**Основні поняття**

**Кібербезпека або cyber security**— це заходи, які вживають для захисту даних або пристроїв, підключених до мережі, від несанкціонованого доступу та використання у злочинних цілях. Кібербезпека це те, що забезпечує конфіденційність, цілісність і доступність даних протягом їх всього життєвого циклу.

Якщо фізична безпека спрямована на захист від злочинної діяльності або випадкового пошкодження людей та фізичного майна, то кібербезпека захищає комп’ютерні та серверні системи, програми користувачів та дані, які вони в них зберігають. Кібербезпека може захистити все: від особистої інформації до складних державних систем.

**Кіберзахист** — здатність запобігати кібератакам. Це вжиття активних заходів для прогнозування кібератак з боку зловмисника та протидії вторгненням. Усі стратегії та тактики кіберзахисту мають спільну мету — запобігати кіберзагрозам, припиняти та реагувати на них.

**Чому забезпечення кібербезпеки сьогодні важливе?**

Сьогодні у кіберзлочинців набагато більше можливостей та мотивації, щоб здійснювати кібератаки: через фінансову вигоду, політичні чи соціальні мотиви. Чому? Як ми вже говорили вище, критична інфраструктура, включаючи охорону здоров’я, фінансові установи, уряди та виробництво, використовує комп’ютери або інтелектуальні пристрої як основну частину своєї діяльності

За останні два десятиліття кібератаки були здійснені проти критично важливої інфраструктури у всіх розвинених країнах, і незліченна кількість підприємств зазнали великих збитків. Щорічно у світі відбувається понад 2000 підтверджених джерел даних, кожен з яких коштує в середньому понад 3,9 мільйона доларів. З 2000 року кіберзлочинці вкрали особисту інформацію понад 3,5 мільярда людей, що становить половину населення світу, тому сьогодні фахівці з кібербезпеки дуже затребувані, як і знання запобіжних заходів, про які ми говоритимемо нижче.

**Основні види кібератак**

Для того, щоб уберегти себе від кібератак, потрібно спочатку розуміти, які види загроз можуть бути:

⛔️ **Фішинг** — зловмисники надсилають електронні листи або повідомлення жертвам, замасковані під законні, і таким чином виманюють гроші або важливі дані. Також вони можуть замінювати URL-адресу.

**⛔️ Боти та автоматичні атаки**— більшість кібератак здійснюють автоматизовані боти, які можуть сканувати системи на наявність вразливостей, намагатися вгадувати паролі та заражати системи шкідливими програмами.

**⛔️ DDoS-атаки** — надсилання великих обсягів фальшивого трафіку до комп’ютерної системи доти, доки обсяг трафіку не переповнить її, позбавивши доступу законних користувачів.

**⛔️ Шкідливе програмне забезпечення** — програмне забезпечення, створене для допомоги чи проведення кібератак або заподіяння шкоди комп’ютерним системам. Зазвичай воно здатне поширюватись і заражати додаткові комп’ютерні системи.



**Напрями кібербезпеки**

1. **Кібербезпека критичної інфраструктури**

Організації критичної інфраструктури більш вразливі до атак, ніж інші, тому що диспетчерське управління та збір даних часто покладаються на застаріле програмне забезпечення, тому вони потребують забезпечення кібербезпеки.

1. **Безпека мережі**

Безпека мережі включає усунення вразливостей, що впливають на ваші операційні системи та мережеву архітектуру — сервери і хости, маршрутизатори і точки бездротового доступу, а також мережеві протоколи.

1. **Хмарна безпека**

Хмарна безпека пов’язана із захистом даних, застосунків та інфраструктури у хмарі.

1. **Безпека IoT (Інтернету речей)**

Безпека IoT — захист інтелектуальних пристроїв, підключених до IoT. Вони підключаються до мережі без втручання. Наприклад, це можуть бути інтелектуальні пожежні сигналізації, освітлення, термостати та інші пристрої.

1. **Безпека застосунків**

Безпека програм — усунення вразливостей, що виникають внаслідок небезпечних процесів розробки під час проєктування, кодування та публікації програмного забезпечення або вебсайту.

