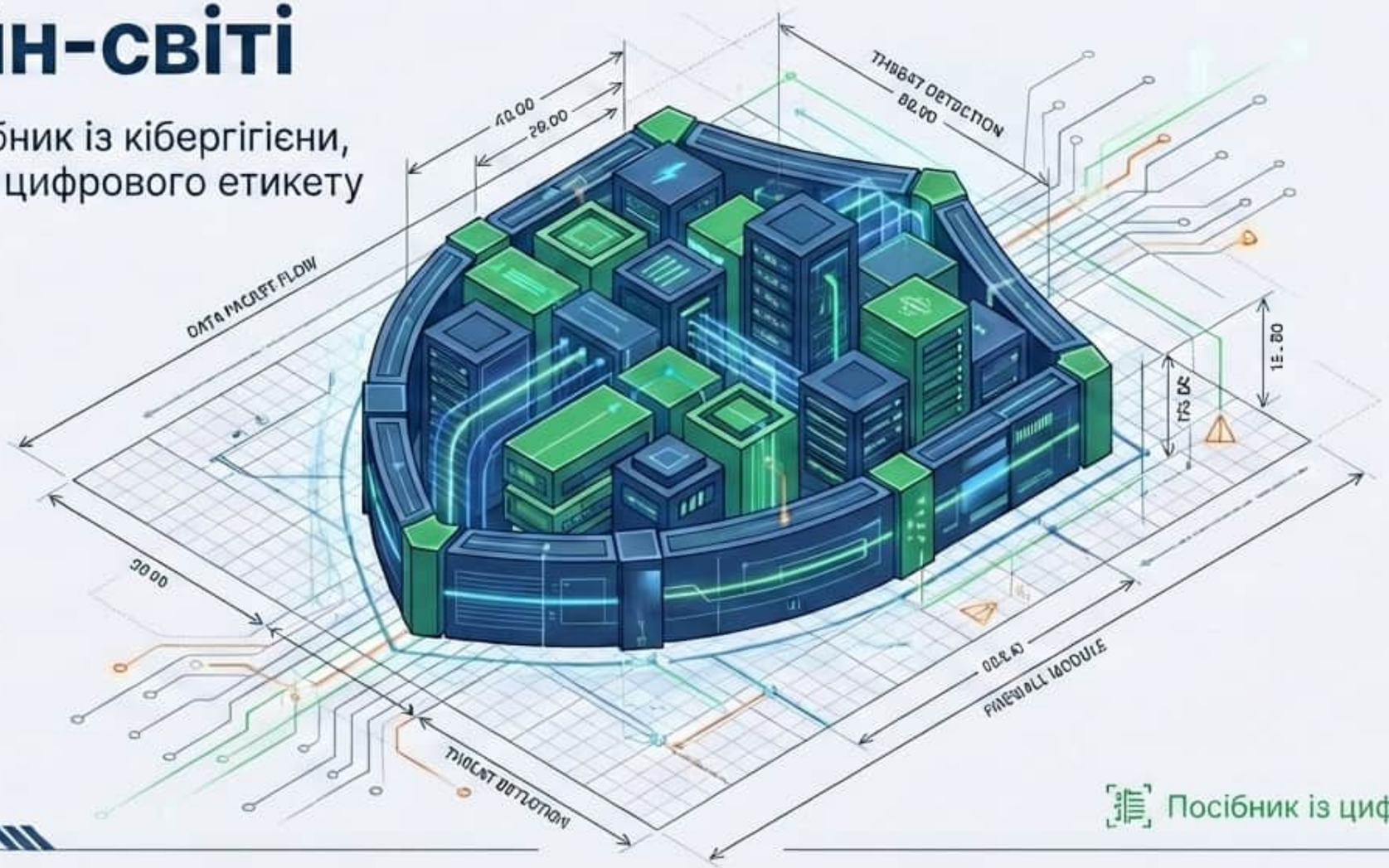
Цифрова Фортеця: Стратегія виживання в онлайн-світі

Механіко-технологічний фаховий коледж ОНТУ, ц.к КІТтаМ.
Відкрита лекція, к.т.н. Ярового І.І.

