

Правила безопасности в Интернете

Нурбек Тентиев

ntentiev@gmail.com

2017

Интернет содержит в себе только положительные аспекты, но и может быть угрозой компьютерной безопасности:

- можно скачать компьютерный вирус
- Вашу учетную запись или адрес электронной почты могут взломать
- Ваши персональные данные могут использоваться злоумышленниками
- можете потерять учетную запись на любимом сайте

1) Используйте надежный пароль

2) Заходить в Интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом (брандмауэр).

3) Пользуйтесь **одноразовыми почтовыми ящиками**, если Вы хотите скачать какой-то материал из Интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты (таким образом, обычно Ваш адрес попадает в списки рассылок, по которым потом вам будут регулярно высылать рекламу или спам).

4) Ни в коем случае не говорите никому свой пароль к Вашему основному (основным) адресу электронной почты, с которым Вы регистрировались на форумах, соц.сетях и прочих сервисах, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам.

5) Скачивайте программы с официальных сайтов производителя программного обеспечения. 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 ненадежных сайтах. В лучшем случае, Вы поможете автору сайта заработать небольшие деньги за клики, а в худшем — получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.
- 7) Если Вы работаете за общим компьютером, к которому имеют доступ другие люди (на работе или в Интернет-кафе), не сохраняйте пароли в браузере.
- 8) Не открывайте письма от неизвестных Вам пользователей (адресов).
- 9) Игнорируйте сообщения с предложением легкой выгоды (якобы выигрыш в лотерее, просьба о помощи получить наследство через Ваш банковский счет и т.п.)
- 10) Не нажимайте на различные всплывающие окна, появляющиеся при просмотре Интернета, в которых написано, что Ваша учетная запись в социальной сети заблокирована, Ваш компьютер заражен вирусом и предлагается через сайт вылечить компьютер и т.д. Это проделки злоумышленников! Доверяйте только сообщениям в самой социальной сети, или от администрации используемых Вами сайтов. Если требуется Ваше внимание к Вашей учетной записи на каком-либо, то администрация обязательно Вам отправит электронное письмо.
- 11) Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля.
- 12) Не записывайте пароли в местах (клочки бумаги, блокноты и т.п.), к которым есть свободный доступ у других людей. Лучший способ – хранить пароли в голове. Но если это не возможно, то хотя бы храните записи с пароли в укромном месте.
- 13) Устанавливайте на компьютере антивирусное программное обеспечение с последними обновлениями антивирусной базы
- 14) Регулярно обновляйте антивирусное ПО или разрешите автоматическое обновление
- 15) Регулярно обновляйте пользовательские программы, которые Вы часто пользуетесь, в особенности, браузеры, почтовые программы.
- 16) При использовании средств общения в Интернете (чаты, мессенджеры и т.д.) никогда не открывайте присланные файлы из ненадежных источников и от незнакомых людей, предварительно не проверив антивирусной программой.
- 17) Не переходите по ссылкам, присланным Вам по почте, если они вызывают у вас подозрения.

Некоторые антивирусные программы:

- ESET NOD32
- Kaspersky Internet Security
- Avast! Internet Security
- McAfee Internet Security
- Avira Premium Suite

10 способов защиты личных данных

Как не стать жертвой интернет-мошенников



Не указывайте лишнюю личную информацию в профиле в социальных сетях, используйте сокрытие данных от всех, кроме друзей



Своевременно обновляйте программное обеспечение



Установите на свой (свой) ПК защитное ПО (антивирус и фаервол) и следите за регулярностью обновлений антивирусных баз



Тщательно выбирайте онлайн-магазин, прежде чем сообщать данные банковской карты, пользуйтесь услугой SMS-информирования от банка



Обращайте внимание на характер данных при регистрации в онлайн-сервисах.

Не указывайте данные, которые в действительности не нужны для получения услуг от сервиса (номера удостоверений личности и т.п.), а в случае необходимости ищите менее требовательные к персональным данным сервисы-аналоги



Не запускайте подозрительные вложения, присланные по электронной почте и через интернет-мессенджеры



Установите пароль доступа к смартфону и специализированные приложения для поиска аппарата и удаленного стирания данных. Внимательнее относитесь к установке малоизвестных приложений. Отключайте неиспользуемые беспроводные интерфейсы



Установите свой собственный пароль домашней сети Wi-Fi



Проверяйте интернет-адреса при переходе из почты и с сайтов



Не используйте один пароль для всех интернет-ресурсов