

Рекомендации по безопасному использованию Wi-Fi от Google

Обращайте внимание на адрес сайта: кажется ли он подлинным? Удостоверьтесь, что он начинается с комбинации <https://> — это значит, что ваше соединение с веб-сайтом зашифровано и злоумышленникам будет сложнее получить ваши личные данные. Кроме того, в некоторых браузерах рядом с обозначением протокола <https://> отображается значок замка: это значит, что соединение защищено и более безопасно.

При подключении через общедоступную сеть Wi-Fi любой желающий может отследить информацию, которой обменивается ваш компьютер и точка доступа. Не пользуйтесь платежными системами и другими важными сервисами при работе с таким соединением.

При использовании Wi-Fi у себя дома обязательно защитите сеть паролем. Не используйте пароль, предлагаемый по умолчанию, он может быть известен злоумышленникам. Следуйте инструкциям интернет-провайдера и используйте собственную комбинацию символов. В настройках точки доступа выбирайте протокол WPA2 — на сегодняшний день он наиболее эффективен.

Более подробные рекомендации по безопасности в Сети — на образовательном портале Google «Полезно знать»: <http://www.google.ru/intl/ru/goodtoknow/>.

Рекомендации для надежности пароля

1. Надежный пароль — это важный элемент защиты, который позволяет значительно повысить безопасность онлайн-транзакций. Ключевые элементы надежности пароля — длина и сложность. Идеальный пароль — это длинная комбинация различных знаков, которая включает в себя буквы и цифры, а также знаки пунктуации и символы. Если это возможно, старайтесь использовать восемь и более знаков.

2. Не используйте один и тот же пароль везде. Злоумышленники крадут учетные данные на сайтах со слабой безопасностью, а затем пытаются использовать те же пароли и имена пользователя, чтобы получить доступ к более защищенным ресурсам, например, банковским сайтам.

3. Старайтесь регулярно менять свои пароли. Установите автоматическое напоминание, которое будет уведомлять вас о необходимости сменить пароли на используемых вами ресурсах.

4. Чем больше разнообразных символов вы используете в пароле, тем лучше. Тем не менее, помните, что программы для подбора паролей автоматически проверяют их на замену распространенных комбинаций букв на символы, например «to» на «2».

5. Обеспечьте защиту для записанных паролей. Будьте внимательны к тому, где вы храните или записываете пароли. Вместо того чтобы придумывать пароли, а тем более их помнить, можно использовать автоматизированные средства генерации и хранения паролей, например: KeePass (<http://keepass.info/download.html/>).

6. Будьте аккуратны с паролем к своему почтовому ящику. Именно он, как правило, служит ключом для несанкционированного доступа к разным сайтам от имени пользователя, поскольку через email производится регистрация практически на любых сервисах.

Посмотрите также более подробные рекомендации по созданию надежных паролей на портале Google «Полезно знать»: <http://www.google.ru/intl/ru/goodtoknow/online-safety/passwords/>.

Как защитить компьютер или другое устройство от вирусов: рекомендации от Google

- Регулярно обновляйте браузер и операционную систему. Обычно операционные системы и приложения сами сообщают вам о том, что их можно обновить. Не откладывайте обновление на потом! Уязвимостями в устаревших версиях ПО могут пользоваться злоумышленники, чтобы получить доступ к вашим данным. Браузер Chrome автоматически обновляется до последней версии при каждом запуске, обеспечивая надежную защиту без усилий со стороны пользователя.
- Внимательно следите за тем, какие веб-сайты вы открываете и что загружаете. Это относится к музыке, фильмам, файлам, плагинам и дополнениям для браузера и т. д. Остерегайтесь всплывающих окон, которые предлагают вам установить ПО или устранить неполадки. В таких сообщениях часто указано, что ваш компьютер заражен и предлагаемое ПО может исправить проблему. Не верьте этому. Закройте всплывающее окно и не нажимайте на ссылки в нем. Не открывайте файлы неизвестных типов и не нажимайте на подозрительные предупреждения в браузере, предлагающие открыть какие-либо файлы. Если вы все-таки перешли на предлагаемую страницу, иногда вредоносное ПО не дает покинуть ее (например, отображает запрос на загрузку снова и снова). В этом случае нужно закрыть браузер в диспетчере задач или мониторе активности вашей операционной системы.
- Мы рекомендуем добавить нужные вам сайты в закладки, переходить на них с помощью поисковой системы или вводить URL в адресную строку браузера. Убедитесь, что адрес веб-сайта начинается с `https://`. Это протокол зашифрованного подключения, которое обеспечивает более эффективную защиту данных.
- Устанавливайте ПО только из надежных источников.
- Какова репутация магазина? Пользуйтесь только авторитетными ресурсами, такими как встроенный магазин приложений или сайт разработчика, а не сторонними сайтами для загрузки ПО. Мы также рекомендуем изучить отзывы о разработчике. Попробуйте найти обзор интересующего вас приложения или комментарии пользователей. Если окажется, что оно многим не понравилось или вызывало технические проблемы, вряд ли стоит его загружать.
- Обнаружив после загрузки любые подозрительные признаки (устройство медленно работает, появляются всплывающие окна или выполняются непонятные платежи), немедленно удалите ПО и проверьте систему с помощью последней версии антивирусной программы.
- Многие браузеры предупреждают пользователя о том, что он пытается открыть сайт, распространяющий вредоносное ПО. Получив такое предупреждение, посмотрите на URL и подумайте, стоит ли переходить на такой сайт. Даже если вы уже бывали на нем, с вашего прошлого посещения он мог быть взломан. В таком случае не следует пользоваться веб-ресурсом, пока владельцы не восстановят его.
- Если ваш компьютер заражен вредоносным ПО, постарайтесь немедленно его удалить. Чтобы очистить компьютер, просканируйте его с помощью хотя бы одного, а лучше нескольких высококачественных антивирусов. Эффективность таких мер не гарантирована, но последние версии антивирусного ПО обычно справляются с возложенными на них задачами. На сайте <http://av-comparatives.org/> можно найти сведения о различных антивирусных программах и ознакомиться с результатами их тестирования.