Практичний посібник із кібергігієни, захисту даних та цифрового етикету



mtfk.ontu.edu.ua

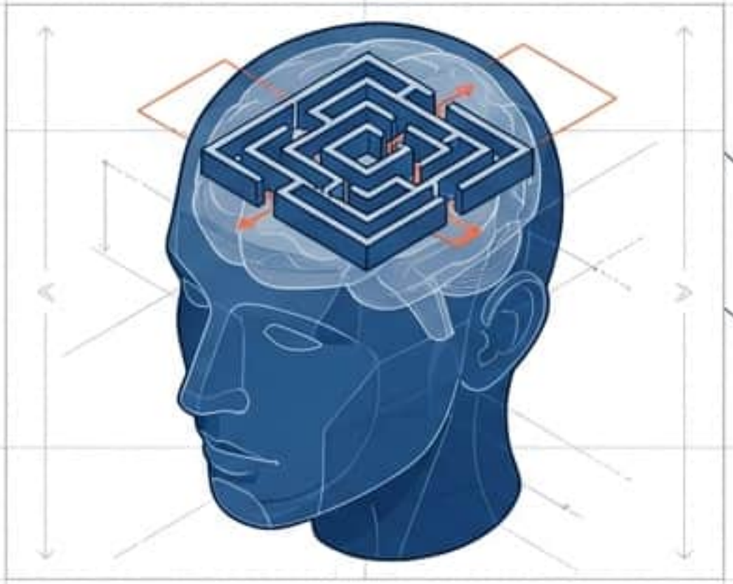
Посібник із цифрової безпеки

NotebookLM

Ландшафт загроз: Хто атакує вашу фортецю?

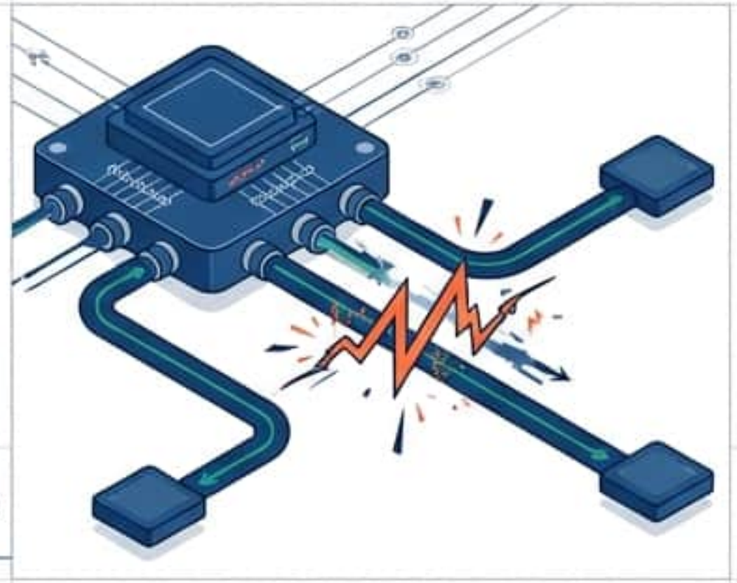
Технічні атаки

- **Malware:** Віруси, трояни, шпигунське ПЗ.
- **Мережеві загрози:** DDoS-атаки, бот-мережі (Botnets).



Психологічні атаки

- **Соціальна інженерія:** Маніпуляція довірою (Фішинг, Смішинг, Вішинг).
- **Кібербулінг:** Психологічний терор та залякування.



Гібридні загрози

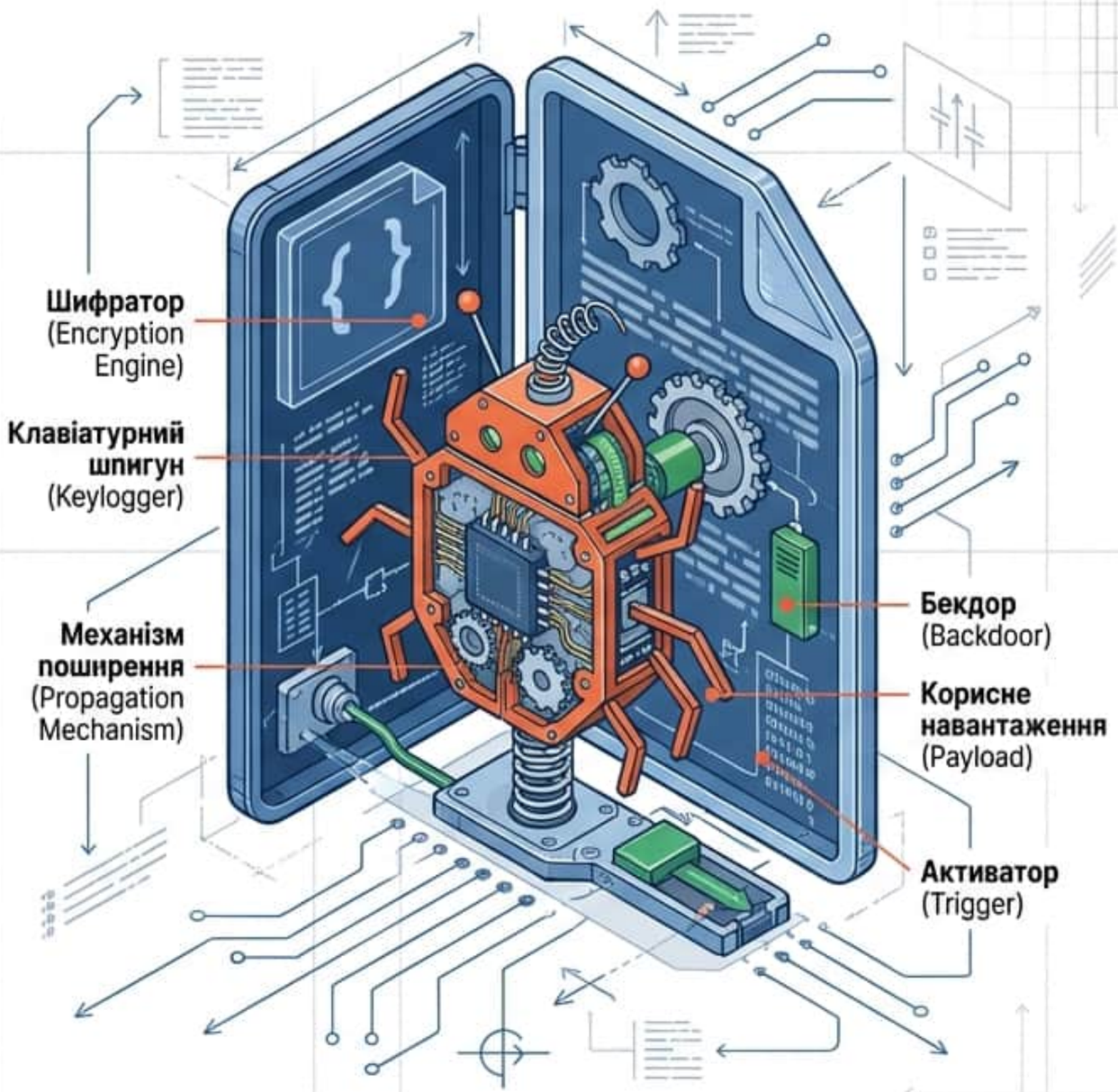
- **Атака «Людина посередині»:** Перехоплення даних у каналах зв'язку.
- **Supply Chain Attack:** Атака через менш захищеного партнера.

