KPMG

Як безпечно працювати з дому

Оскільки COVID-19 перетворює «роботу з дому» на просто «звичайну роботу», ми повинні адаптуватися та зосередитися на кібербезпеці в умовах нових обставин.

Олексій Янковський

Партнер,
керівник практики з надання консультаційних послуг у сфері IT та кібербезпеки

ayankovski@kpmg.ua

1

Захистіть своє середовище роботи
Спробуйте виділити та обладнати окрему кімнату під свій домашній офіс, зачиняйте двері, якщо можливо. Переконайтеся, що ваші приватні розмови залишаються приватними та не забудьте вимикнути Alexa та Google Assistant.

2

Дотримуйтесь політики чистого робочого столу
Переконайтесь, що всі паперові копії конфіденційних документів зберігаються у надійному місці, коли вони не використовуються. За можливості знищуйте, коли папери більше не потрібні.

3

Тримайте окремо робочі та домашні пристрої
Не використовуйте робочі пристрої для завантаження програм для особистого користування або інструментів для проведення конференцій, не отримавши дозволу. Використовуйте особисті пристрої для власних неробочих потреб.

4

Переконайтесь, що ваше з'єднання здійснюється через VPN
Щоб забезпечити шифрування Інтернет-з'єднання, а також захист ваших даних та активності у мережі, підключайтеся за допомогою VPN.

5

Остерігайтесь фішингових атак на тему COVID-19
Організовані злочинні групи використовують нашу стурбованість щодо COVID-19, щоб направити на нас цілу низку афер.
Слідкуйте за електронними листами, які:

- Починаються із загального привітання на кшталт «Шановний колега»;
- Містять граматичні чи орфографічні помилки;
- Вимагають персональні чи фінансові дані;
- Пропонують ліки або тести на вірус чи дефіцитні предмети;
- Вимагають від вас швидкої дії або містять погрози;
- Просять про благодійну пожертву через незвичні канали.

6

Блокуйте екрани робочих пристроїв
Блокуйте екрани робочих пристроїв, коли не користуєтесь ними, та вимикайте їх після завершення робочого дня. Не залишайте ноутбуки без нагляду.

7

Встановлюйте надійні паролі
Захистіть свої робочі пристрої надійними паролями, подумайте про використання менеджера паролів.

8

Дбайте про свою конфіденційність
Будьте уважні до того, що знаходиться в кадрі вашої веб-камери. Переконайтеся, що ви знаєте, хто бере участь у ваших конференц-дзвінках.

9

Захистіть свою точку доступу Wi-Fi
Переконайтеся, що бездротовий маршрутизатор використовує WPA2 та захищений надійним паролем.

10

Що робити, якщо ви вже «попалися»
Найголовніше, що потрібно робити, – не панікувати.

- Відкрийте антивірусне програмне забезпечення та проведіть повне сканування. Уважно слідуйте усім інструкціям.
- Зверніться до свого IT-відділу – вони скажуть, що вам потрібно робити далі.
- Якщо вас обдурили, виманивши пароль, вам слід змінити його якнайшвидше.