Советы по безопасности в сети интернет.

Используйте новейшую версию антивирусной программы

Многие комплексные антивирусы предлагают эффективную защиту от троянов, вирусов и других вредоносных приложений. Сочетание антивирусной защиты, фаервола, спам-фильтра и других инструментов позволит защитить компьютеры, смартфоны и планшеты от дополнительных угроз из Интернета, например, от хакерских атак.

https://www.comss.ru/page.php?id=6861 – ссылка на обзор лучших антивирусов 2020 года по мнению пользователей

Своевременно устанавливайте обновления

Онлайн атаки обычно нацелены на бреши в безопасности операционной системы, браузеров и популярных приложений. С помощью обновлений разработчики постоянно устраняют уязвимости в своих продуктах. Именно поэтому важно регулярно обновлять программы, в том числе и антивирусы. Защитные продукты постоянно получают информацию об обнаружениях вредоносных программ в Интернете. Обновления для Android, MacOS и Windows должны выполняться регулярно и своевременно.

Используйте безопасные пароли

При выборе паролей, пользователи должны проявить свои творческие способности и должны создавать различные пароли для каждого аккаунта! Надежные пароль должен состоять минимум из 8 символов. Наиболее безопасная комбинация включает заглавные и строчные буквы, цифры и специальные символы. Легко запомнить пароли, состоящие из строки песни с добавлением года выхода композиции. Бесплатные менеджеры паролей также очень полезны при управлении большой коллекцией паролей.

https://www.comss.ru/list.php?c=passwords – бесплатные менеджеры паролей

Зашифрованные подключения для безопасной передачи данных

По возможности используйте зашифрованные подключения каждый раз при посещении интернет-магазинов, интернет-банкинга или почтового сервиса. Адрес зашифрованных подключений начинается с "https" вместо "http". Кроме того, браузеры показывают иконку замка при безопасных подключениях.

Соблюдайте меры предосторожности при использовании общественных сетей Wi-Fi

Общественные сети Wi-Fi являются очень практичными, когда требуется зайти на сайт на короткое время или определить текущее местоположение с помощью смартфона. Тем не менее, они не подходят для интернет-банкинга или передачи конфиденциальной информации. Пользователь не может знать, кто администрирует сеть и какие меры защиты предпринимаются. Именно поэтому рекомендуется совершать финансовые

транзакции в защищенной домашней сети и по возможности избегать доступа к важным аккаунтам, если устройство подключено к публичной точке доступа.

Осторожно обращайтесь с личными данными

Личная информация, которая предоставляется веб-сайтам и приложениям часто раскрывается и даже продается третьим лицам. Именно поэтому пользователи должны указывать как можно меньше личных данных, заполняя только требуемые поля. Обычно политика обработки данных указывается в общих условиях использования или в правилах соблюдения конфиденциальности онлайн сервисов, программ и приложений.

Остерегайтесь бесплатного

При использовании бесплатных приложений и веб-сервисов пользователь должен всегда задавать себе вопрос, какую пользу указанная им информация может принести разработчикам. Очень часто пользователи “платят” за использование бесплатных приложений и сервисов своими личными данными, которые монетизируются поставщиками услуг. Например, пользователь может получать нежелательную рекламу на указанные номера телефонов и адреса электронной почты.

Используйте надежные источники

Файлы, программы и приложения должны открываться или устанавливаться только если они загружены из достоверных источников. Новейшие версии браузеров и антивирусов предупреждают пользователя о посещении потенциально опасных ресурсов. Приложения лучше устанавливать из официальных магазинов приложений Google Play, App Store или из Магазина приложений Windows

Регулярно создавайте резервные копии

Всегда существует риск потери данных, даже если устройство не потеряно, не украдено или не уничтожено. В случае с троянами-вымогателями, резервные копии могут снизить риск вымогательства со стороны злоумышленников. Нужно регулярно создавать резервные копии важных данных на внешние диски с помощью специализированных программ. Некоторые программы для резервного копирования распространяются бесплатно.

https://www.comss.ru/list.php?c=backup – список программ для резервного копирования

Советы по безопасности в сети интернет для родителей

Родителям необходимо помнить о том, как сделать интернет безопасным и обучающим инструментом для ребенка, чтобы защитить его от негатива и разнообразных рисков. Только отрицаниями и запретами нельзя бороться с компьютерной зависимостью и неприятностями, поджидающими детей в интернете. Необходимо помнить, что Сеть не только несет большие риски, но

и содержит множество полезной информации и знаний. Именно поэтому об определенных фильтрах должен знать каждый родитель. Они позволят обезопасить детей в Сети.

1. Соблюдайте время нахождения ребенка в сети интернет.
2. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
3. Используйте специальные детские поисковые машины, типа MSN Kids Search.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.
6. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
7. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
8. Научите детей не загружать файлы, программы или музыку без вашего согласия.
9. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
10. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
11. Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
12. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Руководитель отдела информационно-технического обеспечения
Валеев А. Р.