Цифровые стены домашнего офиса

Владимир Безмалый

Несмотря на то, что всем нам все чаще и чаще приходится работать из дома, пользователи, на мой взгляд, пока еще не уделяют должного внимания вопросам информационной безопасности при работе из дома.

Причина достаточно банальна. Люди не привыкли относиться к своему домашнему ПК как к инструменту, за безопасностью которого нужно наблюдать и которую нужно строить! И все же, что делать если вам приходится работать дома или в дороге?

Избегайте общедоступного Wi-Fi; при необходимости используйте личные точки доступа или какой-либо способ шифрования вашего веб-соединения

Общедоступный Wi-Fi представляет значительный риск для безопасности, и его следует по возможности избегать.Если вам нужен доступ в Интернет используя общедоступный Wi-Fi, вам нужно решить две важные проблемы.

Во-первых, другие люди имеют доступ к этой сети, и без брандмауэра между вами и ними злоумышленники могут атаковать ваш компьютер.Во-вторых, любые заинтересованные наблюдатели в текущей сети или любых других общедоступных сетях, в которые ваши данные попадают между вами и вашим рабочим местом, могут отслеживать ваш трафик по мере его прохождения.
Важно найти способ защитить свой компьютер и зашифровать свой трафик.

Один из хороших вариантов — использовать личную точку доступа с выделенного устройства или вашего телефона.Хотя ваш веб-трафик между точкой доступа и местом назначения не будет зашифрован, использование точки доступа устраняет проблему взлома людьми того же общедоступного Wi-Fi.У большинства основных операторов связи вы можете заплатить номинальную плату за возможность настроить частную сеть Wi-Fi с помощью своего мобильного телефона.Конечно, это будет учитываться в ваших данных, но стоимость минимальна по сравнению с потенциальным недостатком серьезного взлома систем или компьютера вашей компании.Если ваша компания предоставляет услуги сотовой связи, нет причин не использовать, чтобы избежать общедоступного Wi-Fi, особенно с учетом того, что во многих городах услуги 4G или 5G почти такие же быстрые, как доступ к вашей домашней сети.

Для многих приложений удаленного доступа следует использовать VPN.VPN обеспечивают гибкое соединение для подключения к различным службам (веб-страницы, электронная почта, сервер SQL и т. д.) и могут защитить ваш трафик.Имейте в виду, что далеко не все VPN стоят своих денег.Имейте в виду, что услуги VPN, предоставляемые в целях обеспечения

конфиденциальности, защищают только данные, передаваемые поставщику VPN и от него, а не к месту назначения, поэтому не подходят для защиты удаленного доступа.

Наконец, для некоторых случаев использования вы также можете настроить зашифрованные удаленные подключения к удаленному рабочему столу или другому отдельному серверу.Многие из этих типов подключения (RDP, HTTPS, SSH) включают шифрование как часть своего направления обслуживания и не требуют дополнительной VPN или другой службы шифрования для защиты передаваемых данных.

Храните рабочие данные на рабочих компьютерах

Думаете о том, чтобы позаботиться о нескольких электронных письмах дома перед сном?Если вы примете меры предосторожности, такие как использование рабочего компьютера, безопасный Wi-Fi, VPN, зашифрованные диски, антивирус и защита конечных точек, это может быть совершенно нормально.С учетом сказанного, может возникнуть соблазн использовать ваш персональный компьютер, если ваш рабочий компьютер находится в другой комнате или вы забыли зарядное устройство в офисе. Это риск для вас и для компании!

Если вы работаете в организации с эффективной ИТ-командой, они могут устанавливать регулярные обновления, запускать антивирусное сканирование, блокировать вредоносные сайты и т. д., и эти действия могут быть прозрачными для вас.Есть большая вероятность, что вы не следовали тем же протоколам на вашем персональном компьютере, которые являются обязательными на работе.Более того, ваша компания, вероятно, может позволить себе более сложные технические средства контроля, которые доступны вам лично.По сути, вводя персональный компьютер в рабочую сеть, даже удаленно, вы подвергаете риску корпоративные сети и себя, принимая на себя потенциальную ответственность за значительный корпоративный ущерб в результате нарушения политики, практики или того и другого.

Если ваш работодатель предоставляет вам доступ к порталу или среде удаленного доступа, такой как Office 365 , вы можете работать в Интернете и избегать загрузки или синхронизации файлов или сообщений электронной почты на личное устройство.Всегда лучше всего использовать только свойрабочий ноутбук.для бизнеса, связанного с работой.Фактически, многие компании прекратили политику «минимального использования», которая позволяет сотрудникам вести личный бизнес с активами, принадлежащими работе, с целью снижения рисков безопасности.

Заблокируйте линии обзора

Если вы находитесь в кафе, обратите внимание на линию обзора. Если кто-то идет за вами, они могут видеть все, что вы печатаете. Более того, кто-то с правильными навыками наблюдения (например, киберпреступник) может легко наблюдать за тем, что вы делаете, и идентифицировать конфиденциальную информацию. И держите свои устройства при себе; за то время, пока вы пользуетесь туалетом, ваше устройство может быть быстро взломано злоумышленником с USB-накопителем, который набирает заранее запрограммированные

последовательности со скоростью 1000 слов в минуту. На личном уровне вы также должны делать это при вводе PIN-кода банкомата.

Шифруйте конфиденциальные данные в электронных письмах и на своем устройстве

Отправка электронных писем с конфиденциальными данными всегда сопряжена с риском. Он может быть перехвачен или увиден третьими лицами. Если вы зашифруете данные, вложенные в электронное письмо, это предотвратит просмотр информации непреднамеренным получателем. Также убедитесь, что на вашем устройстве все сохраненные данные зашифрованы на случай кражи.

15 декабря, 2020