

Надійні паролі

✓ Унікальні для кожної електронної скриньки та акаунту.

✓ Щонайменше 12-15 символів з літерами, цифрами та спеціальними символами.

✓ Періодично змінюйте їх.



Двофакторна автентифікація



- ✓ **Налаштуйте двофакторну автентифікацію пошти. Видаліть скриньки та акаунти, якими не користуєтесь.**

Додатки



✓ Перегляньте, яку інформацію можуть зчитувати і до яких папок мають доступ. Завантажуйте їх лише з офіційних «магазинів».

Публічні Wi-Fi



- ✓ Не використовуйте публічні Wi-Fi точки доступу для обміну важливою конфіденційною інформацією. Практикуйте VPN-з'єднання.



Завантаження



- ✓ **Будьте уважними під час завантаження програм, файлів, архівів із маловідомих або сумнівних ресурсів. Одна з ознак безпеки з'єднання на сайті - наявність «замочку» в полі адреси та літер**

https.



Режим Інкогніто



- ✓ **Періодично використовуйте режим Інкогніто в браузері, видаляйте історію пошуку та файли cookies, які допомагають сайтам вас «запам'ятовувати».**



Контент



- ✓ **Будьте уважними до контенту, який ви поширюєте та лайкаєте. Він достовірний? Може не треба додавати геодані до посту?**

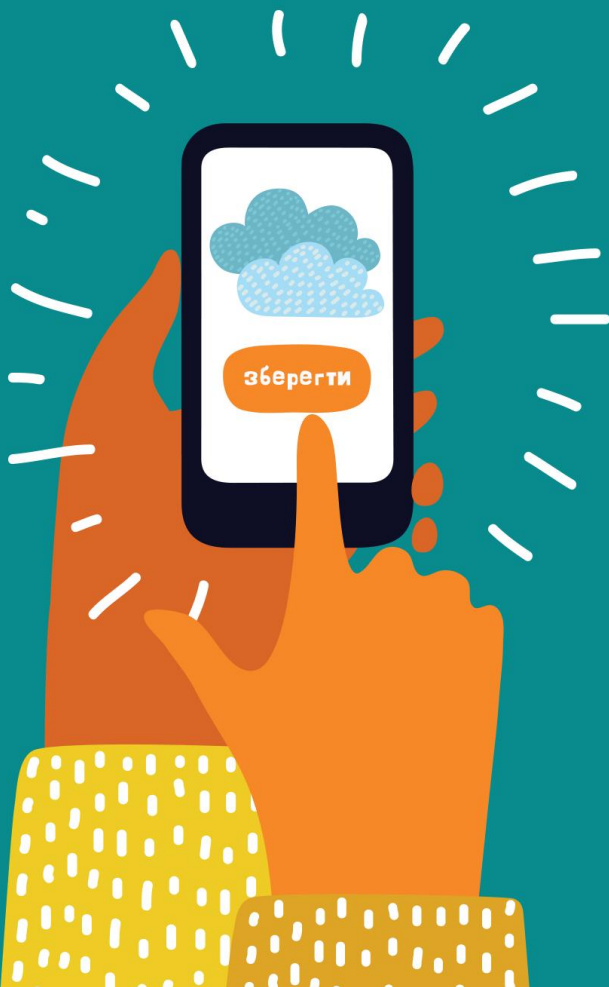


Налаштування конфіденційності



- ✓ **Перегляньте налаштування конфіденційності у Вашому браузері та акаунтах у соцмережах. Переконайтеся, що ви ділитеся лише тими даними, на які дали дозвіл.**

Резервні копії



✓ Створюйте резервні копії важливої інформації та видаляйте програми і додатки, якими не користуєтесь.

Онлайн-покупки



✓ **Здійснюйте
онлайн-покупки
тільки з
безпечних,
перевірених сайтів.**

