КІБЕРБЕЗПЕКА — ЦЕ КУЛЬТУРА, ЩО ПОЧИНАЄТЬСЯ З ТЕБЕ.

DSPU CYBER SEC

Захищай себе і свою організацію

КІБЕР БЕЗПЕКА ДЛЯ ВСІХ

cybersecurity.dspu.edu.ua

Проєкт реалізується за підтримки

with support from Google.org

virtual routes

Обізнаний — значить захищений!

with support from Google.org

virtual routes

НАВІЩО ЦЕ ПОТРІБНО ВСІМ?

У цифровому світі кожен з нас щодня використовує інтернет, мобільні додатки, онлайн-банкінг, електронну пошту та соціальні мережі. Водночас зростає кількість кіберзагроз — від шкідливих програм і фішингових атак до зламу акаунтів та крадіжки персональних даних.

Кібербезпека — це набір щоденних практик, які допомагають захистити себе, свій пристрій, інформацію і репутацію. У цій брошурі ти знайдеш прості правила, що допоможуть уникнути неприємностей.

СТАТИСТИКА:

95% інцидентів трапляються через людський фактор.

60% кіберзлочинців націлюються на освітній сектор.

50% користувачів використовують однаковий пароль на всіх сайтах.

2 із 3 людей хоча б раз відкривали підозріле посилання.

Україна посідає **2-ге місце** у світовому рейтингу кіберзлочинності.

ТВОЇ ЗВИЧКИ = ТВІЙ ЗАХИСТ

ЩО РОБИТИ У РАЗІ ІНЦИДЕНТУ?

У кіберпросторі трапляються помилки. Це нормально.

Головне — знати, як діяти швидко і правильно, щоб зменшити ризики.

КОЛИ ВАРТО РЕАГУВАТИ?

* Тебе викинуло з акаунту, і не вдається увійти.
* Ти випадково натиснув на фішингове посилання.
* Отримав листа, SMS чи інше повідомлення, після якого щось пішло не так.
* Виявив, що хтось діє від твого імені в месенджерах або соцмережах.

ЩО РОБИТИ — ПО КРОКАХ:

1. Зміни паролі
Особливо для основної пошти, Google-акаунту, банкінгу, навчальних сервісів.
2. Вийди з усіх пристроїв
Це можна зробити у налаштуваннях безпеки акаунта.
3. Увімкни MFA
Якщо раніше не активував — саме час.
4. Повідом адміністратора або IT-фахівця
Якщо це стосується шкільного/університетського чи робочого акаунта.
5. Зроби скріншоти / зафіксуй
Листи, сторінки, повідомлення — докази важливі.
6. Просканує пристрій антивірусом
Бажано повна перевірка.
Можна скористатися онлайн-сканером.

КУДИ ЗВЕРТАТИСЯ У СКЛАДНІЙ СИТУАЦІЇ:

Кіберполіція:
cyberpolice.gov.ua

CERT-UA:
cert.gov.ua

ПОВЕДІНКА ОНЛАЙН

У віртуальному світі, як і в реальному, працюють правила безпеки.

Правильна поведінка в інтернеті — це не просто обережність. Це звичка, яка щодня знижує ризик.

ЧОГО НЕ ВАРТО РОБИТИ:

Публікувати персональні дані (паспорт, адреса, інші документи)
Надсилати скановані документи через месенджери
Встановлювати розширення до браузера “щоб зняти рекламу”
Клікати на “виграші” або “акції” у соцмережах
Вірити незнайомим акаунтам
або проханням про допомогу

5 ЩОДЕННИХ ЗВИЧОК КІБЕРГІГІЄНИ:

* **Оновлюй** систему та програми
* **Використовуй** складні паролі + MFA
* **Перевіряй** джерела інформації
* **Видаляй** зайві додатки/доступи
* **Налаштуй** приватність у соцмережах (хто бачить, хто пише)

ЦИФРОВА ОБЕРЕЖНІСТЬ — ЦЕ:

* Не відповідати на підозрілі повідомлення
* Не переходити за сумнівними посиланнями
* Не завантажувати невідомі файли
* Розповідати про підозрілі ситуації керівництву, батькам або IT-адміну

ФІШИНГ, ВІШИНГ, СМИШИНГ

ЩО ТАКЕ ФІШИНГ?

