ОСНОВНІ ПРАВИЛА КІБЕРГІГІЄНИ

85% кібератак пов'язані з людським фактором.
Кожні 11 секунд гакери атакують когось в мережі*

Як вберегти себе від кібератак

ПАРОЛІ

Використовуйте складні паролі

Пароль не повинен співпадати з логіном

Підключіть двофакторну авторизацію

Не використовуйте однакові паролі для всіх облікових записів

Уникайте смислових паролів: поширені фрази або слова, дівоче прізвище або ім'я вашого домашнього улюбленця.

Регулярно змінюйте паролі (не менше 3-4 разів на рік)

Користуйтесь менеджерами паролів (1Password, Bitwarden, Dashlane, KeePassXC)

СОЦІАЛЬНА МЕРЕЖА

Не використовуйте робочий e-mail та однакові паролі для всіх соціальних мереж

Видаляйте застарілі чи непотрібні облікові записи

Слідкуйте за об'ємом інформації, який ви публікуєте в мережі (персональні чи чуттєві дані, геолокація тощо)

Видаліть підозрілі підключення сторонніх сервісів до ваших акаунтів

Вкажіть довірені контакти Facebook Якщо хтось раптом зможе увійти в Facebook з вашим обліковим записом, друзі допоможуть вам повернути над нею контроль, якщо ви заздалегідь вкажете Facebook кому ви довіряєте.

E-MAIL

Створіть окремо пошту для роботи і пошту для реєстрації на інформаційних порталах

Не завантажуйте та не відкривайте вкладені файли з листі, що надіслані незнайомими особами

Перевіряйте домене ім'я відправника, перевіряйте коректність написання (наприклад @mil-gov.ua замість @mil.gov.ua)

Небезпечні листи виглядають загрозливо, лякають на емоційному рівні

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Використовуйте антивірусні програми та firewall

Регулярно оновлюйте програмне забезпечення

Завантажуйте програмне забезпечення лише з перевірених ресурсів (AppleStore або Play Market)

Налаштуйте віддалене знищення особистої інформації, у разі якщо ваш пристрій втрачено.

Не забувайте про резервне копіювання важливих даних. Налаштуйте регулярне автоматичне створення та завантаження на хмарне середовище копій.

ІНТЕРНЕТ

Пам'ятайте: **все** що потрапляє в інтернет там і залишається

Використовуйте лише сайти із захищеним з'єднанням. Всі захищенні сайти почитаються з https://

Якщо є вибір між публічним Wi-Fi та мобільною мережею, використовуйте 3G/4G

НАВЧАННЯ

Не ігноруйте основні правила кібергігієни

Постійно підвищуйте навички кібергігієни через семінари, тренінги, тематичні статті

На будь які цифрові виклики реагуйте тверезо та зважено, не керуйтесь емоціями

USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ

Електронна Республіка
громадська організація

*Human Risk Review 2022, Cybersecurity Ventures)