**Как спастись от киберугроз**

Киберугроза – это распространение вредоносной информации и спама в Сети, которые ставят под угрозу персональную информационную безопасность человека, компании или даже государства. Самыми значимыми источниками вредоносной информации считаются вирусы, шпионское программное обеспечение и вредоносные программы.

Кроме распространения спама, который приводит к засорению информационных каналов, снижению скорости работы, увеличению трафика и оплаты, опасность представляют фишинговые атаки (создание сайта-двойника для получения конфедициальной информации и её незаконного использования), сбои в работе (потеря несохраненных данных, поломка оборудования) и DDoS-атаки (одновременная хакерская атака с большого числа компьютеров с целью доведения до отказа в работе).

**Рекомендации по личной безопасности в Интернете**

При работе с ресурсами сети Интернет, с устройствами и программами необходимо соблюдать следующие правила:

В первую очередь, сохранять критическое мышление и недоверие ко всей поступающей без вашего запроса информации. Все, что попало в Интернет, там и осталось !

Во вторых, использовать средства защиты компьютера:

* персональный межсетевой экран;
* разные учетные записи для работы и администрирования (установки программ);
* антивирусная программа;
* на телефоне – включить настройки ограничений;
* специальные настройки социальных сетей.

**Эти рекомендации можно дополнить следующими принципами:**

1. Никогда ни с чем не соглашаться! Даже доверенные сайты могут быть скомпрометированы и на них мог попасть вредоносный код. Если на странице появилось предложение, которое непонятно, откажитесь от него или закройте.

2. Разные сервисы – разные идентификаторы. В качестве идентификатора могут использоваться либо дубликат номера, либо одноразовая почта. В случае с дубликатом номера, к основному номеру «привязывается» еще один, виртуальный номер, который можно сменить. Для доступа к какому-либо сервису или регистрации на сайте можно воспользоваться одноразовой почтой.

Как понять, насколько хорошо работает компьютер? Может быть, он уже скомпрометирован? Признаками заражения могут быть:

* «торможение» системы, оптимизировать загрузку программ в ОС помогут программы Cleanmymac, CleanmyPC, Ccleaner, Msconfig, Sysinternals;
* лишний трафик;
* непонятные выскакивающие окна и запущенные программы.

3. Использовать для мобильного телефона более сильные механизмы защиты:

* не использовать четырехзначный пароль;
* использовать биометрическую защиту или сложный пароль, чтобы узнать, достаточно ли сложный пароль, рекомендуется пользоваться специальными сервисами. Сервисы проверки паролей:
* LastPass Password Generator
* Kaspersky Secure Password Check

При этом не рекомендуется использовать платные сервисы для проверки паролей и учетных записей на предмет компрометации. Дополнительные рекомендации цифровой гигиены и личной безопасности в пространстве Интернет;

* блокировать телефон и компьютер, когда отходите;
* не использовать стикеры с паролями;
* не «царапать» пин-код на банковской карте.

4. Дополнительные меры цифровой гигиены в Интернете:

* убедитесь, что блоки идентификации и авторизации разделены;
* не отправляйте фотографии и голосовые сообщения неизвестным людям;
* не используйте доступную информацию о себе в качестве восстановления паролей;
* корректно очищайте и сбрасывайте информацию с устройств при продаже или передаче.

5. Не доверяйте передаваемым файлам, проверяйте файлы на специальных сервисах:

* Virustotal
* Kaspersky Virusdesk

6. Не доверяйте присылаемым URL:

* обращайте внимание на сокращения URL;
* проверяйте URL с помощью специальных сервисов.

7. Не поддавайтесь фишингу и мошенникам:

* не вводите логины и пароли на неизвестных сайтах;
* убедитесь в подлинности сайта:
* проверьте URL;
* убедитесь в доверенном сертификате.

8. Следите за тем, с кем общаетесь в социальных сетях и в мессенджере. Как можно распознать злоумышленника?

* Задать личный вопрос.
* Отвечать односложно – у бота «нет контекста».
* Также злоумышленники очень быстро отвечают, либо повторяют сказанные слова.

**Экспертное мнение подготовили ведущие рубрики «Права и обязанности: общий взгляд»**

кандидат технических наук, заведующий кафедройинформационных систем и математического моделирования **О.А. Астафурова**

кандидат технических наук, доцент кафедры информационных систем и математического моделирования **Н.А. Сальникова**