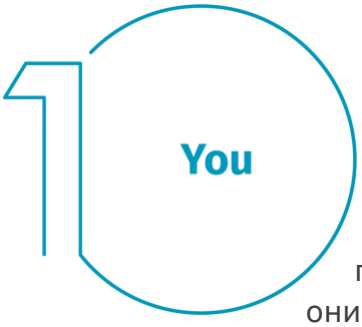
SANS SECURITY AWARENESS

5 главных правил для безопасной работы из дома

Мы знаем, что работа на дому может стать для некоторых чем-то новым и, возможно, обременительным, так как придется приспосабливаться к новой обстановке. Одна из наших целей — сделать работу дома максимально безопасной. Ниже приведены пять простых мер для безопасной работы. Помните: наши рекомендации помогут не только в работе, но и в личной жизни как вам, так и вашим близким, позволяя создать дом с высоким уровнем кибербезопасности.



Вы. Главное правило: технологии сами по себе не могут полностью защитить вас. Лучшая защита — вы сами. Взломщики понимают, что самый простой способ получить нужное — это сделать целью вас, а не ваш компьютер или другие устройства. Если им нужен ваш пароль, рабочие данные или контроль над компьютером, они попытаются обманом заставить вас передать им информацию, зачастую создавая ощущение срочности. Так, преступник может позвонить вам, притворившись специалистом технической поддержки Microsoft, и заявить, что ваш компьютер заражен. Вам также могут отправить предупреждение по электронной почте о невозможности отправки данных. Это обман, чтобы вы щелкнули по вредоносной ссылке. Вот самые частые признаки атаки с применением социального инжиниринга:

- Кто-то нагнетает ощущение срочности с помощью страха, запугивания, критической ситуации, упоминания важного конечного срока. Кибервзломщики умеют убедительно имитировать сообщения от доверенных организаций, таких как банки, правительственные органы и международные организации.
- Давление, принуждающее обойти или проигнорировать политику или процедуры безопасности, либо предложение, которое слишком хорошо, чтобы быть правдой (нет, вы не выиграли в лотерею!).

- Сообщение вроде бы пришло от друга или коллеги, но подпись, тон или подбор слов совсем на него не похож.

В итоге главная защита от подобных атак — это вы.

Домашняя сеть: почти каждая домашняя сеть начинается с беспроводной сети (часто именуемой Wi-Fi). Она позволяет подключать все ваши устройства к Интернету. Большинство домашних беспроводных сетей управляются маршрутизатором или отдельной выделенной точкой беспроводного доступа. В обоих случаях принцип работы одинаков: передача беспроводных сигналов, к которым подключаются домашние устройства. Это означает, что защита беспроводной сети — это ключевая часть защиты вашего дома. Для обеспечения безопасности мы рекомендуем следующие действия:

- Измените установленный по умолчанию пароль администратора устройства, управляющего беспроводной сетью. Учетная запись администратора позволяет настраивать параметры беспроводной сети.
- Убедитесь, что только люди, которым вы доверяете, могут подключиться к вашей беспроводной сети. Для этого обеспечьте высокий уровень безопасности. При включении этого параметра для подключения к беспроводной сети пользователям потребуется пароль, а после подключения их действия в сети будут шифроваться.
- Убедитесь, что пароль, используемый пользователями для подключения к беспроводной сети, надежен и отличается от пароля администратора. Помните, что вам нужно ввести пароль только один раз для каждого из ваших устройств, так как они хранят и запоминают пароль.

Не знаете, как выполнить эти действия? Спросите своего интернет-провайдера, ознакомьтесь с его сайтом, загляните в документацию, прилагаемую к точке беспроводного доступа, или перейдите на сайт поставщика.

Пароли: когда сайт предлагает вам создать пароль, создайте надежный пароль. Чем больше в нем символов, тем он надежнее. Один из простейших способов обеспечения надежного пароля — это использование кодовой фразы. Кодовая фраза — это не более чем пароль, состоящий из нескольких слов, таких как «*медовый пчелиный бурбон*». Использование уникальной кодовой фразы означает, что для каждого устройства или сетевой учетной записи используется своя фраза. Если одна кодовая фраза станет кому-то известной, все остальные ваши учетные записи и устройства останутся в безопасности. Не можете запомнить все пароли?

Используйте менеджер паролей — специальную программу, которая надежно хранит все ваши кодовые фразы в зашифрованном формате (и имеет множество других замечательных функций!). Наконец, по возможности включите двухшаговую проверку (также именуемую двух- или многофакторной аутентификацией). Помимо пароля в этом случае добавляется второй шаг, например код, отправляемый на ваш смартфон, или приложение, которое генерирует код для вас. Двухшаговая проверка — это, вероятно, самая важная мера, которую вы можете принять для защиты своих сетевых учетных записей, и это гораздо проще, чем вы думаете.

Обновления. На каждом компьютере, мобильном устройстве, в программе и приложении должна быть установлена последняя версия программного обеспечения. Кибервзломщики постоянно ищут новые уязвимости в программном обеспечении, используемом вашими устройствами. Когда они обнаруживают уязвимости, они применяют специальные программы для их эксплуатации и взлома устройств, используемых вами. Тем временем компании, создавшие программное обеспечение для этих устройств, усердно работают над устранением уязвимостей, выпуская обновления. Обеспечив быструю установку обновлений на свои компьютеры и мобильные устройства, вы значительно усложните процесс взлома. Чтобы ничего не упустить, достаточно включать автоматическое обновление, когда это возможно. Это правило применяется практически к любой технике, подключенной к сети, включая не только ваши рабочие устройства, но и подключенные к Интернету телевизоры, радионяни, камеры безопасности, домашние маршрутизаторы, игровые приставки или даже ваш автомобиль.

Дети и гости. То, о чем вам, скорее всего, не приходилось беспокоиться в офисе, — это дети, гости или другие члены семьи, пользующиеся вашим рабочим ноутбуком или другими рабочими устройствами. Убедитесь, что члены семьи и друзья понимают, что нельзя пользоваться вашими рабочими устройствами, так как они могут случайно стереть или изменить информацию или, что еще хуже, случайно заразить устройство.