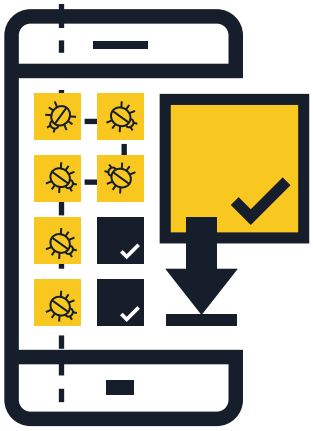
ШКІДЛИВЕ ПЗ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

ЯК ЗАХИСТИТИСЯ: ПОРАДИ Й РЕКОМЕНДАЦІЇ

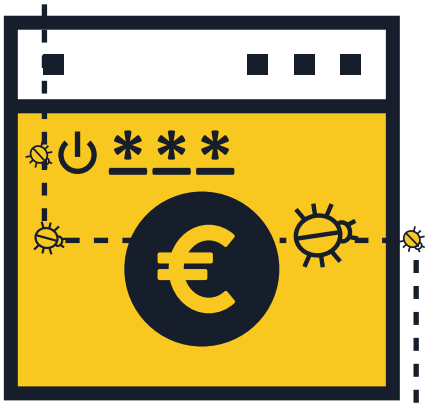
1 Встановлюйте застосунки тільки з перевірених джерел



- **Купуйте в магазинах застосунків, які мають добру репутацію** — Перед завантаженням дізнайтесь якомога більше про застосунок та його видавця. Остерігайтесь посилань, які надходять на електронну пошту та в текстових повідомленнях, - вони можуть спонукати вас до встановлення застосунків від третіх осіб або з невідомих джерел.
- **Поцікавтесь відгуками користувачів та рейтингами,** якщо є така можливість.
- **Прочитайте про дозволи застосунку** — Перевірте, до яких даних має доступ цей застосунок і чи може він передавати інформацію назовні. Якщо умови встановлення викликають підозру або непокоять, не завантажуйте такий застосунок.

2 Не натискайте на посилання чи вкладення в електронних листах чи текстових повідомленнях, надходження яких ви не очікували

- **Не довіряйте посиланням в електронних листах чи текстових повідомленнях, надходження яких ви не очікували** (SMS та MMS) — Негайно видаляйте їх.
- **Ретельно перевіряйте скорочені інтернет-адреси та QR-коди** — вони можуть завести вас на небезпечні веб-сайти або безпосередньо завантажити на ваш пристрій шкідливе ПЗ. Щоб підтвердити дійсність веб-адреси, перш ніж натиснути на неї, скористайтесь інструментами, що дозволяють здійснити попередній перегляд сайта. Перед скануванням QR-коду запустіть зчитувач QR-кодів з попереднім переглядом веб-адреси в коді. Також користуйтеся ПЗ для захисту мобільного пристрою, яке попереджає про сумнівні посилання.



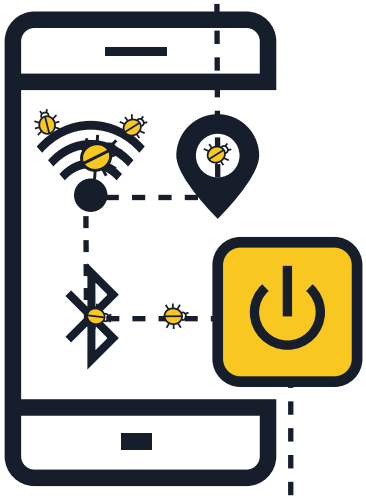
3 Здійснивши платіж, виходьте з облікового запису на сайті

- **Ніколи не зберігайте в мобільному браузері або застосунках імена користувачів та паролі** — Якщо ваш телефон чи планшет загублено або викрадено, до ваших облікових записів зможе увійти будь-хто. Після завершення транзакції вийдіть з облікового запису на сайті, а не просто закрийте браузер.
- **Не користуйтеся банківськими послугами та не купуйте товарів з використанням загальнодоступних мереж Wi-Fi** — Користуйтесь онлайн-банкінгом і здійснюйте операції тільки з використанням відомих та надійних мереж.
- **Ретельно перевіряйте адреси сайтів** — Перш ніж увійти в систему або надіслати конфіденційну інформацію, переконайтеся у правильності веб-адреси. Завантажте офіційний застосунок вашого банку, щоб бути завжди певним в тому, що використовуєте справжній банківський сайт.

4 Регулярно оновлюйте вашу операційну систему та застосунки

- **Завантажуйте оновлення ПЗ для операційної системи вашого мобільного пристрою, щойно їх буде запропоновано** — Найсвіжіші оновлення гарантують не тільки вищу безпеку вашого пристрою, але й вищу продуктивність.

5 Вимикайте Wi-Fi, служби визначення розташування та Bluetooth, коли вони не потрібні



- **Вимикайте Wi-Fi, коли він не використовується** — Кіберзлочинці можуть отримати доступ до вашої інформації, якщо з'єднання не є захищеним. Якщо змога, замість точок доступу використовуйте передачу даних через підключення 3G або 4G. Також ви можете обрати режим віртуальної приватної мережі (VPN) для шифрування ваших даних під час передачі.
- **Не дозволяйте застосункам використовувати без необхідності служби визначення розташування** — Ця інформація може стати відомою іншим та в подальшому використовуватися для надсилання рекламних повідомлень з урахуванням місця вашого перебування.
- **Вимкніть протокол Bluetooth, якщо він не потрібен** — Переконайтеся, що він повністю вимкнений, а не просто перебуває в невидимому режимі. Базові налаштування часто дозволяють іншим підключитися до вашого пристрою, не повідомляючи вас. Зловмисники потенційно здатні копіювати ваші файли, мати доступ до інших пов'язаних пристроїв і навіть отримувати віддалений доступ до вашого телефону, щоб здійснювати дзвінки та надсилати текстові повідомлення на чималі суми.

6 Уникайте надання персональних даних

- **Ніколи не зазначайте особисту інформацію у відповідях** на текстові повідомлення або електронні листи, надіслані нібито вашим банком чи іншою компанією. Натомість зв'яжіться безпосередньо з ними для підтвердження такого запиту.
- **Регулярно переглядайте виписки за вашим мобільним на предмет підозрілих нарахувань** — Якщо ви помітили витрати, яких ви не здійснювали, негайно зверніться до свого постачальника послуг.

7 Не робіть повного зняття обмежень ("джейлбрейк") на вашому пристрої

- "Джейлбрейк" — це процес зняття обмежень безпеки, визначених розробником операційної системи, з отриманням повного доступу до операційної системи та функцій. **"Джейлбрейк" вашого пристрою може значно послабити його безпеку,** розкриваючи прогалини в безпеці, які, можливо, й не були дотепер очевидними.

8 Робіть резервні копії своїх даних

- **Багато смартфонів та планшетів здатні до бездротового резервного копіювання даних** — Дізнайтеся про варіанти резервного копіювання залежно від операційної системи вашого пристрою. Створивши резервну копію для вашого смартфона або планшета, ви можете легко відновити свої персональні дані, якщо пристрій загублено, викрадено або пошкоджено.

9 Встановіть застосунок мобільної безпеки

- Будь-які операційні системи вразливі до зараження. Якщо є така можливість, **використовуйте рішення для мобільної безпеки** яке виявляє та блокує шкідливе ПЗ, шпигунські програми та шкідливі застосунки, а також містить інші функції конфіденційності та захисту від викрадення.