NotebookLM

Анатомія шкідливого програмного забезпечення (Malware)

- **Програми-вимагачі (Ransomware)**
  Блокують доступ або шифрують файли, вимагаючи викуп. *Приклад: WannaCry.*
- **Шпигунське ПЗ та Кілогери**
  Таємно збирають інформацію та записують натискання клавіш для крадіжки паролів.
- **Троянські програми**
  Маскуються під легальне ПЗ. Часто ховаються у піратських версіях програм або ігор.

Insight: Завантаження піратського контенту або «безкоштовних» версій платних програм — найшвидший шлях інфікувати систему.



NotebookLM

Соціальна інженерія: Злам людського мозку

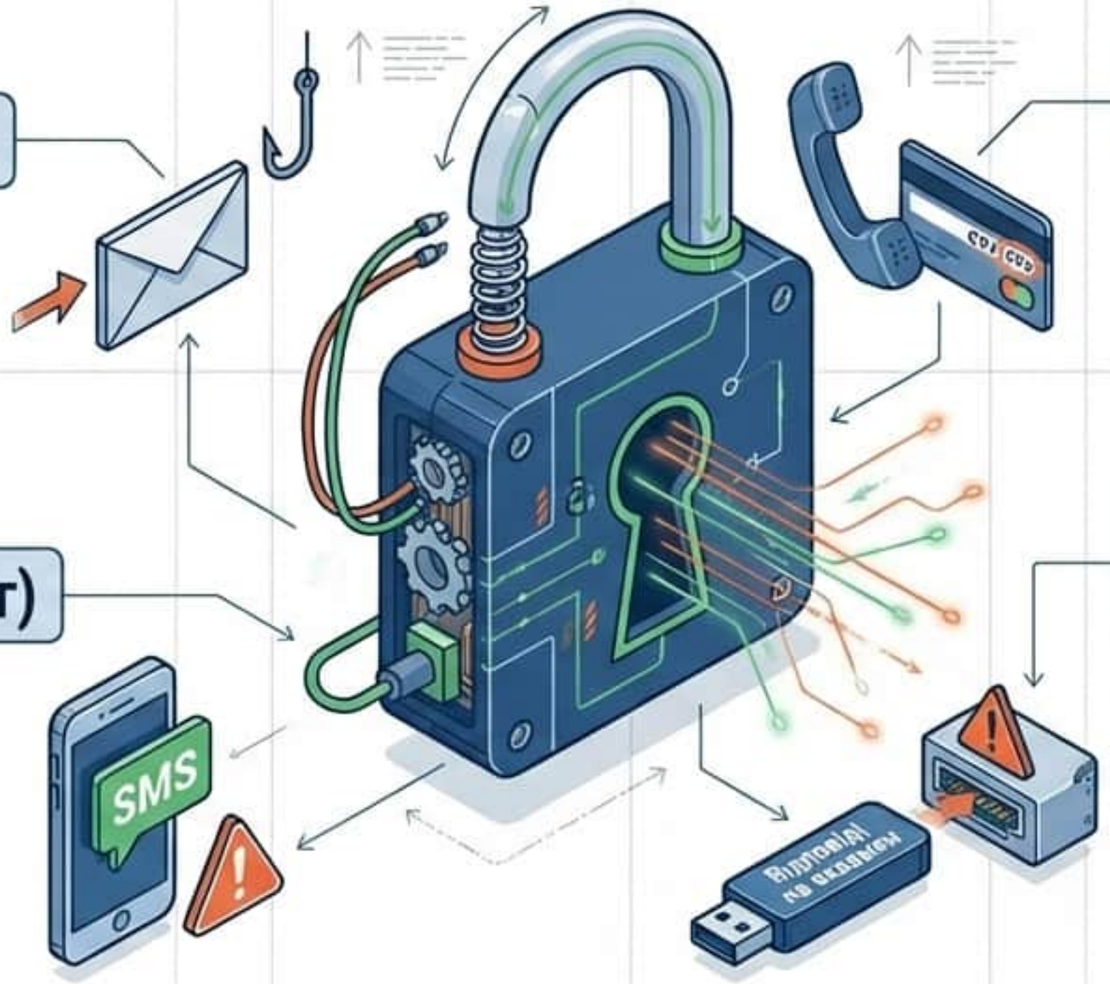
Метод маніпуляції, що змушує жертву добровільно віддати дані.

Phishing (Фішинг)

Масове розсилання фальшивих листів.

Smishing (Смішинг)

Шахрайство через SMS-повідомлення.



Vishing (Вішинг)

Телефонне шахрайство (наприклад, дзвінок від псевдоспівробітника банку з вимогою назвати CVV-код).

Tactic «Road Apple» (Дорожнє яблуко)

Підкидання фізичних носіїв (флешок) з інтригуючими назвами (наприклад, «Відповіді на екзамен»), які автоматично встановлюють віруси при підключенні.

NotebookLM

Студент у прицілі: Чому це стосується вас?

Фактори ризику: Активність у соцмережах, публічні Wi-Fi, довіра до «адміністрації».

UNIVERSITY BUILDING
Університетська будівля

CREDIT CARD
Кредитна картка.

SOCIAL MEDIA PROFILE
Профіль у соцмережах.

Фейкова адміністрація
Листи від «університету» з вимогою терміново змінити пароль.

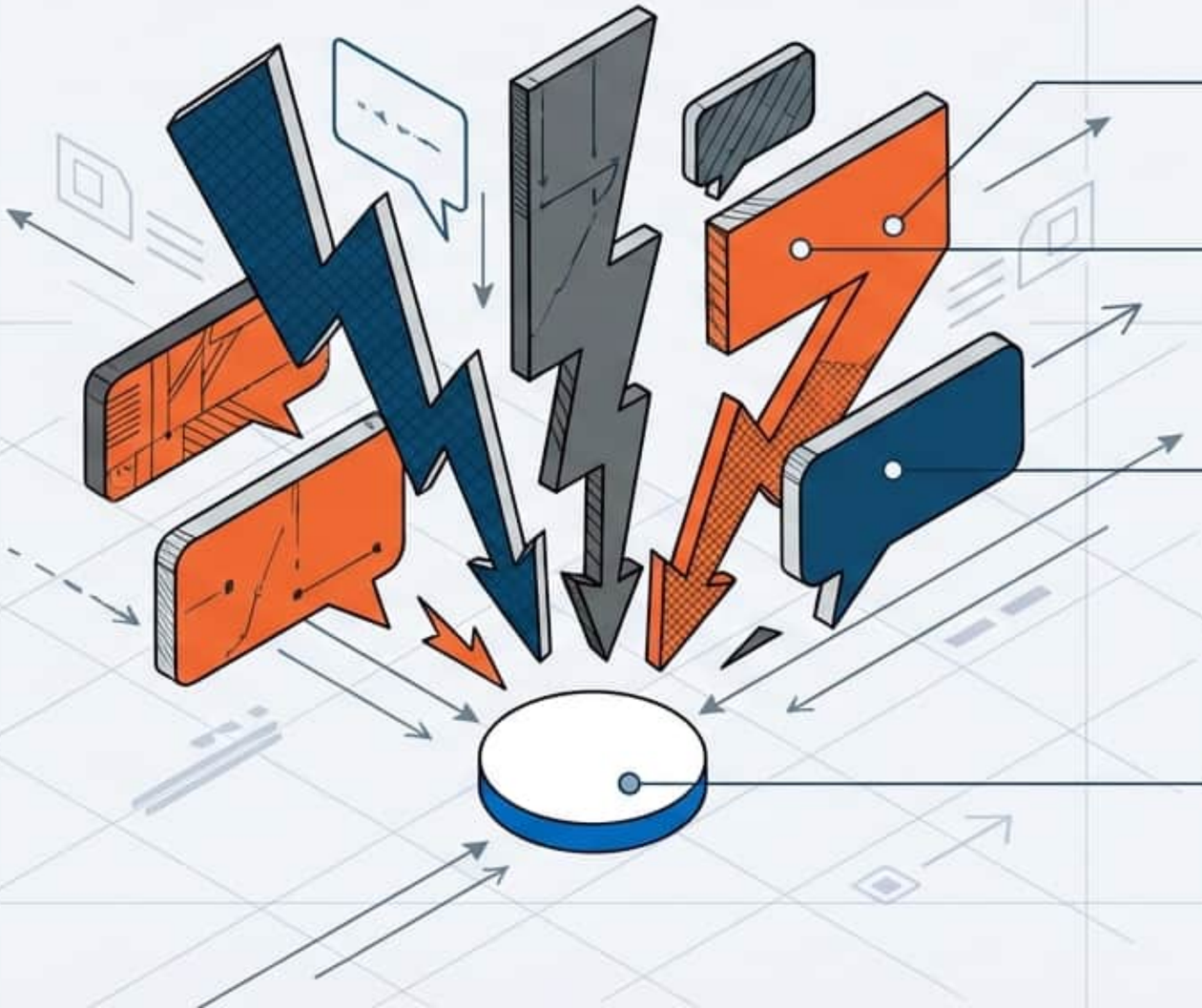
Identity Theft (Крадіжка особистості)
Використання відкритих даних (дата народження, прізвище матері) для оформлення кредитів.

