

Работайте безопасно повсюду

Находясь в пути, мы не оставляем кошелёк или ключи без присмотра. Мы защищаем свои ценные вещи, даже не задумываясь об этом. То же касается и работы вне привычной среды. Простые привычки помогут обеспечить безопасность вашей цифровой информации, где бы вы ни находились.

Маленькие привычки на каждый день

Используйте VPN каждый раз, подключаясь к общественной или незащищённой сети Wi-Fi

Почему это важно?

Общественные сети Wi-Fi, например, в отелях или аэропортах, не всегда безопасны. Виртуальная частная сеть (Virtual Private Network – VPN) шифрует ваш интернет-трафик, помогая защитить ваши данные от перехвата третьими лицами.

Как выработать такую привычку?

Проверьте, предоставляет ли ваша организация VPN-сервис, например, eduVPN. Такие сервисы часто бесплатны для пользователей и быстро настраиваются на устройствах. После установки всегда сначала включайте VPN перед тем, как подключиться к общественной или незащищённой сети Wi-Fi.

Используйте фильтр конфиденциальности для экрана, работая в общественных местах

Почему это важно?

Когда вы работаете в поезде, в аэропорту или в конференц-зале, окружающие могут увидеть то, что отображается на вашем экране. Фильтр конфиденциальности для экрана помогает предотвратить просмотр чувствительной информации посторонними лицами.

Как выработать такую привычку?

Если вы часто работаете в пути, используйте фильтр конфиденциальности для ноутбука. Добавляйте это в привычку каждый раз, открывая устройство в общественном месте.

Проверяйте приложения перед их установкой

Почему это важно?

Не все приложения надёжны. Некоторые содержат вредоносные программы (malware), а другие запрашивают доступ к данным или функциям устройства, которые им на самом деле не нужны, например, к вашим контактам или местоположению. Задумавшись на минуту перед установкой, можно снизить риск непреднамеренной передачи конфиденциальной информации или установки вредоносных программ.

Как выработать такую привычку?

Скачивайте приложения только из официальных магазинов приложений или с платформ, одобренных вашей организацией. Перед установкой ознакомьтесь с запрашиваемыми разрешениями и давайте доступ только к тем данным и функциям, которые действительно необходимы.

Другие полезные практики

Помимо этих привычек, несколько простых мер помогут вам работать безопасно, где бы вы ни находились:

- **Используйте служебное устройство только для рабочих целей.** Это снижает риск возникновения ненужных угроз безопасности из-за использования личных приложений, веб-сайтов или загрузок.
- **Используйте только программы и инструменты искусственного интеллекта, одобренные вашей организацией.** Это помогает предотвратить передачу конфиденциальной информации через незащищённые или неавторизованные приложения.
- **Собираетесь в регион с высоким уровнем риска?** Перед отъездом ознакомьтесь с рекомендациями вашей организации. В зависимости от места назначения вам могут потребоваться дополнительные меры безопасности для защиты ваших устройств и данных.

Узнать больше

- [VPN: безопасный туннель через общедоступную сеть](#) (источник: iBarry)
- [Кибербезопасные поездки в страны с высоким уровнем риска](#) (источник: Jisc)
- [Вредоносное программное обеспечение для мобильных устройств – советы и рекомендации по защите](#) (источник: ENISA)
- [Теневая ИТ-инфраструктура – руководство для организаций](#) (источник: NCSC UK)

SMALL HABITS. BIG IMPACT.



 GÉANT