ST&T

GUARDIAN OF THE MATRIX

ГАЙД FREE

ЗАХИСТ ПАРОЛІВ

🔐 АЛЕ СПОЧАТКУ ТЕСТ: НАСКІЛЬКИ НАДІЙНИЙ ТВІЙ ПАРОЛЬ?

Запитай себе:

🔢 Менше ніж 12 символів?

🔁 Використовуєш той самий пароль у кількох акаунтах?

📅 Є дата народження, ім’я домашнього улюбленця, слово “пароль” або “qwerty”?

📬 Твій email злитий у базах (перевір: haveibeenpwned.com)?

📝 Зберігаєш паролі у нотатках або в браузері?

❗ Якщо відповів «так» на 2 і більше пунктів — настав час терміново змінити паролі

КРОК	ЩО РОБИТИ	НАВІЩО
Унікальні надійні	Створювати довгі (12+ символів) складні паролі з різними символами для кожного сайту	Щоб один зламаний пароль не дав доступ до всіх обліковок
Менеджер паролів	Використовувати Bitwarden, 1Password або інший менеджер паролів — зберігайте всі паролі в зашифрованому сейфі	Щоб не повторювати, не забувати і мати сильні унікальні паролі без головного болю
Двофакторна автентифікація (MFA)	Увімкніть MFA усюди, де можливо — бажано через застосунок (TOTP), ще краще — через апаратний ключ	Щоб зламати ваш акаунт було неможливо лише через пароль — потрібен ще фактор
Захист від фішингу	Не вводити паролі за лінками з пошти/SMS. Завжди перевіряйте URL. Уникайте QR-кодів невідомого походження	Фішинг топ-1 вектор атак. Якщо не клікати — не піддаєтесь
Перевірка витоків	Регулярно перевіряйте свої email на haveibeenpwned.com або через менеджер паролів на злиті облікові дані	Щоб вчасно міняти паролі після зливів, поки ними не скористались злочинці
Оновлення та безпечні пристрої	Оновлюйте ОС, браузери, антивіруси. Не ставте підозрілі програми. Не вносьте зміни в операційну систему	Щоб не підхопити інфостілер і не злити всі паролі за раз
Сталий MFA FIDO2 / Passkeys	Для критичних акаунтів використовуйте апаратні ключі (YubiKey) або Passkeys. Уникайте SMS-кодів як MFA	Щоб не підхопити інфостілер і не злити всі паролі за раз
Менше цифрових слідів	Не публікуйте особисті дані (дати нар., імена домашніх тварин тощо). Не використовуйте їх у паролях	Щоб хакерам було важко дізнатись секретні питання, підбирати паролі або шантажувати
Кейс-менеджмент і знання актуальних атак	Час від часу перечитуйте кейси атак (Snowflake, RockYou, інфостілери), щоб розуміти нові методи хакерів	Хто знає, той живе довше: знання про нові атаки = превентивна безпека

🛠️ ЯК СТВОРИТИ НАДІЙНИЙ ПАРОЛЬ (І НЕ ЗАБУТИ ЙОГО)

Рекомендації:

- ✅ Мінімум 12 символів
- ✅ Випадкові літери, цифри, символи
- ✅ Не використовуй особисті дані (дата народження, імена)
- ✅ Пароль має бути унікальним для кожного сайту

🧠 ЯК ЗАПАМ’ЯТАТИ НАДІЙНИЙ ПАРОЛЬ?

📌 Використай **метод фрази**:

- ✅ “У мами 3 кота, всі пухнасті 🐱!” → Um3k,vp🐱!

📌 Або **менеджер паролів** — він запам’ятає все за тебе

💼 БЕЗКОШТОВНІ ІНСТРУМЕНТИ:

🔐 Менеджери паролів:

- Bitwarden — безкоштовний і надійний
- NordPass Free
- KeePassXC — для технарів

📲 Автентифікатори:

- Microsoft Authenticator
- Google Authenticator
- Authy

🧪 Перевірка витоків:

- haveibeenpwned.com

📌 ST&T НАГАДУЄ:

цифрова гігієна — це нова форма особистої безпеки
Як чистити зуби щодня — так і з цифровими звичками
І чим раніше ви почнете — тим менше шансів, що колись доведеться «платити» за необачність

📲 **Підписуйся, якщо хочеш знати все про цифрову безпеку простою мовою і з реальними прикладами**

https://stt.llc