Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Безопасный старт
- Безопасное использование компьютера
- Восстановление данных

Семь простых шагов для защиты компьютера

ОБ АВТОРЕ

Гай Бруно – автор этого выпуска. Гай является обладателем сертификации GIAC Security Expert (GSE). Он успешно окончил курс SANS Cyber Guardian (Blue Team). Гай работает инструктором Института SANS и входит в состав команды SANS Incident Storm Center. Больше информации о его деятельности можно найти в Твиттере @guybruneau.

ОБЗОР

Портативные устройства, например, смартфоны и планшеты, открывают нам новые технологические возможности. В то же время, компьютеры являются незаменимым инструментом в нашей профессиональной деятельности и личной жизни.
Поэтому, компьютер - дома или на рабочем месте - является главной мишенью для кибер преступников. Сегодня мы поговорим о семи простых шагах, которые помогут защитить ваш компьютер от большинства известных атак.

1. БЕЗОПАСНЫЙ СТАРТ

Первый шаг к безопасности начинается с самого компьютера. Если вы приобрели компьютер непосредственно у известных производителей, то и программному обеспечению можно доверять. Но если вы приобрели бывший в употреблении компьютер, то не стоит доверять ему. Компьютер может быть заражён, намеренно или случайно, вирусами. Обеспечить безопасность уже инфицированного компьютера невозможно. При покупке бывшего в употреблении компьютера, в первую очередь необходимо отформатировать жёсткий диск и переустановить операционную систему (самостоятельно или с помощью своих знакомых, которым доверяете).

2. ОБНОВЛЕНИЯ

Следующий шаг – это обновления. Кибер преступники всегда находят новые слабые места компьютеров и приложений. Когда производителям компьютеров и программного обеспечения становится известно об этих новых уязвимостях, они разрабатывают и выпускают обновления для решения проблемы. Когда вы покупаете компьютер или переустанавливаете операционную систему, скорее всего, она уже устарела. Таким образом, первый шаг, который нужно предпринять, это

Семь простых шагов для защиты компьютера

подключиться к Интернету и обновить операционную систему. Убедитесь, что при подключении к сети используете фаервол или домашнюю точку доступа Wi-Fi. Кроме того, большинство операционных систем, например, Windows и OS X, в том числе и многие приложения имеют встроенную функцию автоматического обновления. Настройка автоматической проверки обновлений хотя бы раз в день обеспечит безопасность вашему компьютеру. Если производитель выпускает обновление, которое нужно установить вручную, обязательно установите его.

3. БЕЗОПАСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

После обновления операционной системы, убедитесь, что у вас установлены и используются программы безопасности. Два самых распространённых вида таких программ: антивирусы и фаерволы. Антивирусы помогают идентифицировать заражённые файлы, которые вы скачали и защищают ваш компьютер от них. Фаерволы работают как виртуальный полицейский: определяют, кто может, а кто нет соединиться с вашим компьютером. Многие производители программ безопасности предлагают пакет, включающий антивирус, фаервол и другие варианты программного обеспечения. Вы можете приобрести целый пакет программ безопасности.

4. БЕЗОПАСНОСТЬ УЧЁТНЫХ ЗАПИСЕЙ

Каждый, у кого есть доступ к компьютеру, должен иметь отдельную учётную запись, защищённую уникальным и

Следуя этим простым шагам, вы обезопасите свой компьютер

сильным паролем. Никогда не делитесь учётной записью. Если это домашний компьютер, создайте учётную запись для каждого члена семьи, особенно для детей. Это позволит вам контролировать каждого пользователя, например, детей, и отслеживать, кто что делает. Кроме того, предоставьте каждому пользователю минимум привилегий. Не обеспечивайте никого, включая себя, правами администратора. Права администратора необходимо использовать только для установки или изменения конфигураций программного обеспечения.

5. МОБИЛЬНАЯ БЕЗОПАСНОСТЬ

Если у вас портативный компьютер, например, ноутбук, рассмотрите возможность полного шифрования диска (FDE). Шифрование гарантирует защиту вашей информации, даже в случае утери ноутбука. Вы также можете ставить блокировку экрана с парольной защитой, чтобы никто не мог получить доступ к системе

Семь простых шагов для защиты компьютера

в ваше отсутствие. Некоторые ноутбуки поддерживают функцию удаленного обнаружения и/или удаления информации: это может помочь найти ноутбук и/или удалить с него всю конфиденциальную информацию.

6. БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРА

Никакие технологии не способны защитить от всех угроз. Все, о чем мы говорили, поможет защитить ваш компьютер. Последний элемент, о защите которого стоит подумать, это вы – пользователь. Помните, что плохие парни всегда будут пытаться обмануть вас. Если вы получили сообщение, которое кажется странным или подозрительным, не открывайте вложения и не переходите по ссылке. Если кто-то звонит и говорит, что компьютер заражён и вам следует установить программное обеспечение, скорее всего, это мошенничество. Во многих ситуациях вы - лучшая защита для компьютера, а не технологии.

7. РЕЗЕРВНЫЕ КОПИИ

Наконец, даже если следовать всем рекомендациям, о которых мы говорили, всегда есть риск, что ваш компьютер взломают, случится сбой жёсткого диска или произойдёт другая неприятность. Ваша последняя защита – резервные копии. Мы рекомендуем регулярно делать резервные копии важной информации (документов, фото, видео и пр.) на внешний жёсткий диск или храните с помощью облачных технологий, в некоторых случаях используйте оба способа.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

Бесплатная проверка безопасности:
http://preview.tinyurl.com/bxph6a8

Центр Информационной безопасности Microsoft:
http://www.microsoft.com/ru-ru/security/

Безопасность Mac OS X:
http://preview.tinyurl.com/abl6xm7

Термины по Информационной безопасности:
http://preview.tinyurl.com/6wkpae5

Институт SANS - Ежедневные советы по Информационной безопасности:
http://preview.tinyurl.com/6s2wrkp

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт: http://www.securingthehuman.org.

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков