ПАМ’ЯТКА КЛІЄНТУ

Idea Bank

#Cashless

ВІШИНГ
телефонне
шахрайство

ЗА ЖОДНИХ УМОВ НЕ РОЗКРИВАЙТЕ ЦІ РЕКВІЗИТИ СВОЇХ КАРТОК!

Вам телефонують і під різними приводами випитують дані платіжної картки, банківські sms-паролі або змушують зняти ліміти?

Припиніть розмову, бо втратите гроші!

ШАХРАЙ МОЖЕ ПРЕДСТАВИТИСЯ ЯК:

- СПІВРОБІТНИК БАНКУ
- ВОЛОНТЕР АБО БЛАГОДІЙНИК
- СПІВРОБІТНИК ПОЛІЦІЇ
- СПІВРОБІТНИК СБУ
- СПІВРОБІТНИК ПЕНСІЙНОГО ФОНДУ АБО ПОДАТКОВОЇ
- ПОКУПЕЦЬ ВАШОГО ТОВАРУ

ЯК РОЗПІЗНАТИ?

Телефонують та запитують реквізити картки
Термін дії, тризначний код зі звороту картки або банківський SMS пароль запитують лише шахраї!

Легкі гроші
Обіцяють гроші, на які ви не очікували (несподіваний виграш у лотерею, перерахунок пенсії тощо).

Наполегливість та поспіх
Наполегливо переконують зробити те, що ви ще хвилину тому робити не збирались.

Телефонують та спрямовують Вас до банкомату чи терміналу
Аргументи та приводи можуть бути різними, а результат один — переказ Ваших грошей на рахунок шахрая.

Тривожна тема
Лякають тим, що ваша картка заблокована, злочинці зламали ваш рахунок.

Запит всіх реквізитів
Для будь-яких зарахувань на вашу картку достатньо її номеру, — жодних інших даних не потрібно.

ЯК ЗАХИСТИТИСЯ?

Давати тільки номер картки
Для отримання будь-якого переказу на вашу картку — достатньо надати покупцеві лише номер картки.

Не розголошувати ці реквізити:
термін дії картки,
тризначний код безпеки з її звороту
та банківський sms-пароль.

Припинити розмову
Якщо телефонують з приводу блокування вашої картки, — припинити розмову і самостійно зателефонувати до банку.

Не виконувати сторонні команди
Не виконувати в банкоматі чи платіжному терміналі команди, які надають телефоном.

ЯК ДІЯТИ?

ЯКЩО ВИ ПІДДАЛИСЯ ШАХРАЙСЬКІЙ ПРОВОКАЦІЇ ТА ПОВІДОМИЛИ ШАХРАЯМ РЕКВІЗИТИ СВОЄЇ КАРТКИ, ПОТРІБНО:

Негайно заблокувати вашу картку

Звернутися із заявою до Кіберполіції онлайн www.cybercrime.gov.ua

#Cashless

БАНКОМАТНЕ
ШАХРАЙСТВО
СКІМІНГ

ЗАХИСТИ СВІЙ ПІН-КОД!

Ваш ПІН-код можуть вкрасти
під час зняття готівки в банкоматі
через встановлені сторонні пристрої.

Прикривай ПІН-код під час введення!

ЯК РОЗПІЗНАТИ?

Незвичний вигляд банкомату
Є відмінності у вигляді банкомату порівняно з екранною заставкою.

Картка входить і виходить з зусиллям
Також може бути встановлено замасковану мікрокамеру.

ЯК ЗАХИСТИТИСЯ?

Прикривати ПІН-код під час введення
При введенні ПІН-коду завжди прикривайте ПІН-клавіатуру рукою або портмоне!

Періодично змінювати ПІН-код картки
Робіть це регулярно, наприклад, один раз на 3 місяці.

Порівняти банкомат з його екранною заставкою
Банкомат має виглядати так само як і зображення на його екранній заставці.

Встановити індивідуальні ліміти на зняття готівки
Це можна зробити онлайн, за телефоном або у відділенні вашого банку.

ЯК ДІЯТИ?

ЯКЩО ВИ ЗРОЗУМІЛИ, ЩО СКОРИСТАЛИСЯ БАНКОМАТОМ ЗІ СТОРОННІМ ПРИСТРОЄМ, ПОТРІБНО:

Негайно повідомити банк за телефоном, що вказаний на банкоматі чи зворотньому боці вашої картки

Негайно змінити ПІН-код або заблокувати вашу картку

Захисти свої гроші!

