

Правила безопасности в интернете

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, чтобы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль.

Генератор паролей создается, чтобы помочь вам с придумыванием устойчивых к взлому и легко запоминающихся паролей.

Часто бывает: вы зарегистрировались где-нибудь, а там просят: «введите пароль». В спешке приходится вводить что-нибудь типа qwerty или 12345. Последствия могут быть фатальными для вашего аккаунта: при попытке взлома такие пароли проверяются в первую очередь. Чтобы этого не происходило, надо создавать сложный пароль, желательно состоящий из букв разного регистра и содержащий цифры и другие символы.

Для создания таких паролей существуют специальные программы. Но, на наш взгляд, гораздо легче набрать наш адрес и просто выбрать понравившийся пароль.

Советы:

- Выбирайте пароль посложнее, состоящий из символов разного регистра, с цифрами и для абсолютной надёжности - знаками препинания.
- Не используйте пароль, связанный с теми данными, которые могут быть о вас известны, например, ваше имя или дату рождения.
- Пароли, которые вы видите на экране создаются в реальном времени на вашем компьютере, поэтому исключена возможность перехвата пароля по сети. Разные посетители сайта видят разные пароли. Если вы зайдете на сайт второй раз, пароли будут другими.
- Вы можете выбрать пункт меню браузера "Файл|Сохранить как...", чтобы пользоваться генератором паролей в оффлайне.
- Генератор паролей полностью прозрачен: скачайте файл passwd.js, чтобы увидеть, как создается пароль, и убедиться в абсолютной надежности.

Источник- <http://genpas.narod.ru/>

2) Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. 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, 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 высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите

риск скачать вирус вместо программы. 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 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.

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

Пользуясь этими правилами безопасности в интернете, Вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте.

<http://www.youtube.com/watch?v=wVDsCpYSpeo>

<http://www.ligainternet.ru/encyclopedia-of-security/article.php?id=464>