**"Как уберечь себя в сети Интернет и при использовании мобильной связи" (5–11-е классы)**

**Что такое приватность данных?**

Объем цифровой информации в мире удваивается каждые два года. По большей части это личные данные пользователей.

Мы пользуемся смартфонами, компьютерами, планшетами, IoT-устройствами – все они собирают информацию об использовании. Мы оплачиваем покупки в онлайн-банках, бронируем билеты и общаемся с друзьями онлайн. Наши дети делают домашнее задание онлайн. В интернете мы работаем, общаемся и даже ищем вторую половинку.

Интернет-пространство меняется с бешеной скоростью, а проблемы с приватностью данных усугубляются.

**Угрожает ли интернет вашей приватности?**

Информация – это деньги. Это главная причина, по которой вашим личным данным угрожает опасность.

Рекламщики охотятся за вашей историей поиска в браузере – они могут извлечь большую выгоду из этой информации. Допустим, вы вбиваете в строке поиска «квартира в аренду» или «купить квартиру». Увидев историю вашего поиска, рекламщик поймет, что вы вскоре планируете переезжать. Это повод показывать вам рекламу грузового такси, мебели, магазинов стройматериалов и страховых компаний.

Это вполне законно. Однако [на ваших данных могут зарабатывать](https://www.theguardian.com/technology/2017/mar/30/privacy-protection-web-browsing-history-data-congress) и мошенники. В дарквебе в открытую торгуют данными кредитных карт, поэтому для киберпреступника получить доступ к системе бронирования авиакомпании или к базе клиентов онлайн-магазина – большая удача.

Злоумышленники могут использовать любую информацию, которую вы выкладываете в Сеть, – именно поэтому важно следить за безопасностью личных данных. Давайте разберемся, почему приватность в Сети так важна и как вы можете защитить личные данные.

**Что такое приватность в Сети и почему она так важна?**

Вмешательство в вашу личную жизнь в интернете несет реальную опасность. Злоумышленники могут взломать вашу электронную почту, украсть вашу личность, распространить информацию о состоянии вашего здоровья без вашего ведома или передать ваши банковские данные третьим лицам.

Риски намного серьезнее, чем думает большинство людей. Дело в том, что происходит с личной информацией после получения доступа к ней. Использование больших данных предполагает, что вашу историю поиска могут проанализировать и сделать на ее основе нежелательные для вас выводы. Допустим, девушка заказывает добавки с фолиевой кислотой и увлажняющий крем без отдушек. Маркетологи на основе ее покупок или истории поиска могут сделать вывод, что она ждет ребенка, и выслать на ее почтовый ящик рекламные материалы для беременных.

Если девушка живет с родителями или еще не рассказала о беременности партнеру, она вряд ли оценит такое внимание.

Это лишь один из многих примеров, доказывающих, что приватность в интернете касается не только [защиты учетной записи в системе онлайн-банкинга](https://www.kaspersky.ru/resource-center/threats/online-banking-theft) или аккаунта в социальных сетях. Каждый раз, когда вы заходите на сайт или скачиваете приложение, ваши данные сохраняются – возможно, без вашего согласия. Вы можете даже не подозревать об этом. Вы, скорее всего, желаете знать, куда отправляются ваши личные данные и как они будут использованы, а может, и вовсе против того, чтобы их собирали.

**Как защитить личные данные в интернете: безопасное соединение**

Один из способов защитить свои личные данные в интернете – использовать безопасные соединения. Когда вы ищете что-то в интернете, отправляете письмо или пользуетесь навигатором в телефоне, вы обмениваетесь данными с сервером. Пока информация находится в пути, ее нужно защищать.

Один из первых шагов к защите личных данных в интернете – убедиться, что ваше соединение безопасно. На домашнем роутере нужно установить надежный пароль, который сложно подобрать. Было бы неплохо поменять и имя пользователя: часто в нем фигурирует имя вашего провайдера или производителя маршрутизатора. Такая информация может пригодиться злоумышленникам. Если у вас есть домашняя сеть Wi-Fi, применяйте протокол шифрования WPA, и тогда чужие ей не воспользуются.

Теперь бесплатный Wi-Fi есть во многих кафе, гостиницах и других общественных местах – вы можете сидеть в интернете практически где угодно. Но будьте осторожны: [общественный Wi-Fi крайне небезопасен](https://www.kaspersky.ru/resource-center/preemptive-safety/public-wifi). Если в открытой сети используется простая аутентификация, к ней легко подключиться. Однако так же легко вы можете стать жертвой киберпреступника. Не используйте общественный Wi-Fi для оплаты покупок и перевода средств или обмена конфиденциальными данными.

