

Кібербезпека. Безпечний інтернет.

Вітаю у захопливому світі кібербезпеки! Ми готові відкрити вам таємниці безпечного інтернету та надати вам інструменти, необхідні для перетворення на справжніх кіберлідерів. Приготуйтеся до подорожі у футуристичний кіберпростір, де ви навчитесь захищатись від онлайн-загроз та розвивати цінні навички критичного мислення.





Що таке кібербезпека?

Визначення

Кібербезпека - це практика захисту систем, мереж та програм від цифрових атак. Вона включає в себе заходи, спрямовані на запобігання, виявлення та реагування на загрози, які можуть призвести до несанкціонованого доступу, пошкодження або крадіжки інформації.

Важливість

У сучасному цифровому світі кібербезпека є критично важливою. Із зростанням кількості пристроїв, підключених до інтернету, і все більшою залежністю від технологій, захист наших даних та систем має першорядне значення. Кібербезпека допомагає захистити нашу приватність, безпеку та цілісність інформації.

Виклики

Кіберзлочинці постійно вдосконалюють свої методи, а технології швидко розвиваються. Це створює постійну боротьбу між злочинцями та захисниками. Тому важливо, щоб ми всі підвищували свою обізнаність і вживали необхідних заходів для забезпечення належної кібербезпеки.

Типи онлайн-загроз

1 Фішинг

Фішинг - це вид шахрайства, коли зловмисники намагаються отримати конфіденційну інформацію, надсилаючи підроблені електронні листи або створюючи фальшиві веб-сайти.

3 Кібербулінг

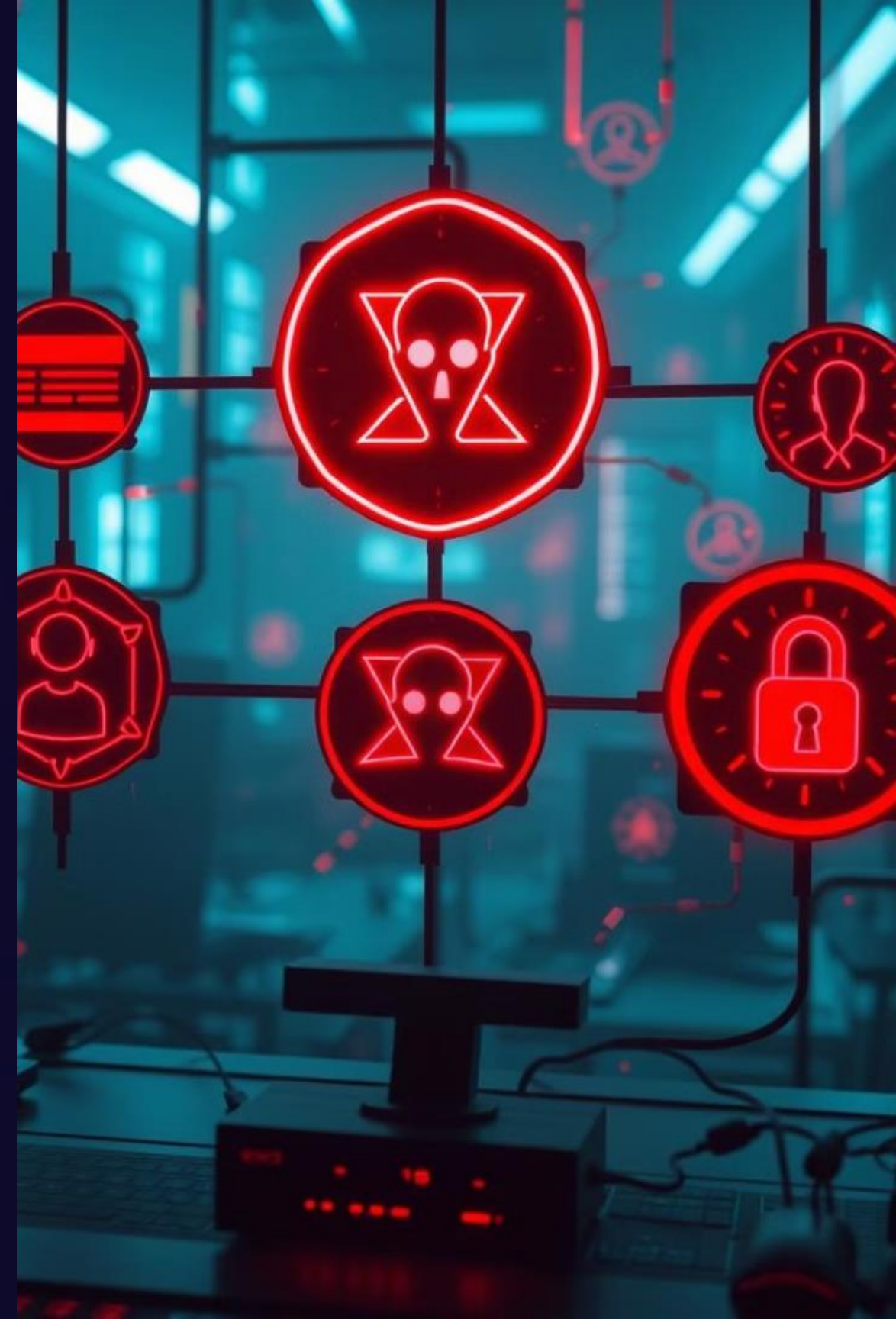
Кібербулінг - це форма залякування або переслідування, що відбувається в онлайн-середовищі. Це може включати поширення чуток, приниження або погрози.

