Полезные привычки кибергигиены

> Хорошая гигиена — это то, чему тебя учат в детстве, и то, что обычно остается с тобой до конца жизни.

Вы слышали о кибергигиене? Конечно, чистка зубов и принятие душа — это не то, что традиционно ассоциируется с технологиями, но этот термин является полезной метафорой для необходимости принимать умные решения при использовании ваших интеллектуальных устройств.

Хорошая гигиена — это то, чему тебя учат в детстве, и то, что обычно остается с тобой до конца жизни. Она включает в себя три основных принципа: использование продуктов и инструментов, которые соответствуют вашим гигиеническим потребностям, правильное выполнение этих гигиенических задач и составление рутины.

Но что такое кибергигиена и какое отношение это имеет к вашему компьютеру и подключенным устройствам?

Cyber Hygiene — это обучение себя проактивному восприятию вашей кибербезопасности — как и вашей повседневной личной гигиене — противостоять киберугрозам и проблемам безопасности в сети. К сожалению, кибербезопасность все еще не воспринимается так серьезно, как чистка полости рта и мытье рук перед едой. Некоторые люди принимают кибербезопасность как нечто сугубо технологическое, но это может измениться, поскольку киберугрозы продолжают развиваться. Между тем, установление строгих правил кибергигиены должно быть таким же обычным делом, как чистка зубов.

Вот несколько советов, которые помогут вам и вашей семье задуматься о правильных правилах кибер-гигиены.

Используйте правильные инструменты для кибергигиены

Вы когда-нибудь пытались чистить зубы без зубной щетки? Без правильных инструментов для работы поддержание личной гигиены было бы немного сложнее, если не невозможно. То же самое верно для управления хорошей компьютерной гигиеной. Без правильных продуктов и инструментов личная информация, которую вы считаете безопасной, фактически может оказаться под угрозой.

Авторитетное антивирусное ПО, сетевой брандмауэр и защита паролем помогают защитить личные данные, хранящиеся на вашем домашнем компьютере. Взятые вместе, эти инструменты могут помочь вам чувствовать

себя уверенно по поводу безопасности вашего домашнего компьютера, ноутбука, смартфона и других устройств.

Кроме того, перед установкой чего-либо на свой компьютер или другие устройства вы всегда должны убедиться, что производитель данного ПО и место, откуда вы его взяли — является надежным источником.

Будьте внимательны, будьте аккуратны с кибергигиеной

Каждый должен пользоваться зубной нитью, верно? Но все ли делают это так, как рекомендует стоматолог? Удаленные, по-видимому, безвозвратно файлы на вашем компьютере время от времени требуют особого внимания.

Например, вы можете подумать, что регулярная очистка мусорной корзины удаляет личные или конфиденциальные данные с жесткого диска. Это не так.

Чтобы окончательно удалить файлы с вашего компьютера, вы должны использовать программное обеспечение для очистки данных. Всякий раз, когда вы вводите новое программное обеспечение, добавляете оборудование или модифицируете системные файлы, вы рискуете потерять данные. Привыкайте регулярно удалять ненужные данные и вытирать их с жесткого диска с помощью невосстановимого стирания.

Еще одна область безопасности, требующая вашего внимания, — это защита паролем. Не ленитесь и не экономьте на создании сложных уникальных паролей для каждой учетной записи, используя комбинации из 12 букв, цифр и специальных символов. Регулярно меняйте пароли к своим учетным записям, и вы сразу же добьетесь лучшей кибергигиены. Если вы не в состоянии запомнить все ваши пароли, используйте специальное программное обеспечение – так называемые менеджеры паролей.

Сделать кибергигиену частью вашей рутины

Обучение регулярному мониторингу вашей кибербезопасности может повысить ваши шансы избежать онлайн-угроз. Но, как и любая привычка, которую вы хотите сделать привычкой, она требует рутины и повторения.

Начните с установки будильника или пометки календаря с датами для решения ряда задач, таких как сканирование на наличие вирусов с помощью антивирусного программного обеспечения, обновления операционных систем на всех ваших устройствах, проверки обновлений безопасности, очистки жесткого диска и изменения ваших паролей. Как только вы начнете овладевать кибергигиеной, она станет для вас второй натурой.

Ключевые шаги для хорошей компьютерной гигиены

Хорошая кибергигиена — это общая практика, которая может помочь вам обеспечить безопасность в сети, но есть несколько рекомендаций, которые помогут вам обеспечить максимальную безопасность вашей кибергигиены. Вот девять основных шагов.

Шаг 1. Установите авторитетное антивирусное и вредоносное программное обеспечение.

Первый и, возможно, самый важный шаг — установка антивирусного программного обеспечения. Для чего? Антивирусное программное обеспечение — это программа или комплекс программ, которые сканируют и уничтожают компьютерные вирусы и другие вредоносные программы. Это жизненно важный компонент вашей общей кибергигиены в защите от нарушений безопасности, а также других угроз.

В частности, антивирусное программное обеспечение обеспечивает защиту, выполняя ключевые задачи, в том числе следующие.

Определение конкретных файлов для обнаружения вредоносного программного обеспечения.

Планирование и выполнение автоматического сканирования.