Воспользуйтесь виртуальной частной сетью (VPN) – она поможет защитить Wi-Fi от взлома. Эта технология устанавливает между вашим устройством и сервером соединение, защищенное шифрованием. С ее помощью вы скроете свои действия в интернете от посторонних глаз. Так что VPN обеспечит вам безопасность, даже если вы пользуетесь общественным Wi-Fi.

Для передачи конфиденциальных данных лучше использовать безопасный браузер и сайты с протоколом HTTPS, а не HTTP. HTTP-страница может быть взломана шпионской программой, которая будет запоминать все введенные вами данные (например, логин и пароль от онлайн-кабинета в банке).

HTTPS-сайты используют протоколы SSL и TSL для шифрования вашего соединения. Проще говоря, такой протокол создает защищенную цифровую среду, в которой вы можете обмениваться данными через браузер без риска быть «подслушанными» – что-то вроде безопасного рукопожатия. При использовании SSL в адресной строке вашего браузера появится изображение замка, а само название веб-сайта будет начинаться не с http, а с https. Если хотите узнать больше о сертификате сайта, нажмите на замок.

Некоторые онлайн-мессенджеры очень ненадежны в плане приватности. Например, ваша переписка в Facebook не защищена, пока вы не включите режим «Секретная переписка». Эта функция есть только в приложении Facebook Messenger для устройств iPhone и Android, в браузерной версии она недоступна. Мессенджеры WhatsApp и Viber, напротив, используют шифрование, поэтому они намного безопаснее.

## Как защитить личные данные в интернете: не выкладывайте все подряд

Не стоит публиковать в интернете все сведения о себе. Наверняка какие-то аспекты вашей личной жизни вы бы не хотели афишировать по вполне обычным причинам. Кто-то стесняется своей фамилии, а у кого-то могут быть хобби, о которых они не хотят рассказывать коллегам. Ваши личные данные будут в безопасности, [если вы будете тщательно отбирать публикуемую информацию](https://www.kaspersky.ru/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online) и людей, которые смогут видеть ее.

Подумайте о том, как личная информация, которой вы делитесь в социальных сетях, может повлиять на вашу безопасность. Проблема приватности в интернете — это проблема безопасности в реальной жизни. Например, вы отдыхаете в Диснейленде и решили поделиться этой новостью с друзьями, что вполне нормально. Но домушники тоже могут оценить эту новость. Если для контрольного вопроса в банке вы выбрали девичью фамилию матери, первый автомобиль или имя своего питомца, не публикуйте такую информацию в социальных сетях.

Внимательно следите за тем, какая информация на каких социальных платформах становится видна другим пользователям автоматически. Это может быть ваше местоположение или то, с кем вы сейчас проводите время. Многие люди не осознают, что в поле «О себе» указывают информацию, которой мошенникам вполне достаточно для успешной кражи личных данных или проведения атаки с использованием социальной инженерии. Указали дату рождения, чтобы друзья знали, когда вас поздравлять? Учтите, что эта информация используется в онлайн-банке и других конфиденциальных аккаунтах в качестве идентификатора. Изучите настройки приватности в социальных сетях, чтобы ограничить доступ к личной информации.

Если вы пользуетесь LinkedIn, то можете и не знать, что на вкладке «Действия» отображается все, что вы только что делали. Ваш работодатель может увидеть, что вы подписались на пару других компаний, и ваш поиск новой работы сразу перестанет быть тайной. Отключите эту функцию в настройках конфиденциальности, если не хотите, чтобы все ваши действия видели другие пользователи LinkedIn.

Многие грамотные пользователи Facebook сейчас открывают доступ к своим публикациям только друзьям. При этом если вы создадите «более публичную» запись, чтобы, например, попросить друзей поделиться с их друзьями ссылкой на какую-то предвыборную кампанию, настройки этого поста могут быть применены и ко всем последующим. Убедитесь, что к вашим записям по-прежнему по умолчанию открыт доступ только для друзей.

Мы начали говорить о друзьях. Уверены ли вы, что знаете всех из списка ваших друзей на Facebook? Нужно ли вам оставлять в списке человека, с которым вы познакомились в отпуске пять лет назад и с тех пор не общались? Вы можете [изменить настройки Facebook, чтобы защититься от злоумышленников](https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html), рассылающих поддельные заявки в друзья: разрешите добавляться к вам в друзья только «друзьям друзей». Так вы уменьшите шансы стать жертвой мошенников.

Возможно, стоит убрать адрес электронной почты или номер телефона из публичного доступа на своих страницах в социальных сетях. Разрешите показывать такие данные только друзьям или скройте их совсем. Вы также можете запретить поисковыми системам показывать вашу страницу в результатах поиска. В таком случае, если кто-то введет ваше имя в Google, он не увидит ни одной вашей записи на Facebook.