**Основні заходи щодо захисту особистих даних**

Ми з вами розібралися в тому, що та кібербезпека, які є її види і тепер найголовніше — як захистити себе від кібератак? Читайте нижче основні поради.



♻️ **Встановіть надійне антивірусне програмне забезпечення**

Хороша та надійна антивірусна програма – обов’язковий елемент будь-якої системи кібербезпеки. Вона виявляє та видаляє віруси та шкідливі програми. Вона також сканує та відфільтровує потенційно небезпечні завантаження та електронні листи. Важливий момент: щоб убезпечити себе, потрібно буде не забувати регулярно оновлювати це програмне забезпечення.

**♻️ Використовуйте складні паролі**

Будь то відповіді на контрольні питання або паролі, переконайтеся, що вони складні, щоб хакерам було важко зламати їх.

Щоб отримати відповіді на контрольні питання, спробуйте перекласти їх іншою мовою. Це може зробити їх важкими для розшифровки, а також менш сприйнятливими до соціальних технологій.

Використання пробілу перед або після ваших паролів також гарна ідея, щоб збити хакера з пантелику. Використання комбінації верхнього та нижнього регістру також допомагає.

**♻️ Захистіть мережу за допомогою брандмауера**

Чим відрізняється брандмауер від антивірусної програми? Брандмауер захищає як апаратне, так і програмне забезпечення, що робить його зручним для будь-якої компанії із фізичними серверами. Але брандмауер також блокує чи утримує віруси від проникнення у вашу мережу, тоді як антивірус націлюється на програмне забезпечення, яке вже уражене вірусом. Інакше кажучи, вони добре працюють разом. Установка брандмауера допомагає захистити мережевий трафік малого бізнесу як вхідний, так і вихідний. Це може завадити хакерам атакувати вашу мережу, заблокувавши певні вебсайти. Його також можна налаштувати так, щоб обмежити відправлення службових даних та конфіденційних електронних листів із мережі вашої компанії.

**♻️ Встановіть програмне забезпечення для шифрування**

Якщо ви щодня працюєте з даними, які належать до кредитних карток, банківських рахунків та номерів соціального страхування, вам потрібно мати програму шифрування. Шифрування забезпечує безпеку даних, перетворюючи інформацію на комп’ютері на коди, що не читаються. Шифрування розроблено з урахуванням найгіршого сценарію: навіть якщо ваші дані будуть вкрадені, вони не будуть цінними для хакера, оскільки він не матиме ключів для розшифрування даних та інформації.

**♻️ Ігноруйте підозрілі електронні листи та повідомлення**

Зробіть звичкою ніколи не відкривати та не відповідати на підозрілі електронні листи, навіть, якщо вони здаються вам знайомими, не натискайте на підозрілі посилання та не завантажуйте вкладення. Це може зробити вас жертвою онлайн-крадіжки фінансів та особистих даних за допомогою «фішингової» афери, про яку ми говорили вище. Через фішингові електронні листи хакер намагається отримати ваші особисті та фінансові дані. Для більшої безпеки змінюйте пароль електронної пошти кожні 60–90 днів. Крім того, утримайтеся від використання одного і того ж пароля скрізь, де є ваші дані.

**♻️ Часто створюйте резервні копії даних**

Потрібно або вручну створювати резервні копії всіх даних на зовнішньому жорсткому диску або хмарі, або просто запланувати автоматичне резервне копіювання, щоб забезпечити безпечне зберігання вашої інформації. Таким чином, навіть якщо ваші системи будуть скомпрометовані, ваша інформація, як і раніше, буде з вами в безпеці.

**♻️ Захистіть мережу Wi-Fi і не підключайтеся до загальнодоступної мережі**

Перестаньте використовувати мережу WEP (або Wired Equivalent Privacy), якщо ви все ще використовуєте її, і натомість перейдіть на WPA2 (це Wi-Fi Protected Access версії 2), оскільки остання набагато безпечніша. Щоб захистити мережу Wi-Fi від зламування хакерами, приховайте ім’я бездротової точки доступу або маршрутизатора, щоб воно не відображалося у списку мереж.