Схема «Позич гроші»
Створення клонів профілів для шахрайства з друзями жертви.

NotebookLM

Темна сторона комунікації: Психологічна безпека

- **Кібербулінг:** Систематичне цькування та приниження.



Флеймінг: Публічні емоційні сварки в чатах.

Самозванство: Злам акаунту для розсилання образливих повідомлень від імені жертви.

Грумінг: Спроби дорослих встановити довірливі стосунки з метою експлуатації.

Небезпечний контент: «Смертельні квести», пропаганда насильства та ігрова залежність.

NotebookLM

Фундамент оборони: Паролі та Аутентифікація

- **Правило 12 символів:** Пароль має містити мінімум 12 символів (великі й малі літері, літери, цифри, спецсимволи).
- **Унікальність:** Один сервіс = Один унікальний пароль.
- **Менеджери паролів:** Використовуйте Bitwarden або KeePass замість записників.

Критичний захист: Двофакторна автентифікація (2FA)

Це обов'язковий бар'єр — навіть якщо пароль викрадено, зловмисник не пройде без не коду з SMS/застосунку.

NotebookLM

Захист периметра: Пристрої та ПЗ

- **Active Defense**

  Встановлення надійного антивірусу та увімкнення брандмауера (мережевого екрану).

- **Patching Vulnerabilities**

  Оновлення ОС та програм закриває «діри», якими користуються хакери. Не ігноруйте нагадування про оновлення.

- **Source Control**

  Завантажуйте програми лише з офіційних джерел. Піратське ПЗ — це «троянський кінь» для вашої системи.