Подробнее на портале Google «Полезно знать»:
<http://www.google.ru/intl/ru/goodtoknow/online-safety/device/>

Контроль над личной информацией

Если вы не хотите, чтобы ваша личная информация появлялась в Сети без вашего ведома, воспользуйтесь сервисом «Я в Интернете». Благодаря нему вы сможете получать оповещения, как только кто-то опубликует в Интернете какие-либо сведения о вас, например ваши адреса электронной почты или номера телефонов.

Чтобы настроить оповещения, выполните следующие действия:

- Войдите в свой аккаунт Google и откройте раздел «Я в Интернете».
- Нажмите «Мои оповещения».
- Нажмите красную кнопку, чтобы создать оповещение.
- Вы увидите поле со своим именем пользователя. Нажмите на него, чтобы просмотреть другие личные данные, публикацию которых можно отслеживать (например, адрес электронной почты или мобильный телефон). Для создания оповещения нажмите «Добавить», для редактирования — значок карандаша, а для удаления — значок корзины.
- С помощью списка «Частота отправки» выберите, как часто вы хотите получать оповещения.
- С помощью списка «Доставка» укажите адрес электронной почты для отправки оповещений.

Подробнее в соответствующем разделе портала Google «Полезно знать»:
<http://www.google.ru/intl/ru/goodtoknow/>

Сервисы Google — образовательные ресурсы

Интернет открывает огромное пространство для образования, в том числе для людей с ограниченными физическими возможностями, — в этом заключается большое преимущество сетевых технологий по сравнению с офлайновой эпохой. Вот несколько примеров из опыта Google, который может быть интересен в рамках образовательного процесса:

- «Google Книги» позволяют пользователям осуществлять поиск по текстам более 15 млн книг на 400 языках из более 100 стран мира (<http://books.google.ru/>).
- С помощью проекта Ngram Viewer, построенного на «Google Книгах», можно провести лингвистический анализ текстов мировой литературы за разные периоды времени. Попробуйте: <http://books.google.com/ngrams/>.
- «Google Академия» индексирует полные тексты научных публикаций разных форматов и дисциплин и позволяет анализировать большинство рецензируемых онлайн-журналов крупнейших научных издательств Европы и Америки, включая труды на русском языке (http://scholar.google.com/schhp?hl=ru&as_sdt=0/).
- Проект «Просмотр улиц» предоставляет доступ к ключевым объектам культурного наследия разных стран, включая Римский Колизей и Римский Форум, Помпеи, Собор Парижской Богоматери, Вестминстерское аббатство и многие другие. К проекту присоединилась и Россия. С помощью технологии «Просмотр улиц» можно даже совершить виртуальное путешествие по маршруту «Москва — Владивосток», наслаждаясь стуком колес или слушая аудиокнигу «Война и мир», «Мертвые души» и не только (<http://www.google.ru/intl/ru/landing/transsib/>).
- С помощью «Арт-проекта Google» пользователи Интернета могут совершить виртуальную экскурсию по более чем 200 музеям из 40 стран мира. Из российских музеев в проекте участвуют Государственный музей изобразительных искусств имени А. С. Пушкина, Русский музей, Государственная Третьяковская галерея, Государственный Эрмитаж и Музей имени Н. К. Рериха. В 2012 году 46 участников проекта выбрали по одному произведению искусства, которые были оцифрованы в сверхвысоком гигапиксельном разрешении с использованием уникальных технологий. В том числе были сняты две картины из российских музеев: ГМИИ им. А. С. Пушкина предоставил для съемки произведение Джованни Антонио Каналь Каналетто «Возвращение Бучинторо к молу у Дворца Дожей», а Русский музей — «Последний день Помпеи» Карла Брюллова. Каждый снимок состоит из 7 млрд пикселей, что позволяет зрителю изучать мельчайшие детали картины или патину, которые невозможно заметить невооруженным глазом. В рамках проекта можно не только посмотреть произведения искусства, но и совершить виртуальную экскурсию по залам музеев с помощью специальной панорамной технологии съемки (<http://googleartproject.com/>).

- Изучать историю можно с помощью исторического архива «Академии культуры Google», представляющей собой платформу для цифровых архивов разных стран по истории современности и не только (<http://www.google.com/culturalinstitute/#!/home/>).
- Видеохостинг YouTube содержит огромное количество профессионального видео, полезного контента, в том числе образовательного. Это каналы о кино, искусстве, спорте, новостях, мультипликации и многом другом. Свои официальные каналы имеют органы государственной власти, различные СМИ. На каналах «Мосфильма» и «Ленфильма» собрана классика отечественного кинематографа. Большой театр транслирует балеты в режиме реального времени.