Работаете дома?

Ознакомьтесь с рекомендациями по защите технических средств, применяемых компаниями и сотрудниками для удаленной работы

Для работодателя

Настройте двухфакторную аутентификацию. В дополнение к паролю используйте для аутентификации специальные мобильные приложения или биометрические средства.

Заранее настройте системы для удаленной работы. Выполните оценку безопасности, подготовьте рекомендации для сотрудников, предоставьте им необходимые средства защиты.

Создайте резервные копии данных. Следуйте правилу «3-2-1»: создайте три копии данных, применяя два разных формата хранения, причем одна из этих копий должна быть размещена вне компании.

Позаботьтесь о достаточном количестве лицензий VPN. Необходимо, чтобы число лицензий и пропускная способность соответствовали количеству пользователей.

Ограничьте время использования VPN. Требуйте, чтобы пользователи периодически заново входили в сеть со своими учетными данными.

Рекомендации для сотрудников

Пользуйтесь компьютером, предоставленным компанией. Компьютеры, предоставленные работодателем, должны использоваться только сотрудниками.

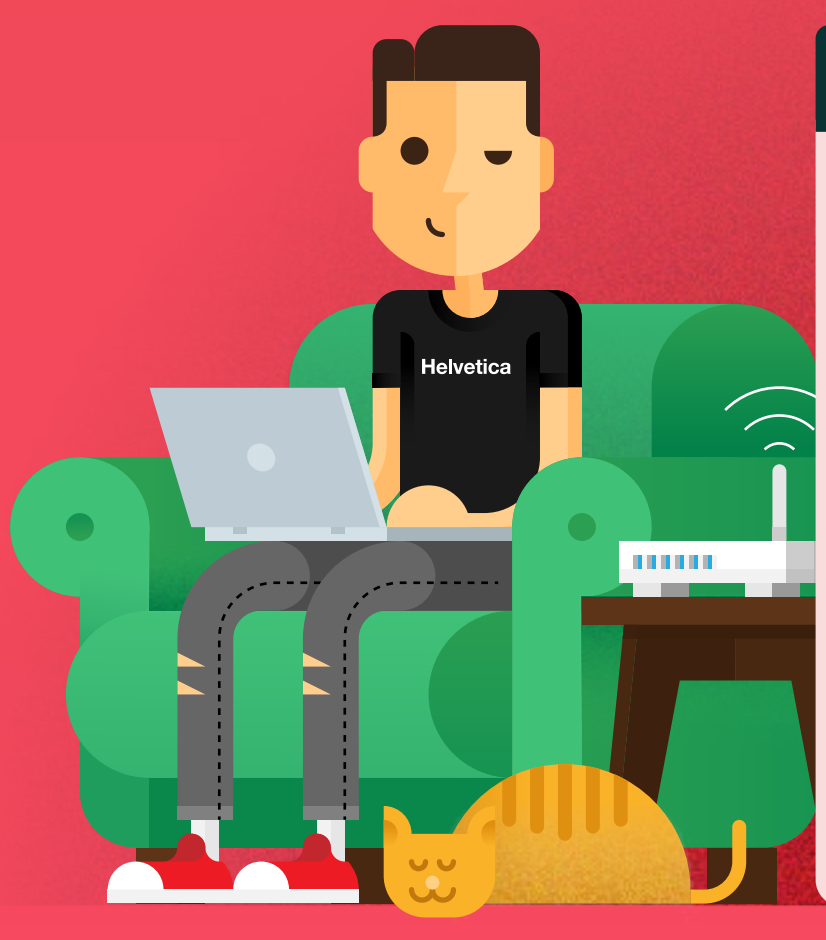
Соблюдайте правила безопасности вашей компании. Если пользуетесь личным ПК, установите на него ПО безопасности, соответствующее требованиям работодателя, и следуйте принятым в компании стандартам защиты.

Пользуйтесь VPN в соответствии с требованиями компании. На рабочем компьютере пользуйтесь VPN-серверами, которые назначил работодатель. Избегайте работы в общедоступных сетях Wi-Fi.

Сегментируйте сети. Настройте гостевую сеть для изоляции корпоративного компьютера от личных устройств.

Подготовьте средства для создания резервных копий. Предусмотрите оборудование (например, внешний жесткий диск, подключаемый по USB) и установите ПО для создания резервных копий.

Остерегайтесь онлайн-мошенничества. Мошеннические сообщения, отправители которых пользуются сложившейся в мире ситуацией, распространяются по электронной почте, через социальные сети, фальшивые приложения и вредоносные сайты.



Основы безопасности домашней сети

Обеспечьте защиту маршрутизатора. Пользуйтесь надежными паролями, обновите прошивку маршрутизатора, установите ограничения для пользовательских учетных записей.

Для опытных пользователей: применяйте прокси-сервер. Блокируйте рекламные объявления с помощью приложений класса Pi-hole или сетевого хранилища (NAS).

Увеличьте надежность паролей. Воспользуйтесь диспетчером паролей для удобства управления паролями от нескольких учетных записей.

Обновляйте программное обеспечение. Регулярно устанавливайте заплаты и обновления.

Основы безопасности Интернета для всей семьи

Обеспечьте защиту всех используемых компьютеров. Защищайте компьютеры всех членов семьи, пользуясь рекомендациями из раздела «Основы безопасности домашней сети».

Обеспечьте защиту смартфонов. Устанавливайте самые новые версии прошивки, загружайте только легальные приложения из официальных магазинов, установите мобильный антивирус.

Экономьте трафик. Ограничивайте просмотр онлайн-видео и другие трафикоемкие действия, особенно в рабочее время.

Обсудите важность безопасности в Интернете. Напомните членам семьи о необходимости соблюдения правил безопасности и конфиденциальности при использовании Интернета.

TREND MICRO | research