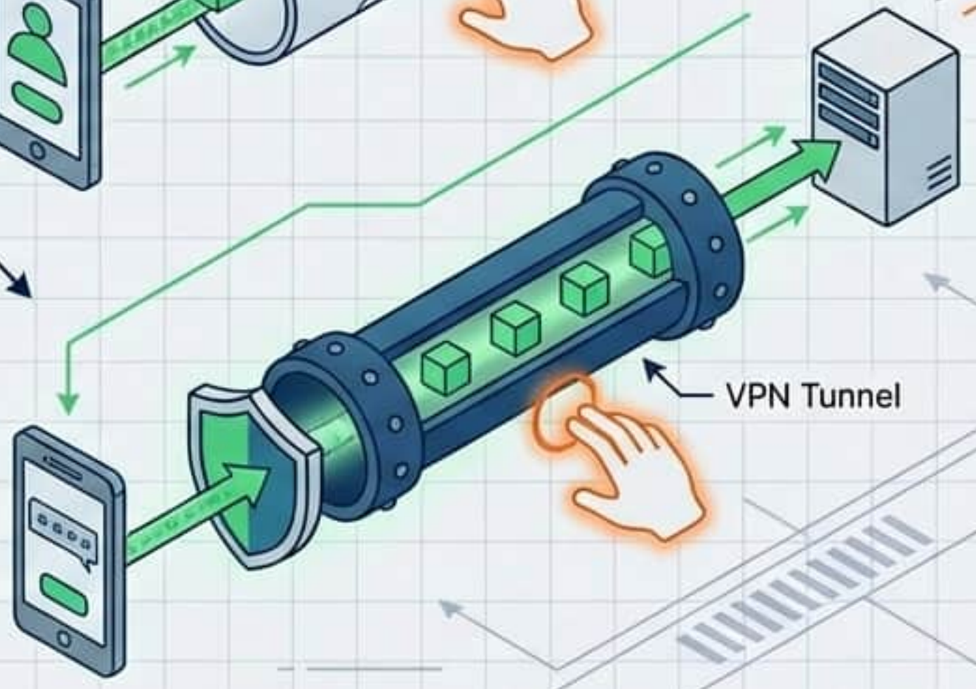
NotebookLM

Безпечні шляхи: Робота в мережах Wi-Fi

Alert

Загроза: Атака «Людина посередині» (Man-in-the-Middle). Хакери створюють мережі-двійники у кафе для перехоплення трафіку.

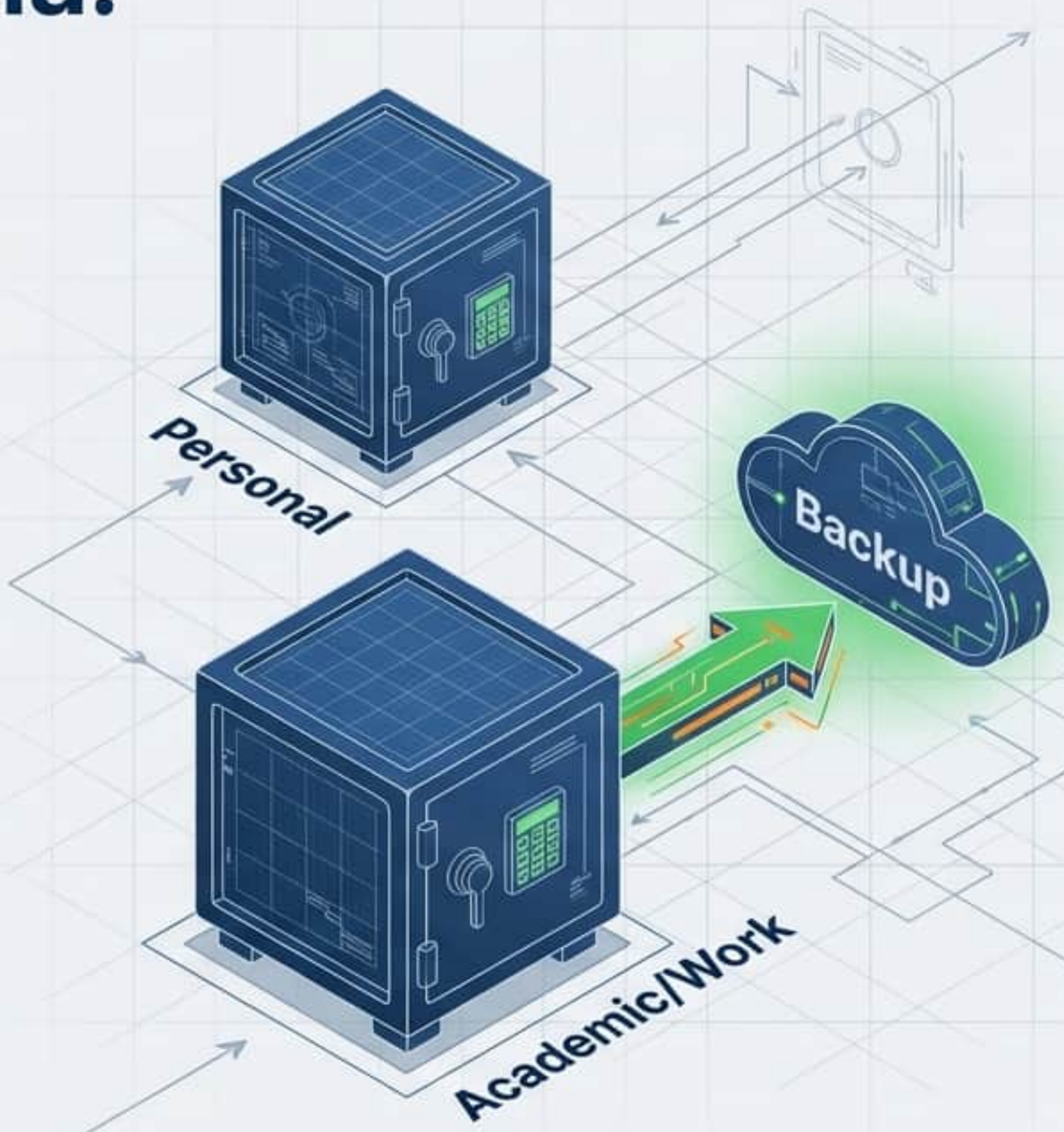
- **Протокол List:**
  1. Уникайте відкритих мереж без пароля.
  2. Завжди перевіряйте **HTTPS** (значок «замочка»).
  3. **VPN**: Обов'язковий інструмент для шифрування трафіку у публічних мережах.