2 Кіберзлочини

Кіберзлочини - це будь-які незаконні дії, вчинені за допомогою комп'ютерів або мереж. Вони можуть включати крадіжку даних, шантаж, вірусні атаки та багато іншого.

4 Розкриття конфіденційної інформації

Розкриття конфіденційної інформації - це ситуація, коли ваші особисті дані, такі як паролі, фінансова інформація або медичні записи, потрапляють до незнайомців.



Безпечні онлайн-практики



Приватність

Будьте обережні з тим, що ви публікуєте в Інтернеті. Перевіряйте налаштування конфіденційності на своїх облікових записах і сайтах.



Паролі та двофакторна автентифікація

Використовуйте надійні паролі, які складно вгадати. Увімкніть двофакторну автентифікацію для додаткового захисту ваших облікових записів.



Мережевий етикет

Будьте ввічливими та поважними в Інтернеті. Не поширюйте небажаний контент, не погрожуйте та не дискримінуюте інших.

Кібервиживання

Критичне мислення

Вміння критично аналізувати інформацію в Інтернеті, розпізнавати фейки та маніпуляції. Задавайте запитання, перевіряйте джерела та використовуйте логічні міркування.

Розв'язання проблем

Розробляйте творчі стратегії для вирішення кіберзагроз. Будьте готові адаптуватися, експериментувати та навчатися на помилках.

Стійкість

Підтримуйте високий рівень обізнаності про кіберзагрози, будьте стійкими до стресу та невдач. Зберігайте спокій і не впадайте в паніку.

Командний дух

Співпрацюйте з іншими, діліться знаннями та підтримуйте одне одного. Разом ми сильніші у протистоянні кіберзагрозам.





Створення безпечного цифрового відбитку



Приватність

Будьте обережні з тим, що ви публікуєте в Інтернеті.

Перевіряйте налаштування конфіденційності та обмежуйте доступ до вашої особистої інформації.



Кібергігієна

Використовуйте надійні паролі, оновлюйте програмне забезпечення та будьте пильні щодо фішингових атак.



Цифрова ідентичність

Будьте обережні при створенні онлайн-профілів. Стежте за тим, як ви представляєте себе в Інтернеті, та контролюйте свій цифровий відбиток.



Мережева безпека

Використовуйте безпечні мережі Wi-Fi, VPN і захищайте домашній маршрутизатор. Будьте обережні при підключенні до публічних мереж.

Підвищення кібербезпеки разом

1

Учні

Учні мають стати кіберлідерами, підвищуючи свою обізнаність про кіберзагрози та поширюючи знання серед однолітків.

2

Учителі

Вчителі відіграють ключову роль у навчанні учнів безпечним онлайн-практикам та розвитку цінних навичок критичного мислення.

3

Батьки

Батьки повинні бути залучені до підвищення кібербезпеки, контролюючи онлайн-активність дітей та допомагаючи їм використовувати технології безпечно.

