



Правила дистанційної роботи

Дотримуйтеся принципів кібербезпеки під час дистанційної роботи, зокрема:

1. Не допускайте до службового обладнання (наприклад, до ноутбука, телефону) сторонніх осіб, включно з домочадцями.
2. Блокуйте комп'ютер, якщо ви відходите від нього. Для цього слід натиснути:
для систем Windows - клавішу з логотипом Windows + L;
для систем Mac OS - Command + Control + Q;
3. Після закінчення роботи зберігайте документи в безпечному місці.
4. Не ведіть службові розмови в місцях, які не гарантують конфіденційності, наприклад, на балконі, в ліфті. Не викидайте паперові документи в домашні смітники. Після повернення на роботу їх потрібно знищити в шредері або викинути у спеціальний контейнер для утилізації документів.
5. Встановіть на смартфоні пароль для розблокування.
6. Використовуйте лише домашню безпроводну мережу через VPN компанії (Pulse Secure).
7. Зовнішні носії інформації, наприклад, флешки, портативні диски повинні бути зашифровані.
8. Заборонено підключати до службового обладнання приватні носії інформації.
9. Заборонено надсилати незашифровані конфіденційні дані. Пароль для відкриття файлів слід надсилати в SMS-повідомленням або вказати по телефону. Слід враховувати, що пароль *Budimex1* - це слабкий пароль.
10. Заборонено копіювати, зберігати, записувати, фотографувати службові документи на приватних пристроях.

Звертайте увагу на отримані електронні листи, не відкривайте вкладення та не натискайте на посилання невідомих відправників. Тема коронавірусу використовується злочинцями для фішинг-атаку.