#Cashless

БАНКОМАТНЕ
ШАХРАЙСТВО
кеш-трепінг

ОПЕРАЦІЮ ЗАВЕРШЕНО, А ГРОШІ ДЕ?

Ваші гроші можуть вкрасти
під час зняття готівки в банкоматі
через встановлені сторонні пристрої.

Не відходьте від банкомату!

ЯК РОЗПІЗНАТИ?

Операцію завершено, а гроші не з’явилися

Ви почули, як банкомат відрахував готівку, але гроші не з’явилися в отворі.

Отвір для отримання готівки закритий

Виходу готівки перешкоджає планка або липка стрічка.

ЯК ЗАХИСТИТИСЯ?

Не відходити від банкомату

Якщо операцію завершено, а гроші в отворі не з’явилися — залишайтеся біля банкомату.

Перевірити отвір для отримання готівки

На нього може бути встановлено «накладку» з двостороннім скотчем для захоплення готівки.

ЯК ДІЯТИ?

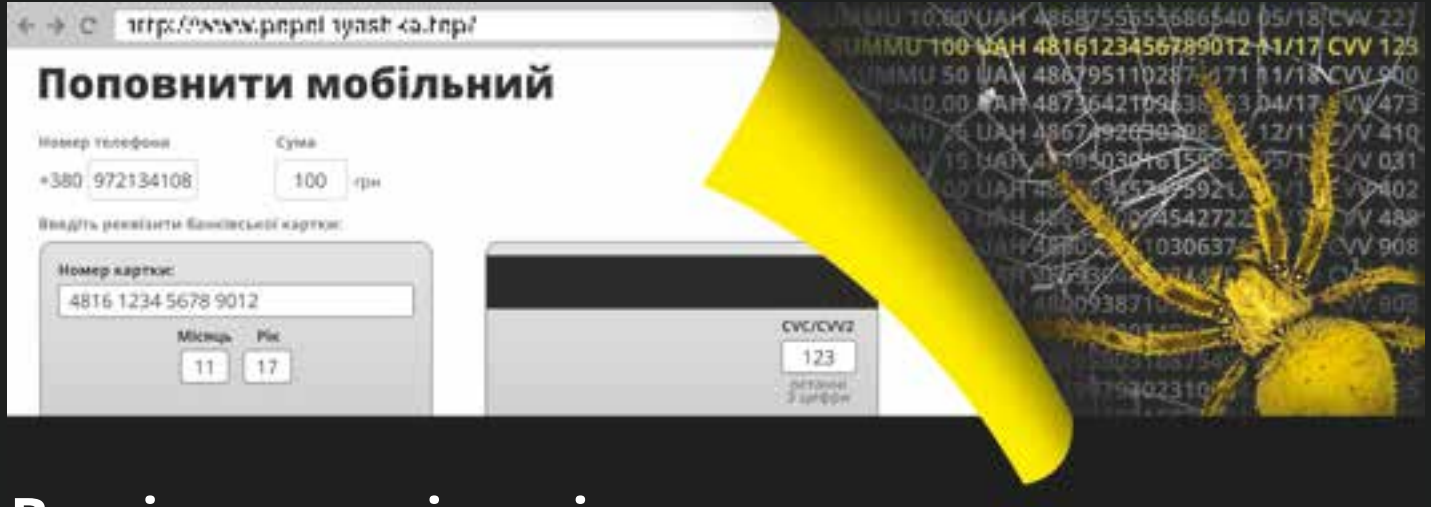
Негайно повідомити банк за телефоном, що вказаний на банкоматі чи зворотньому боці вашої картки

Збережи свої гроші!

#Cashless

ФІШИНГ
шахрайські
платіжні сайти

ПЕРЕВІР САЙТ, ЯКОМУ РОЗКРИВАЄШ КАРТКОВІ ДАНІ!



Ваші карткові дані можуть вкрасти на шахрайських сайтах, що маскуються під сайти платіжних сервісів та банків.

ema.com.ua/blacklist
БАЗА ШАХРАЙСЬКИХ САЙТІВ ТА ЇХНІ ОЗНАКИ

ШАХРАЙСЬКІ САЙТИ МОЖУТЬ МАСКУВАТИСЯ ПІД:

- **САЙТИ ПЕРЕКАЗУ З КАРТКИ НА КАРТКУ**
- **САЙТИ ПОПОВНЕННЯ МОБІЛЬНОГО ТЕЛЕФОНУ**
- **САЙТИ ОНЛАЙН-КРЕДИТУВАННЯ НА КАРТКУ**
- **САЙТИ З ПРОДАЖУ АВІА-КВИТКІВ**

ЯК РОЗПІЗНАТИ?

