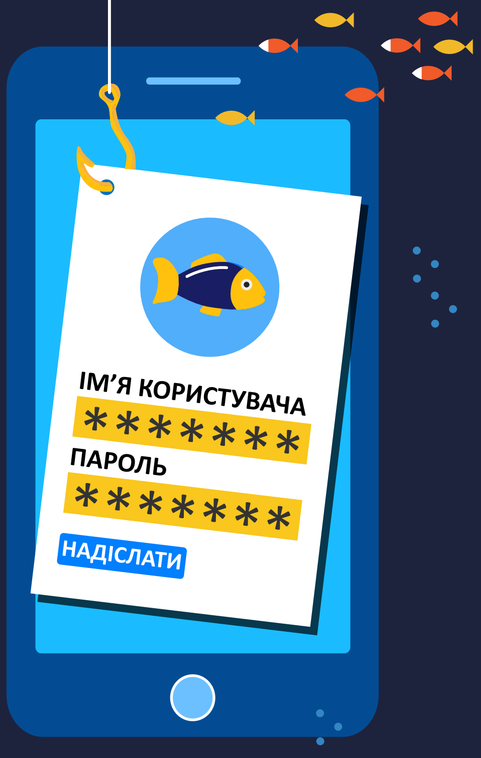
ВЕБ-ЗАГРОЗИ

ПЕРШ НІЖ ЩОСЬ НАТИСНУТИ, ДВІЧІ ПОДУМАЙТЕ



Ви можете втратити свої гроші, персональну інформацію і навіть збережені вами дані, в разі якщо пристрій перестане працювати. Не впіймайтесь на гачок!

ЯК ТАКЕ МОЖЛИВО?

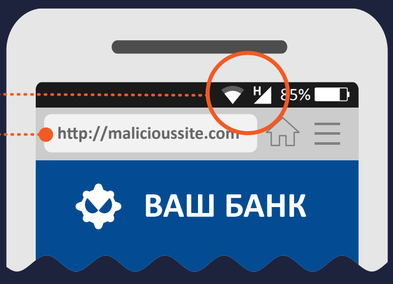
ФІШИНГОВІ АТАКИ: Розповсюджуються через електронну пошту, текстові повідомлення, соціальні медіа та виманюють персональну інформацію, удаючи з себе звернення від легітимних компаній, яким користувачі довіряють.

ПЕРЕГЛЯД САЙТІВ: Ваш мобільний пристрій може інфікуватися просто через відвідини небезпечного сайту.

ЗАВАНТАЖЕННЯ ФАЙЛІВ: Шкідливі посилання та вкладення можуть міститися безпосередньо в електронному листі.

ЧОМУ ЦЕ ТАК ДІЄВО?

Мобільні пристрої **ПОСТІЙНО ПІДКЛЮЧЕНІ** до мережі Інтернет.



ЗМЕНШЕНИЙ РОЗМІР ЕКРАНУ ПРИСТРОЮ — це загальний обмежувальний чинник. Браузери для мобільних пристроїв показують інтернет-адреси в обмеженому екранному просторі, через що важко перевірити справжність домену.

БЕЗЗАСТЕРЕЖНА ВІРА КОРИСТУВАЧІВ у приватність мобільного пристрою.

ЩО З ЦИМ РОБИТИ?

Ставтеся з підозрою до SMS та дзвінків від компаній, які просять вас надати персональну інформацію. Ви можете перевірити повідомлення чи дзвінок на справжність, зателефонувавши безпосередньо за офіційним номером компанії.

https://

Переглядаючи веб-сторінки зі свого мобільного пристрою, переконайтеся в тому, що ваше з'єднання захищене за протоколом HTTPS. Ви завжди можете перевірити, чи це так, подивившись на початок інтернет-адреси.

Ніколи не натискайте на посилання чи вкладення в електронних листах чи SMS, на отримання яких ви не очікували. Негайно видаляйте такі повідомлення.

^BE:%}
W@RY
*)Z#$=

Остерігайтесь відвідання сайтів з поганою граматикою, орфографічними помилками чи низькою роздільною здатністю.

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

EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware