



**Главный  
радиочастотный  
центр**

# **Основные правила безопасности в социальных сетях**

Центр правовой помощи гражданам в цифровой среде



**Браузер** — это компьютерная программа-обозреватель, которая позволяет выполнять запросы и просматривать сайты.

Браузеры имеют несколько **режимов использования**:



## Основной режим

(браузер сохраняет много информации: история просмотров, закладки, пароли, изображения и др.)



## Режим синхронизации браузера с аккаунтом

(личная информация пользователя сохранится на серверах компании, будет работать автозаполнение и автоматический доступ к информации)



## Гостевой режим и режим инкогнито

(загружаемые сайты и файлы не будут записываться в историю)

Для входа в соцсети используйте только распространенные браузеры.  
Установите и обновляйте антивирусные программы, сканируйте компьютер на наличие вредоносного ПО.  
Устаревшие версии не могут гарантировать защиту устройства от ежедневно обновляющихся угроз информационной безопасности, а значит, и вашей личной безопасности.



Перед регистрацией в социальной сети ознакомьтесь с текстами **Согласия на обработку персональных данных, Пользовательским соглашением и Политикой конфиденциальности**, а также иными документами, размещенными на сайте. Так вы сможете понять, кому ваши персональные данные могут быть переданы.

**Пользовательское соглашение** регулирует отношения между владельцем сайта и посетителем:

- обладает силой договора
- в нем определяется статус контента, способ регистрации учетной записи, объем обрабатываемых персональных данных

**Политика конфиденциальности** встречается на сайтах, где применяются веб-технологии сбора и обработки персональных данных:



если на сайте нужно заполнять профиль при регистрации (почта, ФИО, пол)



если есть механизм подписки (например, на почтовую рассылку)



если нужно заполнить форму обратной связи (сайты подачи объявлений, оформления заказов)

В **Политике** владелец сайта:

- сообщает, каким образом, кому и когда он будет передавать конфиденциальную информацию, в том числе и персональные данные пользователя;
- указывает, какие права есть у пользователя, сколько хранятся данные, куда можно обратиться чтобы прекратить обработку личных данных.

**(!) Иногда в Политике конфиденциальности указывается возможность передачи данных непоименованным 3 лицам. Это запрещено законом.**



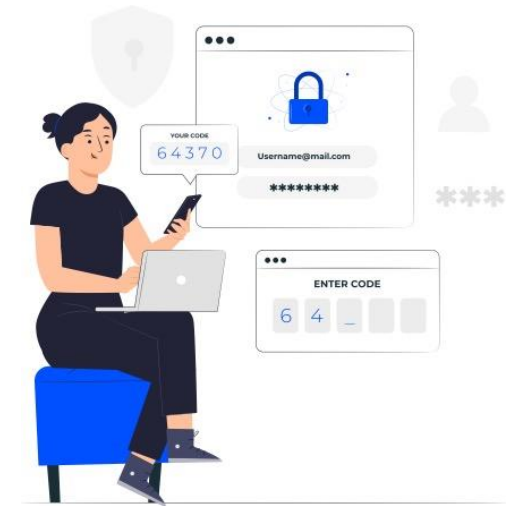
Используйте разные пароли для соцсети и для электронной почты, которую указываете в социальной сети. Пользуйтесь специализированными генераторами паролей или выбирайте сложные пароли, регулярно их меняйте и не храните в открытом виде.



Заведите два адреса электронной почты:

- частный – для переписки (который не публикуете в общедоступных источниках)
- публичный – для соцсетей, форумов, чатов и т.д.

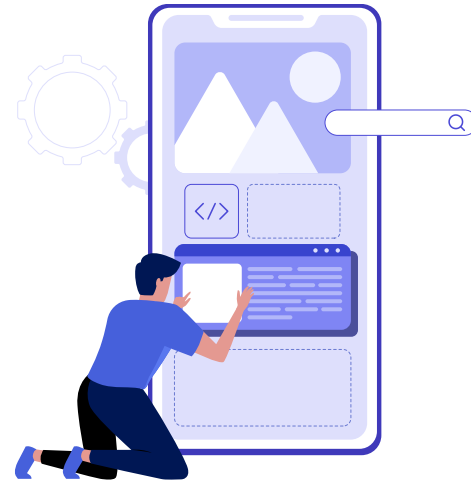
Если нужно сообщить свой приватный адрес в переписке, лучше сделать это способом, непригодным для автоматического прочтения сборщиком адресов, например, в виде картинки.



Установите двухфакторную идентификацию, чтобы иметь возможность подтвердить вход в ваш профиль с нового устройства с помощью дополнительного кода, направляемого в СМС-сообщении.



Настройте ваш профиль в социальной сети таким образом, чтобы только друзья могли его просматривать. Такая настройка лишит злоумышленников возможности получить доступ к информации, которую вы скрыли для просмотра незнакомцев.



Внимательно относитесь к информации, которую публикуете о себе в социальной сети. Используйте никнейм. Злоумышленник может использовать вашу личную информацию и войти в Вашу учетную запись, а также создать правдоподобные истории для злоупотребления вашим доверием и хищения ваших денег.



Перед тем как выложить фотографию, оцените каждую деталь: свой внешний вид, окружающую местность, людей, находящихся рядом с вами, и многое другое. Даже если вы сразу удалили публикацию, кто-то мог ее сохранить. Помните о возможных репутационных рисках.



Не устанавливайте приложения для соцсетей, которые позволяют отследить активность подписчиков на вашей странице.

Огромное количество пользователей ищут способ посмотреть, кто заходил на страницу, и, не разбираясь в теме, верят в то, что есть быстрое и бесплатное решение.

Как правило, при установке такие сервисы запрашивают логин и пароль от аккаунта – все это ухищрения хакеров, создающие риски последующего взлома страницы.



Не отправляйте важные документы через социальные сети и не публикуйте фотографии документов.

Часто обнаруживается, что молодые люди, когда получают водительские права, публикуют их фотографии в открытом доступе.

Таковыми фотографиями могут воспользоваться злоумышленники, изменив их с помощью графических редакторов.

Впоследствии от вашего они могут совершать действия, которые будут иметь юридически значимые последствия.

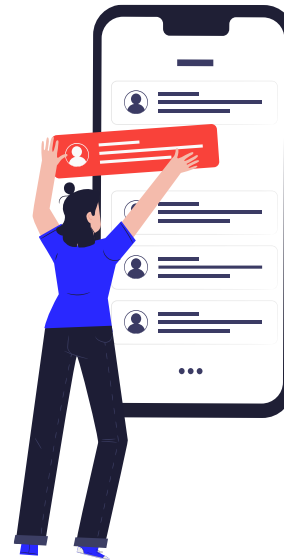


Перепроверяйте сообщения от друзей с просьбой срочно выслать денег.

Сначала перезвоните другу и удостоверьтесь, что просьба действительно направлена от него.



Проявляйте осторожность при переходе по ссылкам, полученным в сообщениях от других пользователей, если вы не знакомы с отправителем.



Воздерживайтесь от ответа на провокационные сообщения и комментарии других пользователей. Блокируйте навязчивых провокаторов.



При завершении работы в социальной сети выходите из своего аккаунта.



**Главный  
радиочастотный  
центр**

**Спасибо за внимание!**