Відсутність репутації
Відсутність інформації про сайт в Інтернет або наявність негативних відгуків.

Новий сайт
Сайт було створено недавно та зареєстровано лише на 1 рік.

Доменна зона — не .UA
Вітчизняний платіжний або банківський сайт зареєстровано не на домені національного рівня .UA

Наприклад:
✓ **ipay.ua** ✗ **ipay.co.ua**

Відсутність маскування введених реквізитів
Легітимні сайти маскують введення карткових реквізитів (наприклад, зірочками) або використовують віртуальну клавіатуру, а шахрайські — ні.

ЯК ЗАХИСТИТИСЯ?

Тільки відомі платіжні сайти
Користуйтесь тільки відомими та перевіреними платіжними сайтами.

Перевірка віку та терміну реєстрації сайта
В адресному рядку браузера введіть: **whois.com/whois/назва сайту** і зверніть увагу на дати **created** і **expires**.

Перевірка репутації сайта
Перед тим як ввести свої карткові дані на сайті, перевірте відгуки про нього в Інтернет. Особливо пильно перевіряйте сайти з поміткою «Реклама».

ema.com.ua/blacklist
Перевірте сайт, послугами якого збираєтесь скористатися, на наявність в списку шахрайських сайтів.

ЯК ДІЯТИ?

ЯКЩО ВИ ЗРОЗУМІЛИ, ЩО СКОРИСТАЛИСЯ ШАХРАЙСЬКИМ САЙТОМ, ПОТРІБНО:

Негайно заблокувати вашу картку

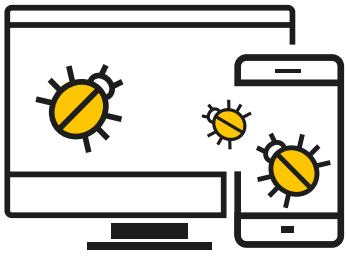
Звернутися із заявою до Кіберполіції онлайн www.cybercrime.gov.ua

Попередити про небезпеку інших ema.com.ua/report

Збережи свої гроші!

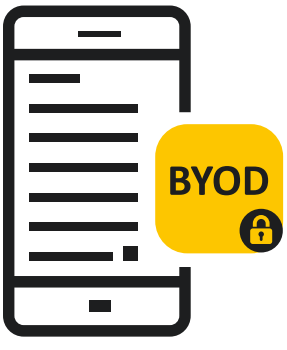
ШКІДЛИВЕ ПЗ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

ПОРАДИ Й РЕКОМЕНДАЦІЇ ДЛЯ ПІДПРИЄМСТВ



1 Інформуйте свій персонал щодо ризиків мобільних пристроїв

- Експлуатація мобільних пристроїв розмиває межу між корпоративним та особистим використанням. Підприємства можуть серйозно постраждати від атаки, первісно спрямованої на особистий мобільний пристрій. Мобільний пристрій — це комп'ютер, тому захищати його потрібно як комп'ютер.

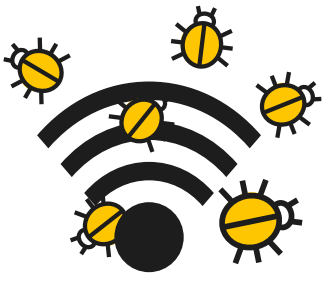


2 Впровадження корпоративної політики для використання власних пристроїв (BYOD)

- Працівники, які використовують свої мобільні пристрої для доступу до інформації та систем підприємства (навіть якщо це тільки електронна пошта, календар чи бази даних контактів), повинні дотримуватися політики компанії. Ретельно обирайте технічні рішення для керування мобільними пристроями та їх захисту, а також для заохочування вашого персоналу до обачності.

3 Зробіть політику безпеки щодо мобільних пристроїв частиною вашої загальної системи безпеки

- Якщо пристрій не відповідає політиці безпеки, він не повинен отримувати дозвіл на підключення до корпоративної мережі і доступ до корпоративних даних. Компанії мають впроваджувати власні рішення для управління мобільними пристроями (Mobile Device Management, MDM) або управляння корпоративними мобільними рішеннями (Enterprise Mobility Management, EMM).
- На додачу, критично важливо встановити рішення для захисту від мобільних загроз. Це забезпечить підвищену видимість та розуміння рівня загроз для застосунків, мережі та операційної системи.



