**Безопасность**

**Рекомендации по правилам личной безопасности ⇒ http://nac.gov.ru/rekomendacii-po-pravilam-lichnoy-bezopasnosti.html**

**В новости:**

**В разделах: Родителям**

**Преподавателям**

**Обучающимся**

**Основные правила работы в сети Интернет**

Каждый современный человек, ежедневно проводит  время в интернете. Но интернет это не только источник информации и возможность общаться на расстояние, 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 пользователь ставил простой пароль. Вы ведь не хотите, что бы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей (например, http://www.infotecs.ru/ downloads/product\_full.php?id\_product=484), чтобы получить надежный пароль.

2) Заходите в интернет  с компьютера, на котором установлен файервол или антивирус с файерволом. Это в разы 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 соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, ни кому 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 высылать рекламу или спам.  В таких случаях пользуйтесь **одноразовыми почтовыми ящиками.**

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).

5) 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**.

6)Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем — получите вирус. **Используйте плагины для браузеров, которые отключают рекламу на сайтах.**

7) 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.

8) Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.

9) Не нажимайте на вплывающие 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.

10) Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля.

+

11) 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.).

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

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

13) Пользователям сети Интернет 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.