Сканирование либо одного конкретного файла, либо всего вашего компьютера, либо флэш-накопителя, в зависимости от ваших конкретных потребностей.

Удаление вредоносного программного обеспечения.

Подтверждение «здоровья» вашего компьютера и других устройств.

Шаг 2: Используйте сетевые брандмауэры

Использование сетевого брандмауэра является еще одной ключевой привычкой для поддержания хорошей компьютерной гигиены. Межсетевые экраны являются первой линией защиты в сетевой безопасности, предотвращая несанкционированный доступ пользователей к вашим веб-сайтам, почтовым серверам и другим источникам информации, доступ к которым можно получить из Интернета.

Шаг 3: регулярно обновляйте программное обеспечение

Регулярно обновляйте свои приложения, веб-браузеры и операционные системы, чтобы убедиться, что вы работаете с последними программами, в которых устранены или исправлены возможные сбои. Настройка этой функции на автоматическое обновление поможет обеспечить вам самые последние средства защиты.

Эти обновления особенно важны, потому что они часто включают исправления программного обеспечения. Разработчики программного обеспечения выпускают исправления безопасности всякий раз, когда обнаруживают недостатки программного обеспечения — недостатки, которые могут использовать вирусы или хакеры. Разработчики не всегда могут предупредить вас, когда был внедрен критический патч. Таким образом, регулярные обновления гарантируют, что эти патчи закроют все известные на момент их выпуска дыры в вашем программном обеспечении.

Шаг 4: Установите надежные пароли

Установка надежных паролей для всех ваших устройств имеет важное значение. Ваши пароли должны быть уникальными и сложными, содержать не менее 12 символов, а также цифры, символы, заглавные и строчные буквы. Регулярная смена ваших паролей необходима для того чтобы уменьшить вероятность их взлома злоумышленниками. Помните! Каждый пароль должен быть уникальным.

Дополнительные элементы управления устройства — пароли прошивки. В то время как шифрование диска препятствует доступу кибер-воров к информации, хранящейся на вашем устройстве, пароли встроенного ПО защищают ваше оборудование, предотвращая перезагрузку или сброс вашей машины без вашего пароля.

Шаг 5: Используйте многофакторную аутентификацию

Двухфакторная или многофакторная аутентификация — это лучшая практика, которая предлагает дополнительный уровень защиты. Для двухфакторной аутентификации обычно требуется, чтобы вы указали свой пароль и имя пользователя, а также, скажем, уникальный код, отправленный на ваш мобильный телефон. Это может быть все, что необходимо для некоторых систем, но многофакторная аутентификация добавляет дополнительные уровни безопасности с использованием биометрических данных, таких как распознавание лиц или отпечатков пальцев, чтобы хакерам было труднее получить доступ к вашему устройству и личной информации.

Шаг 6: Использовать шифрование устройства

Хотя в большинстве компаний автоматически применяются процессы шифрования данных, вам также может понадобиться шифровать ваши устройства и другие носители, содержащие конфиденциальные данные, включая ноутбуки, планшеты, смартфоны, съемные диски, ленты для резервного копирования и облачное хранилище. Фактически, многие устройства используют шифрование по умолчанию для данных, хранящихся на смартфонах. Некоторые приложения используют сквозное шифрование, а

другие службы шифруют данные на ваших устройствах и сохраняют их в облаке. Другой вариант — использовать зашифрованную карту памяти USB для защиты конфиденциальных данных.

Шаг 7: регулярно делайте резервные копии

Также разумно защищать ваши файлы, создавая резервные копии важных файлов в автономном режиме, на внешнем жестком диске или в облаке. Это может помочь защитить от потери данных, особенно если хакеры получают доступ к одному из ваших устройств.

Шаг 8: Держите жесткий диск в чистоте

Если вы продаете свой ноутбук, планшет или смартфон, важно, чтобы ваша личная или конфиденциальная информация при этом не передавалась. Если ваше устройство взломано, чистый жесткий диск означает меньше информации, к которой осуществляется доступ.

Но простого удаления файлов или данных может быть недостаточно. Частью хорошей кибергигиены является переформатирование, а затем чистка жесткого диска. Например, если вы хотите продать свой компьютер и использовать его для онлайн-банкинга, вам следует рассмотреть возможность очистки диска для удаления программного обеспечения и данных с жесткого диска.

Шаг 9: Защитите свой маршрутизатор

Не забудьте защитить свою беспроводную сеть. Это включает в себя отключение и обновление имени по умолчанию и пароля, с которым маршрутизатор пришел от производителя, отключение удаленного управления и выход из системы в качестве администратора после его настройки. Кроме того, убедитесь, что ваш маршрутизатор предлагает шифрование WPA2 или WPA3, чтобы поддерживать наивысший уровень конфиденциальности информации, передаваемой через вашу сеть.

Помните, что практиковать хорошие кибергигиенические привычки — это разумно. Если вы настроите на своем компьютере и других устройствах авторитетные антивирусные программы, будете регулярно обновлять их, создавать надежные пароли и содержать все в чистоте, вы будете на пути к созданию кибернетических привычек, которые могут помочь вам обезопасить себя в сети.

Источник: https://www.securitylab.ru/contest/499710.php