NotebookLM

Інформаційна оборона: Збереження даних

- **Резервне копіювання (Backup)**
  Регулярно зберігайте важливі документи на зовнішніх дисках або у хмарі. Це єдиний порятунок від програм-вимагачів.
- **Сегрегація**
  Розмежуйте особисте та навчальне. Не використовуйте університетську пошту для реєстрації в соцмережах.
- **Data Minimization**
  Не публікуйте адресу, фінансовий стан чи графік відпусток — це запрошення для злодіїв.



NotebookLM

Ваш цифровий слід та репутація

Інтернет пам'ятає все.

Ваші фото, коментарі та лайки формують досьє, яке можуть переглядати роботодавці або шахраї.

Privacy Rules

- Не розголошуйте особисті дані інших (телефон, фото) без дозволу.
- Запитайте згоду перед тим, як позначити друга на фото (Tagging).
- Поважайте авторське право — не привласнюйте чужий контент.

NotebookLM

Нетикет: Кодекс честі в цифровому світі

- **The Golden Rule**

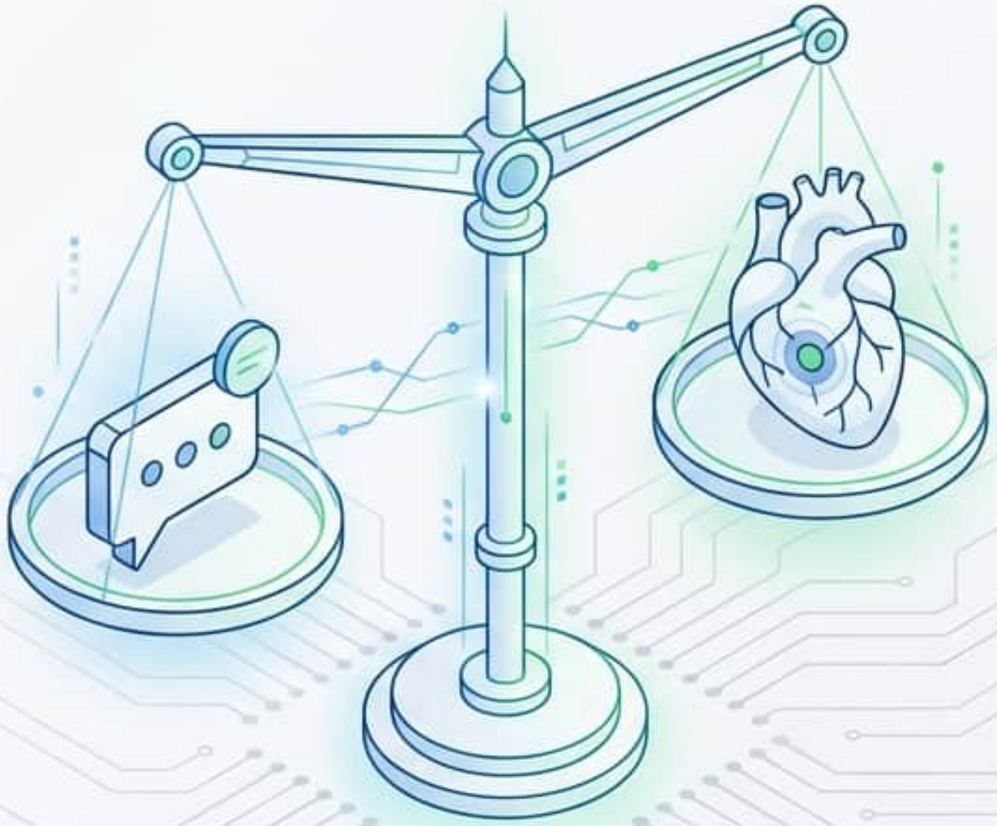
  Пам’ятайте про людину. Не пишіть того, що не сказали б в обличчя.

- **Context Awareness**

  «Озирніться» перед тим, як писати. Правила спілкування в чаті геймерів та на університетському форумі різні.

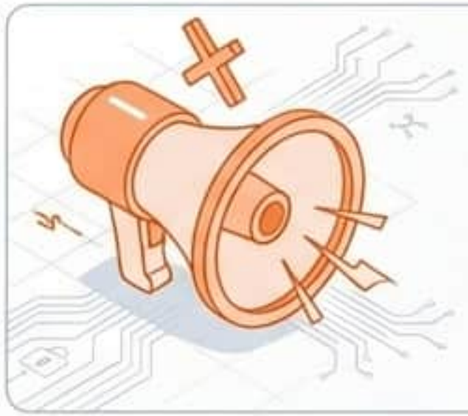
- **Respect Time**

  Не очікуйте миттєвої відповіді. Вказуйте розмір великих вкладень, щоб не перевантажувати трафік співрозмовника.



