обращать внимание на предложения легкого заработка.

Включите файрвол

Файрвол проверяет данные, которыми обмениваются компьютер и интернет, и блокирует подозрительные соединения. Он дополнительно защищает операционную систему от вирусов.

Включите файрвол: Windows 10,Windows 8, Windows 7,Windows XP.

Нажмите правой кнопкой мыши кнопку Пуск → Панель управления (просмотр по категориям) → Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows (в левом меню страницы). Включите брандмауэр для всех сетей — доменных, частных и общественных.

Нажмите правой кнопкой мыши кнопку Пуск → Панель управления (просмотр по категориям) → Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows (в левом меню страницы). Включите брандмауэр для всех сетей — доменных, частных и общественных.

Пуск → Панель управления (просмотр по категориям) → Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows (в левом меню страницы). Включите брандмауэр для всех сетей — доменных, частных и общественных.

Пуск → Панель управления → Центр обеспечения безопасности → Брандмауэр Windows → Включить.

Придумывайте сложные пароли

Хороший пароль содержит не меньше 8 символов, среди них — цифры, буквы и специальные символы: ! # $ % ^ { } [ ] ( ) " : \ |.

Не используйте простые сочетания вроде 123456, qwerty, password. Посмотрите на подборки худших паролей в интернете. Мошенники часто взламывают учетные записи, перебирая варианты из таких списков.

Меняйте пароли хотя бы раз в три месяца.

Выбирайте легальное ПО

Скачивайте программы только с официальных сайтов. Не пользуйтесь взломанными версиями. Запуская их, вы рискуете безопасностью: злоумышленники внедряют вирусы в установочные файлы таких программ.

Делайте резервные копии ценных данных

Вредоносные программы портят данные, шифруют жесткие диски и предлагают разблокировать их за деньги. Платить — значит финансировать разработку новых, еще более изощренных вирусов. Делайте резервные копии информации на других носителях. Подойдут CD, DVD, внешние диски, флеш-накопители, облачные сервисы.

Не открывать файлы, скачанные из непроверенных источников.

Не высылать никому свои логины и пароли.

С платежными системами безопаснее работать через специальные приложения, а не через официальный сайт.

Следить за интернет-трафиком. Резкое увеличение трафика без всякой причины – серьезный повод для беспокойства.

Игнорировать сообщения о крупных выигрышах или получении наследства.

Использовать только проверенные варианты при совершении покупок в интернет – магазинах.

Включить обновление ОС

Кроме этого, полезно делать резервные копии наиболее ценных данных, так как вредоносные программы и вирусы могут заблокировать доступ к файлам, зашифровать или уничтожить их. Так удастся сохранить все необходимое и не беспокоиться о восстановлении доступа к заблокированным данным.

Несмотря на то, что система с отключенным брандмауэром и антивирусом не ограничивает работу пользователя, не снижает быстродействие системы, не требует авторизации и переключения учетных записей, иногда стоит пожертвовать удобством ради безопасности. Потому что отсутствие защиты может привести к потере данных, которая будет стоить намного дороже, ведь среди них могут быть результаты работы, фотографии, коллекции, данные для авторизации, платежные данные, сообщения и другая личная информация. Даже если учитывать только потери времени, то на однократное восстановление данных и работоспособности системы обычно уходит больше, чем на соблюдение правил техники безопасности работы с интернетом.

Помимо технических способов защитить компьютер от угроз, пользователь должен руководствоваться здравым смыслом и быть внимательным. Для этого следует знать об уловках злоумышленников, чтобы в дальнейшем не попадаться на них и не подвергать систему риску заражения.

Советы по безопасности при работе в Интернете:

Не заходите на подозрительные сайты и ссылки, полученные от незнакомых людей. Не нажимайте на всплывающую рекламу.

Используйте сложные пароли.

Не сообщайте свои данные посторонним.

При авторизации используйте экранную клавиатуру.

При использовании браузера установите специальные дополнения такие, как например, дополнение **Adblock Plus**. При использовании этого дополнения вы не увидите большую часть рекламы, том числе и вредоносную.

Проверяйте и контролируйте настройки антивируса и брандмауэра.

Не открывайте письма от неизвестных отправителей, и не загружайте прикрепленные к таким письмам файлы.

Помните о снижении безопасности при использовании беспроводного соединения в общественных местах.