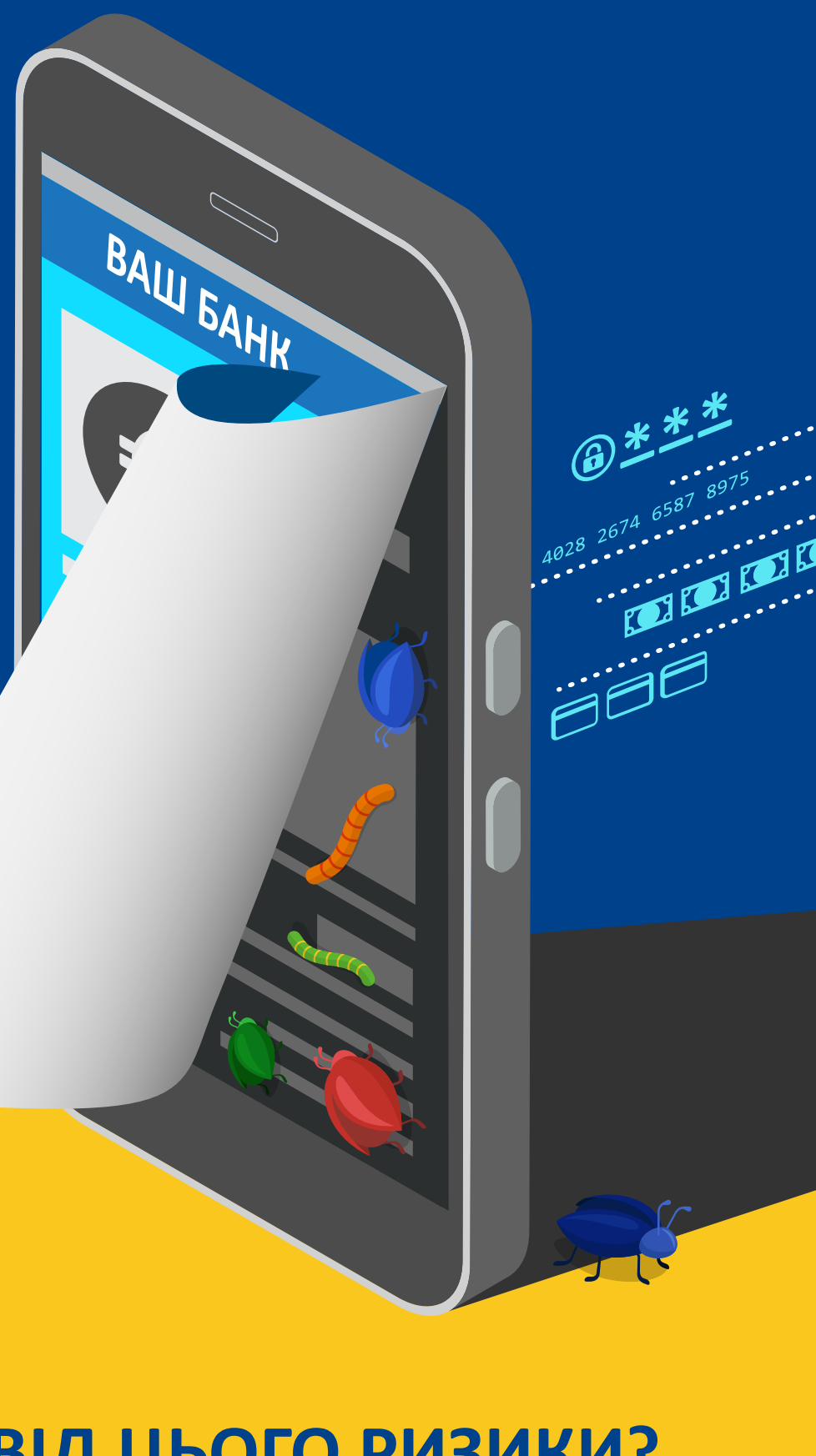
ШКІДЛИВЕ ПЗ ДЛЯ МОБІЛЬНОГО БАНКІНГУ

ШКІДЛИВЕ ПЗ МОЖЕ ДОРОГО ВАМ КОШТУВАТИ

Шкідливе ПЗ для мобільного банкінгу призначене для викрадення фінансової інформації, що зберігається у вашому мобільному пристрої.



ЯК ВОНО ПОШИРЮЄТЬСЯ?

При відвідуванні шкідливих веб-сайтів

При завантаженні шкідливих застосунків

Засобами фішингу

ЯКІ ВІД ЦЬОГО РИЗИКИ?

Збір інформації, яка засвідчує вашу особу

Несанкціоноване зняття грошей

ЩО З ЦИМ РОБИТИ?

https://

Завантажте офіційний застосунок вашого банку і щоразу переконуйтеся, що ви на справжньому сайті вашого банка.

Уникайте автоматичного входу в обліковий запис на банківському сайті чи в застосунку.

Нікому не передавайте і не розголошуйте номер вашої банківської картки чи пароль.

Якщо є така можливість, встановіть застосунок мобільної безпеки, який сповістить вас про будь-яку підозрілу діяльність.

Якщо ви загубили ваш мобільний телефон або змінили номер, повідомте про це свій банк для оновлення інформації.

Не передавайте будь-яку інформацію щодо вашого рахунку текстовими повідомленнями або електронною поштою.

При підключенні до мобільного сайту чи застосунку вашого банку завжди користуйтеся захищеною мережею Wi-Fi. Ніколи не робіть цього за допомогою відкритої мережі Wi-Fi!

Періодично перевіряйте свої фінансові виписки.

EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware