OUCH! Февраль 2023

SANS SECURITY AWARENESS

Ежемесячный информационный бюллетень по безопасности

Нужно ли мне программное обеспечение для безопасности?

Обзор

Когда вы покупали новый компьютер много лет назад, вам часто приходилось устанавливать на него дополнительное программное обеспечение безопасности, чтобы защититься от кибератак. Однако в большинство современных компьютеров и устройств уже встроены многочисленные функции безопасности, такие как автоматическое обновление, брандмауэры, шифрование диска и защита файлов. Кроме того, Microsoft предоставляет на компьютерах с Windows функцию безопасности под названием Microsoft Defender, которая включает в себя дополнительные функции, такие как антивирус. Во многих отношениях современные системы по умолчанию гораздо более безопасны. На самом деле ВЫ, скорее всего, сейчас самая большая слабость. Вот почему кибер-злоумышленники постоянно нацеливаются на людей, пытаясь заставить вас делать то, что вы не должны делать, например сообщать свои пароли, переходить по ссылкам или открывать вложения электронной почты, которые устанавливают вредоносное ПО на ваши компьютеры или предоставляют информацию о вашей кредитной карте.

Что следует учитывать?

Если вы хотите предпринять дополнительные шаги для защиты своих систем, вы можете рассмотреть несколько дополнительных программ безопасности.

Менеджеры паролей: Пароли могут быть сложными и длинными, особенно если необходимо помнить сотни разных паролей. Менеджер паролей — это безопасное хранилище, которое защищает и хранит все ваши пароли, поэтому вам нужно помнить только один мастер-пароль. Кроме того, они могут регистрировать вас на веб-сайтах, генерировать для вас пароли и помогать проверять определенные веб-сайты.

Виртуальные частные сети (VPN): Виртуальные частные сети в первую очередь сосредоточены на защите вашей конфиденциальности, шифруя ваше подключение к Интернету и скрывая ваше исходное местоположение.

Комплекты безопасности: это пакеты программного обеспечения для обеспечения безопасности, которые предоставляют набор дополнительных функций безопасности сверх того, что уже предоставляет ваша операционная система. Например, фильтрация опасных веб-сайтов, родительский контроль и часто VPN. Каждый комплект имеет разные функции, поэтому изучите тот, который, по вашему мнению, лучше всего подходит.

Выбор поставщика систем безопасности

Если вам необходимо приобрести дополнительные средства безопасности или программное обеспечение, есть много разных поставщиков, из которых можно выбирать. Какой из них выбрать? Довольно часто разные поставщики похожи по предлагаемым ими функциям. Главное — использовать решение от надежного поставщика. Вы же не хотите случайно купить и установить что-то, распространяемое киберпреступниками и зараженное вредоносным ПО.

Используйте только известных поставщиков, о которых вы слышали и которым доверяете. Никогда не покупайте у компании, о которой вы ничего не знаете, которая является совершенно новой, не имеет комментариев или имеет много негативных отзывов. Вы хотите быть уверены, что решение, которое вы покупаете, является законным и активно обновляется и поддерживается. Возможно, вы даже захотите узнать, в какой стране находится поставщик. Существует множество онлайн-сайтов, на которых есть обзоры надежных поставщиков, демонстрирующие различия в функциях и стоимости их программного обеспечения для безопасности.

Будьте осторожны с бесплатными средствами безопасности. Хотя бесплатные средства безопасности существуют, сними могут быть некоторые проблемы. Эти средства могут иметь ограниченные возможности, быть сложными в использовании или обновляться нечасто. В некоторых случаях злоумышленники могут разрабатывать бесплатные программы, а затем их заражать вредоносными ПО.

Помните, что хотя эти инструменты безопасности полезны, начните сначала со встроенных функций безопасности вашего компьютера, включая включение автоматического обновления. Современные операционные системы очень безопасны по умолчанию. Вы, безусловно, лучшая защита. Будьте осторожны с любыми странными или подозрительными телефонными звонками, электронными или текстовыми сообщениями. Никакое программное обеспечение для обеспечения безопасности в мире не может защитить вас от того, кто пытается обмануть или заставить вас сделать то, что вы не должны делать.

Приглашенный редактор

Нико «Dutch_OsintGuy» Декенс — сертифицированный инструктор SANS и бывший аналитик правительственной разведки, специализирующийся на разведке с открытым исходным кодом (OSINT).
Подробнее о Нико здесь:https://www.sans.org/profiles/nico-dekens/
и тут https://www.dutchosintguy.com.

Ресурсы

Менеджеры паролей: https://www.sans.org/newsletters/ouch/password-managers/
Сила обновления: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Виртуальные частные сети: https://www.privacyguides.org/vpn/
Социальная инженерия: https://www.youtube.com/watch?v=lc7scxvKQOo
Обзоры пакета безопасности: https://www.pcmag.com/picks/the-best-security-suites

Роман Полаков