NotebookLM

Техніка ефективної комунікації



NO CAPS LOCK:
Текст великими літерами сприймається як крик.

Conciseness:
Уникайте оверквотингу (надмірного цитування). Відповідайте по суті.

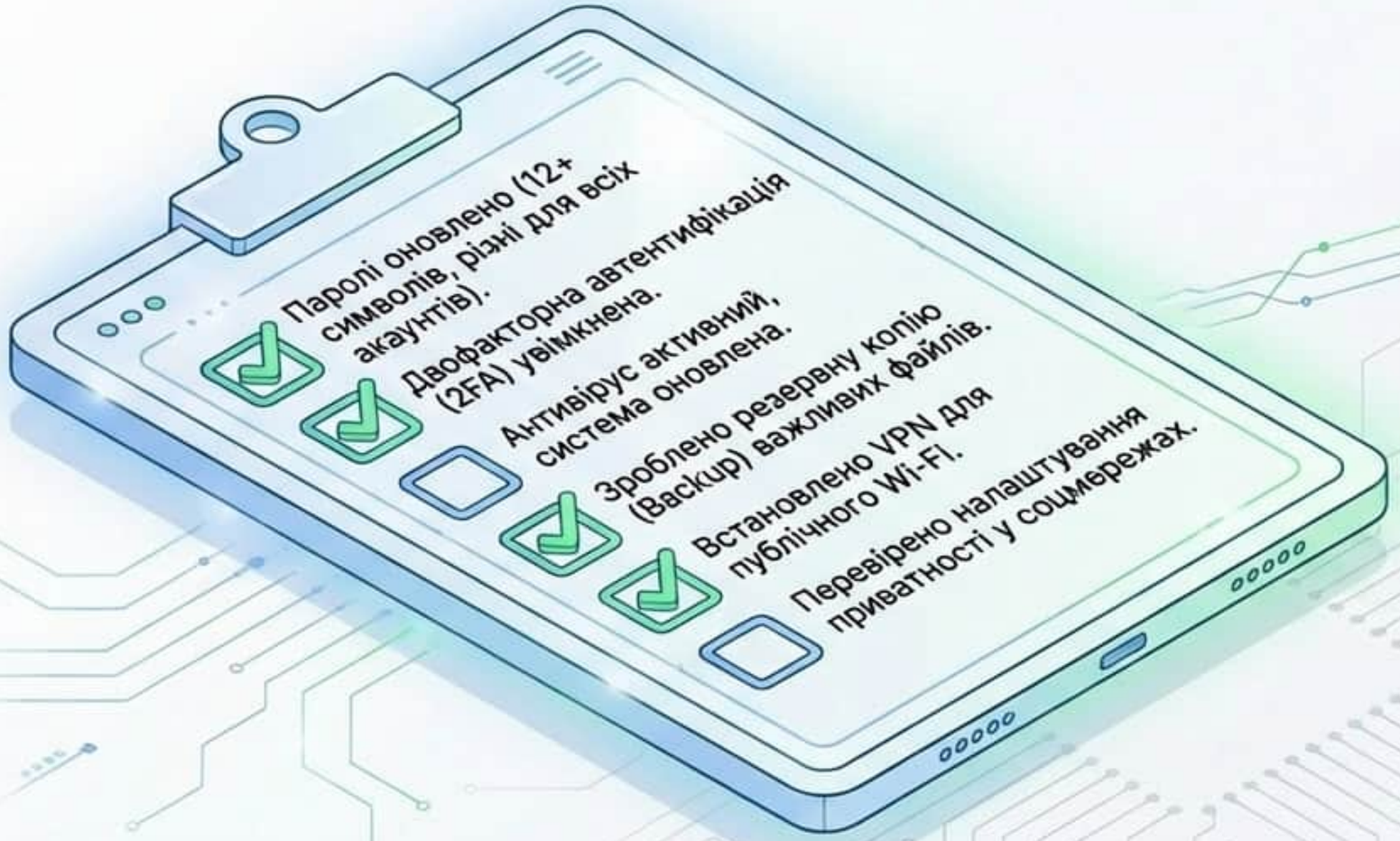
Subject Line:
Тема листа має чітко відповідати змісту.

Emotion Control:
Використовуйте смайли доречно, але не зловживайте ними.

Conflict Management:
Не годуйте тролів. Найкраща реакція на агресію — ігнорування.

NotebookLM

Чек-лист безпеки: Перевір свою фортецю



NotebookLM

Безпека — це процес, а не результат

Цифрове середовище змінюється щодня. Ваша найкраща зброя — це критичне мислення та постійне навчання.

Будьте свідомими споживачами контенту. Створюйте безпечний освітній простір навколо себе.

Дотримання цифрової гігієни та етикету — це запорука не лише захисту даних, але й вашого психологічного комфорту.

NotebookLM