

## **Основные правила работы в Интернете**

Каждый современный человек ежедневно проводит время в Интернете. Но Интернет – это не только источник информации и возможность общаться на расстоянии, но и угроза личной и компьютерной безопасности. Вы можете скачать из Сети компьютерный вирус, вашу учетную запись, адрес электронной почты или персональную информацию может взломать злоумышленник.

1. Используйте надежный пароль. Первое и главное правило сохранности ваших данных, учетных записей, почтовой пересылки – это надежный пароль! Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользовательставил простой пароль. Вы ведь не хотите, чтобы ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль.

2. Заходите в Интернет с компьютера, на котором установлен файервол или антивирус с файерволовом. Это в несколько раз уменьшит вероятность поймать вирус или зайти на вредоносный сайт.

3. Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в социальных сетях и прочих сервисах вы будете указывать его. Это необходимо, если вы забудете пароль или имя пользователя. Ни в коем случае не говорите никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан ваш почтовый адрес.

4. Если вы хотите скачать какой-то материал из Интернета, на сайте, где не нужна регистрация, но от вас требуют ввести адрес своей электронной почты, то, скорее всего, на ваш адрес будут высыпать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5. При предложении ввода личного номера телефона и просьбы подтверждения на четырехзначный номер, то вероятнее всего, после подтверждения, с вашего счета будет списана определенная сумма средств (достигает нескольких сотен рублей).

6. Скачивайте программы либо с официальных сайтов разработчиков, либо с крупных торрент трекеров. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так вы уменьшите риск скачать вирус вместо программы. Используйте лицензионное программное обеспечение.

7. Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они ни были. В лучшем случае вы поможете автору сайта получить деньги, а в худшем – получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.

8. Если вы работаете за компьютером, к которому имеют доступ другие люди (на работе или в Интернет-кафе), не сохраняйте пароли в браузере. В противном случае любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя ваш пароль.

9. Не открывайте письма от неизвестных вам пользователей (адресов) или письма с оповещением о выигрыше в лотерее, в которой вы просто не участвовали.

10. Не нажимайте на всплывающие окна, в которых написано, что ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если вас вдруг заблокируют, вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит вам электронное письмо.

11. Периодически меняйте пароли на самых важных сайтах. Так вы уменьшите риск взлома вашего пароля.

12. Личную персональную информацию размещайте только на официальных и проверенных сайтах (к персональной информации

относятся: имя, фамилия, возраст, номер мобильного телефона, адрес электронной почты, домашний адрес, фото, видео и т.д.).

13. Порядок размещения персональной информации иных лиц определяется законом от 27 июля 2006 года N 152-ФЗ «О персональных данных».

14. Запрещается посещать сайты, содержащие информацию, запрещенную к распространению в Российской Федерации, а также осуществлять действия, запрещенные законодательством Российской Федерации.

– Пользователям Интернета в стенах колледжа категорически запрещается:

посещать сайты, содержащие информацию, не совместимую с задачами образования;

– устанавливать какое-либо дополнительное программное обеспечение и/или вносить какие-либо изменения в программное обеспечение, установленное на компьютере;

– работать с объемными ресурсами (video, audio, chat, игры и др.) без согласования с сотрудниками отдела ИТ;

– изменять конфигурацию компьютеров, в том числе менять системные настройки компьютер.

**Совет:** Контролируйте свое время работы за компьютером, т.к. неограниченное использование компьютера может привести к физическим и психологическим расстройствам, а также нанести серьезный вред вашему здоровью.