

Кібербезпека у світі та в освіті: як захистити себе та учнів

Кіберпростір як ще один фронт

Кіберпростір — частина війни, у якій бере участь кожен з нас.

Викладачі — важливий елемент в цій боротьбі, бо вони ті, хто мають навчити захищатися дітей та протистояти **самостійно** великій кількості дезінформації.

Приклади:

- Підроблені листи “від МОН”.
- Telegram-боти з опитуваннями, що крадуть контакти.

📄 💬 “Будучи слабким в цифровому світі — неможливо протистояти ворогу в реальному.”

Людський фактор: як нас ламають не кодом, а словами

9 з 10 атак починаються не з вірусу, а з повідомлення.

Використовуються емоції: страх, терміновість, цікавість, авторитет.

Приклади:

- “Тремін дії Вашого паролю минув, оновіть зараз.”
- “Терміново подайте звіт МОН та надішліть на цю пошту.”
- “Вам надійшла посилка, перейдіть за посиланням для сплати”



💬 “Хакери не зламують комп’ютери — вони зламують людей через довіру.”



Як розпізнати фішинг

Перевірка відправника

Дивитись не на логотип, а на відправника й адресу.

Перевірка посилань

Перевіряти посилання, особливо якщо лист просить зробити дію "терміново".

Приклад: Адреса "classroom.googIe.com" (з літерою "I" замість "l").



"Буквально одна літера може стояти між вами та зловмисником. Ваша увага – це ваш захист."

4 основи кібергігієни

Без цих чотирьох речей жодна система не допоможе.



Надійний пароль

Довгий, різний для кожного акаунту.



Менеджер паролів

Замість блокнота використовуйте рішення, які дозволять зберігати багато паролей і не тримати їх в блокноті чи пам'яті



Двофакторна автентифікація

Ваш телефон, це ваша додатковий ключ для захисту своїх даних. Не нехтуйте одним додатковим кроком, щоб кратно ускладнити життя зловмисникам.



Оновлення систем

Це “вакцина” проти вразливостей і ні, жоден виробник не має на меті зробити ваш телефон повільнішим. Він глючить через старість, а не оновлення.

🗒️ “Кібергігієна — це як догляд за здоров'ям. Здоровим всеодно не помреш, а приймаєш житимеш з меншою кількістю потенційних проблем, таких як колектори, вкрадені кошти та постійна реклама через дзвінки.”

Типові помилки викладачів

Зберігання документів

Документи зберігаються на робочому столі без паролю.

Фізична безпека даних

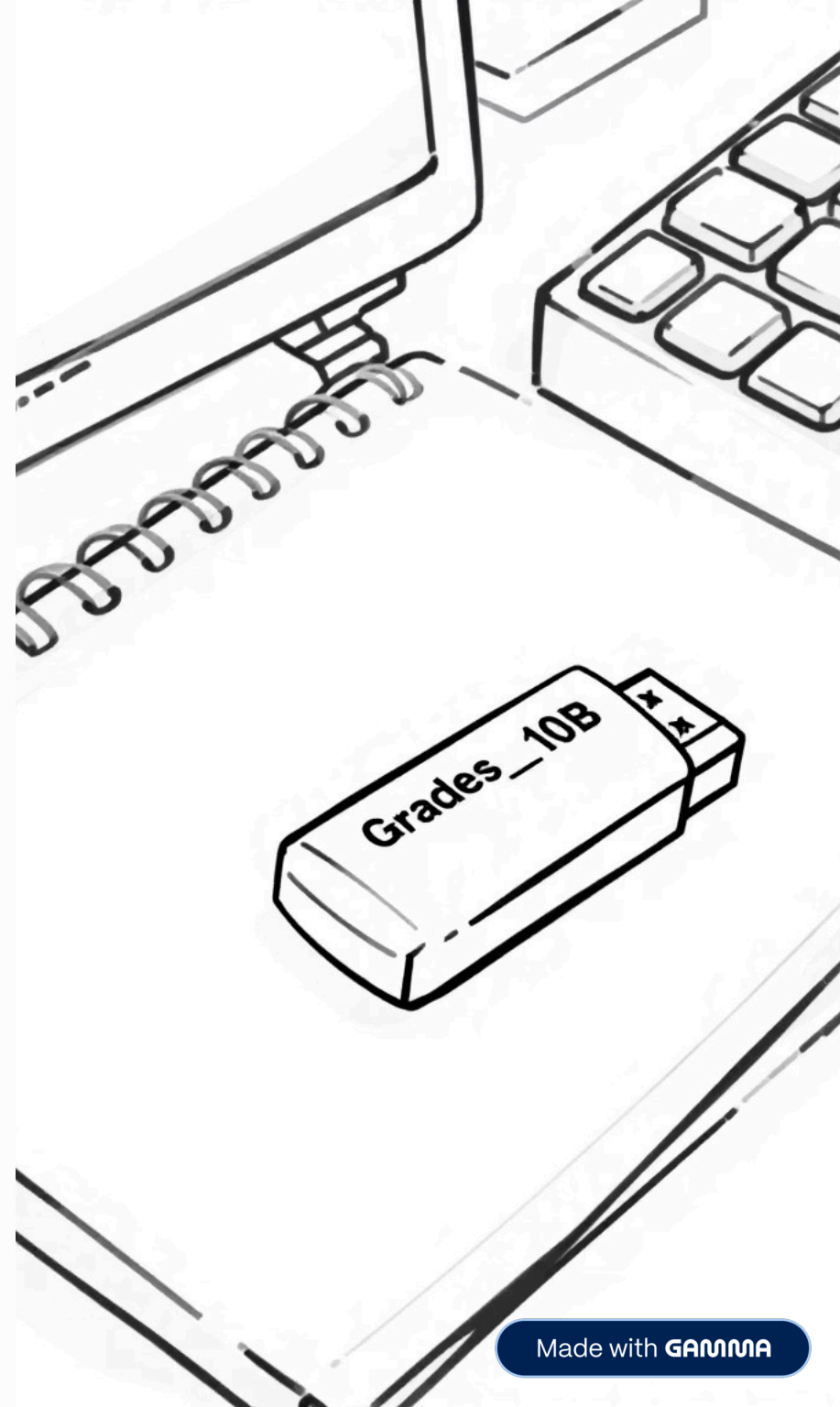
Флешки з мігрують між учнями та викладачами без жодного захисту та засобів попередньої перевірки.