Це підроблений лист, повідомлення або дзвінок, який змушує тебе натиснути посилання або поділитись паролем. Виглядає як повідомлення від банку, школи чи знайомого сервісу.

ВИДИ:

Фішинг (email): лист із фейковим посиланням типу “Ваша пошта заблокована — увійдіть терміново”.

Смишинг (повідомлення): коротке повідомлення в будь-якому месенджері з підозрілим лінком ("Ваш акаунт буде деактивовано").

Вішинг (дзвінок): телефонна розмова, де тебе просять назвати одноразовий код, нібито для “підтвердження”.

ЯК РОЗПІЗНАТИ ПІДРОБКУ?

* У листі є помилки, незрозумілі посилання.
* Відправник не той, за кого себе видає.
* Тебе лякають (“акаунт заблокують”) або кваплять (“виконай до 10 хв”).
* Посилання веде на незнайомий або схожий, але не той сайт (наприклад, google.com).

НІКОЛИ НЕ РОБИ ЦЬОГО!

Не натискай на підозрілі посилання.
Не передавай коди з SMS навіть “працівнику банку”.
Не вводь паролі, якщо сумніваєшся у сайті.

ЩО РОБИТИ?

* Перевір адресу відправника та посилання.
* Перепитай офіційно (через реальний сайт або додаток).
* Повідом адміністратора або IT-фахівця.
* Видали підозрілий лист/повідомлення.

ПОРАДА:

Якщо сумніваєшся — не клікай. Краще перевірити двічі, ніж втратити все!

ПАРОЛІ ТА MFA

Пароль — це ключ до твоїх акаунтів. Якщо він слабкий, тебе зламають за секунди. Використання багатофакторної автентифікації (MFA) в рази підвищує безпеку.

НАДІЙНИЙ ПАРОЛЬ:

Мінімум 12 символів.

Велика й мала літера, цифра, символ.

Унікальний для кожного сайту.

Уникай шаблонів, дат, імен, слів зі словника.

НЕНАДІЙНІ ПАРОЛІ

```
123456, qwerty, admin,
password, ivan2005,
veronika, school123
```

НАДІЙНІ ПАРОЛІ

```
T4m@rA$2024!
G7k^91w!xZ2p
M4-StudySafe_!
```

MFA:

* Це додатковий рівень захисту, який вимагає два або більше факторів входу
* Код із SMS або мобільного додатку
* Відбиток пальця або Face ID
* Апаратний ключ

ПОРАДИ:

* Використовуй менеджер паролів.
* Не зберігай паролі в нотатках чи на стікерах.
* Не передавай паролі третім особам

ПРИСТРОЇ ПІД ЗАГРОЗОЮ

Твій телефон або комп'ютер — це не просто техніка. Це місце, де зберігається все важливе: листи, банківські додатки, фото, навчальні матеріали.

І все це можна втратити після одного натискання.

ЗАГРОЗИ ПРИСТРОЮ:

* Віруси: шкідливі програми, які крадуть дані або блокують пристрій.
* Трояни: маскуються під корисні застосунки, але передають зловмиснику доступ.
* Шпигунське ПЗ: непомітно стежить за тобою, клавішами, екраном.
* Кейлогери: записують усе, що ти вводиш (паролі, повідомлення).

ЗАХИСТ ПРИСТРОЮ:

* Встановлюй лише перевірені програми з офіційних джерел.
* Увімкни автоматичне оновлення ОС та програм.
* Використовуй антивірус (навіть на телефоні!).
* Захищай екран паролем, PIN або біометрією.
* Видаляй непотрібні застосунки та кеш.
* Перевір дозволи застосунків: чи не слухають вони тебе?

ВІДКРИТІ МЕРЕЖІ В КАФЕ, ГОТЕЛЯХ ЧИ ТРАНСПОРТІ — НЕБЕЗПЕЧНІ. ЗЛОВМИСНИКИ МОЖУТЬ ЛЕГКО ПЕРЕХОПИТИ: ЛОГІНИ І ПАРОЛІ, ПОВІДОМЛЕННЯ І ФАЙЛИ, ДАНІ БАНКІВСЬКИХ ДОДАТКІВ.

ПОРАДИ:

* Не вводь чутливу інформацію через відкриті Wi-Fi.
* Використовуй VPN.
* Зміни пароль до Wi-Fi-роутера вдома (ніколи не залишай "admin").