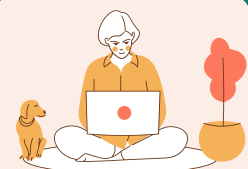


★★★★★

Зберігайте свою особисту інформацію та використовуйте її лише на безпечних сайтах.



Створюйте паролі з комбінаціями букв, цифр і символів.



★★★★★

Слідкуйте за оновленням програмного забезпечення пристрою, щоб він не був уразливим до зловмисного програмного забезпечення.

★★★★★

Деякі веб-сайти можуть викрасти вашу особисту інформацію, попросивши вас пройти тест. Будьте обережні!



Перш ніж купувати щось на веб-сайті, переконайтеся, що це безпечно.

ДОТРИМУЮЧИСЬ ЦИХ ПРАВИЛ, ВИ ЗНАЧНО  
ЗМЕНШИТЕ РИЗИКИ ТА ЗРОБИТЕ СВІЙ  
ДОСВІД В ІНТЕРНЕТІ БЕЗПЕЧНИМ!



«НЕ ДОВІРЯЙ НЕЗНАЙОМЦЯМ  
ОНЛАЙН – ТВОЯ БЕЗПЕКА В ТВОЇХ  
РУКАХ!»



## Золоті правила безпеки в Інтернеті

"Створи, спілкуйся та  
поважай – безпечний  
інтернет обирай!"



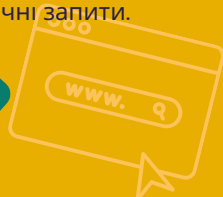


## Паролі та їх безпека

- Використовуйте складні паролі, які містять літери (великі та малі), цифри та спеціальні символи.
- Не використовуйте один пароль для різних акаунтів.
- Змінюйте паролі регулярно (раз на 3–6 місяців).
- Зберігайте паролі в надійному менеджері паролів, а не в нотатках чи файлах на комп'ютері.

## Захист особистої інформації

- Не публікуйте в соцмережах адреси, номери телефонів, номери документів чи іншу конфіденційну інформацію.
- Перевіряйте, кому ви надсилаєте особисту інформацію, особливо якщо це незнайомі люди або незвичні запити.



## Фішинг та підозрілі посилання

- Не відкривайте посилання, отримані від незнайомців чи з огляду на джерела.
- Перевіряйте адреси сайтів перед введенням своїх даних. Сайти повинні починатися з "https://" і мати значок замка.
- Якщо отримали підозрілий лист чи повідомлення, не відповідайте на нього та не відкривайте вкладення.

http://

## Програми та оновлення

- Завантажуйте програми лише з офіційних магазинів (Google Play, App Store) або офіційних сайтів.
- Регулярно оновлюйте операційну систему та програмне забезпечення, щоб усунути вразливість.
- Використовуйте антивірусне програмне забезпечення та регулярно перевіряйте пристрої на наявність вірусів.

## Соціальні мережі

- Перевірте налаштування конфіденційності у своїх акаунтах.
- Обмежуйте доступ до публікацій лише для друзів або обраних осіб.
- Не приймайте запити на дружбу від незнайомих людей без перевірки.



## Електронна пошта

- Не надсилайте через електронну пошту важливу інформацію (наприклад, паролі чи фінансову інформацію).
- Не відкривайте яскраві вкладення чи повідомлення з темами типу «Виграли приз», «Терміново підтвердьте свої дані».

## Фінансова безпека

- Використовуйте двофакторну аутентифікацію для онлайн-банкінгу чи електронних гаманців.
- Не повідомте PIN-коди, паролі чи дані банківських карт працівникам банку.
- Підключайтеся до банківських сайтів лише через захищені мережі (уникайте публічного Wi-Fi).

## Кібербулінг та неприємні ситуації

- Якщо ви стали жертвою кібербулінгу, не відповідайте агресору, робіть скриншоти повідомлень та повідомте адміністрування платформи.
- За потреби Зверніться до поліції чи спеціалізованих служб допомоги.



## Безпечне використання Wi-Fi

- Уникайте введення особистих даних або входу до важливих облікових записів через публічну мережу Wi-Fi.
- Використовуйте VPN для захисту своїх даних під час використання відкритих мереж.

## Вчіться розпізнавати небезпеку

- Регулярно читайте інформацію про нові кіберзагрози та методи їх уникнення.
- Знай базові правила безпеки в Інтернеті: не спілкуватися з незнайомцями, не розголошувати інформацію, додати дорослим про будь-які враження від ситуації.