Повторне використання паролів

Один пароль — на всі сервіси.

Приклад: Учень знаходить флешку “Змінює дані у ваших файлах на якісь сайти із сумнівною репутацією та фотографіями інтимного характеру, а ви потім пояснюєте, що це не ви”.

💬 “Комп’ютер без пароля — це відкрите вікно у ваше особисте життя та прямий вплив на ваше авторитет в колективі”



Як убезпечитись просто



Пароль на комп'ютер

Мінімальний пароль на комп'ютер — уже бар'єр.



Організація файлів

Не тримати документи на "Робочому столі".



Резервні копії

Робити резервні копії.

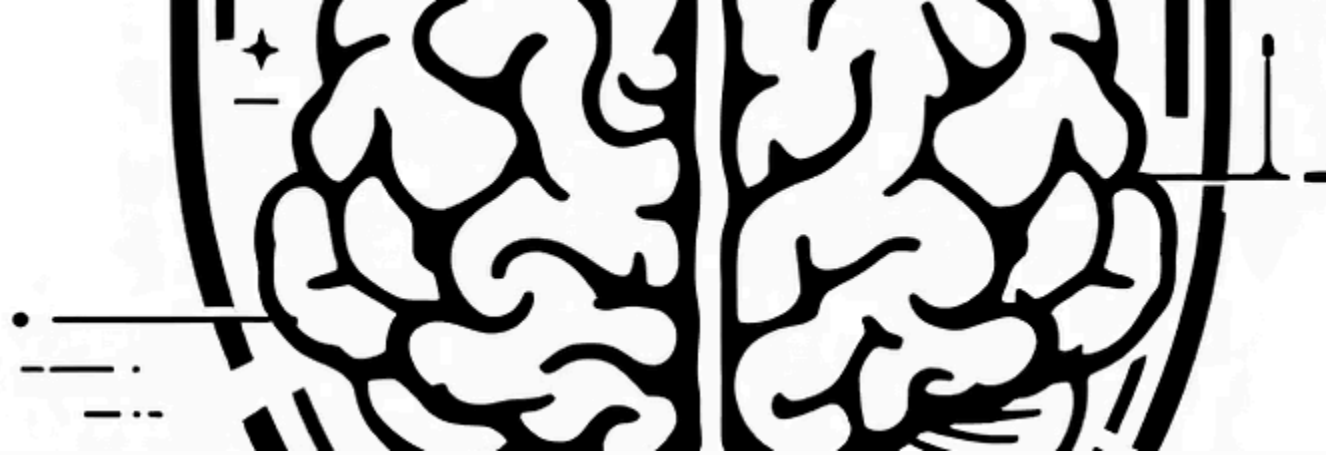


Мінімізуйте контакт власного девайсу із чужими носіями

Нехай учні працюють на комп'ютерах навчального закладу, а файли їм відправляйте через Telegram



"Безпека — не складна. Вона починається з дисципліни, а не з програм."



Критичне мислення як цифровий імунітет

Перед тим як на щось натиснути — поставте собі три запитання:

01

Хто надіслав?

Хто мені це надіслав? Це точно ця людина, а не фейк?

02

Чому мені?

Чому саме до мене звернулися? Чи це моя зона відповідальності?

03

Чому саме таку дію від мене очікують і чи можна її зробити інакше?

Чи можу я відправити цей лист як я це роблю завжди? Чому від мене хочуть отримати дані саме в такий спосіб?

Суть: фішинг і фейки працюють лише там, де люди не сумніваються.

- 🗉 “Клік без роздумів чи через неуважність — це значно більше часу на врегулювання майбутніх проблем, аніж 30 сек уважного читання та заглиблення в суть.”

Як навчити цього учнів



Побутові приклади

Наводьте побутові приклади: "Як мати в різних застосунках різні паролі, але при цьому пам'ятати лише один" звучить краще, ніж "Основи .\"кібербезпеки

Обговорення інцидентів

.Робити короткі обговорення інцидентів

Заохочення

Заохочувати дітей до діалогу, щоб вони самі озвучували проблеми про які вони чули чи .зіштовхувалися раніше



".Коли ти хоча б раз чув про якийсь спосіб атаки, ти вже підсвідомо будеш обережнішим" 

Підсумок: маленькі дії, велика безпека



Відповідальність

Безпека — не про страх, а про відповідальність.



Спільна стійкість

Кожна дрібниця (оновлення, пароль, обережність) — внесок у спільну стійкість.

“Не треба бути айтишником, щоб бути захищеним. Достатньо бути уважним.”

🗉 “Розумну, освідчену людину значно важче ввести в оману, ніж дурня без пам’яті.”