4 Остерігайтесь використовувати для доступу до корпоративних даних загальнодоступні мережі Wi-Fi

- Загалом, загальнодоступні мережі Wi-Fi не є безпечними. Якщо працівник здійснює доступ до корпоративних даних за допомогою безкоштовного підключення Wi-Fi в аеропорту або кав’ярні, ці дані можуть бути доступними і для зловмисників. Компаніям рекомендується в цьому напрямку розробляти політику “раціонального використання”.

5 Регулярно оновлюйте операційні системи та застосунки

- Порадьте своїм працівникам завантажувати оновлення програмного забезпечення для операційної системи їх мобільних пристроїв, щойно такі буде запропоновано. Вивчайте політику операторів мобільного зв'язку й виробників мобільних телефонів щодо оновлень, - особливо це є актуальним для платформи Android. Найсвіжіші оновлення гарантують не тільки вищу безпеку вашого пристрою, але й вищу продуктивність.

6 Встановлюйте застосунки тільки з перевірених джерел

- На тих мобільних пристроях, що підключаються до корпоративної мережі, компанії повинні дозволяти встановлення застосунків тільки з офіційних джерел. Як варіант, розгляньте можливість створення корпоративного магазину застосунків, де кінцеві користувачі матимуть доступ до застосунків, погоджених компанією, зможуть їх завантажувати та встановлювати. Зверніться до свого постачальника рішень безпеки за порадою щодо налаштування або створіть власне рішення.

7 Запобігання повному зняттю обмежень (“джейлбрейку”)

- “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. В корпоративному середовищі не слід дозволяти використання пристроїв з розблокованим обліковим записом суперкористувача.

8 Розгляньте варіанти хмарних сховищ даних

- Користувачі мобільних пристроїв часто хочуть отримувати доступ до важливих документів не тільки через свої робочі ПК, а й зі своїх власних телефонів чи планшетів за межами офісу. Компаніям слід оцінити можливість створення безпечного хмарного сховища та служб синхронізації файлів для безпечного задоволення таких потреб.

9 Заохочуйте свій персонал до встановлення застосунків мобільної безпеки

- Будь-які операційні системи вразливі до зараження. Якщо є така можливість, забезпечте, щоб вони використовували 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.

EUROPOL EC3 European Cybercrime Centre

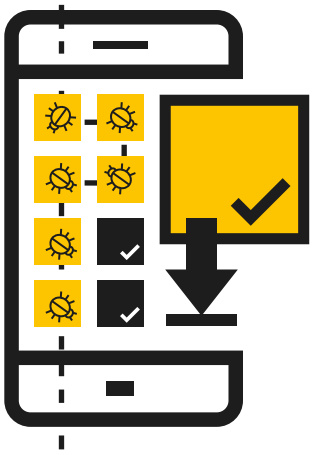
EMA

#MobileMalware

ШКІДЛИВЕ ПЗ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

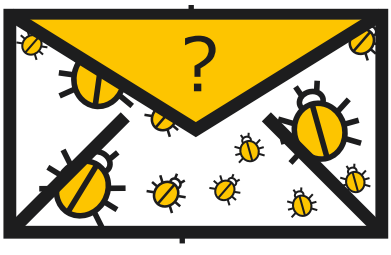
ЯК ЗАХИСТИТИСЯ: ПОРАДИ Й РЕКОМЕНДАЦІЇ

1 Встановлюйте застосунки тільки з перевірених джерел

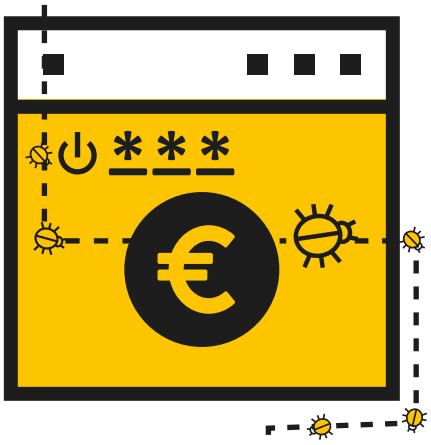


- **Купуйте в магазинах застосунків, які мають добру репутацію** — Перед завантаженням дізнайтесь якомога більше про застосунок та його видавця. Остерігайтесь посилань, які надходять на електронну пошту та в текстових повідомленнях, - вони можуть спонукати вас до встановлення застосунків від третіх осіб 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.



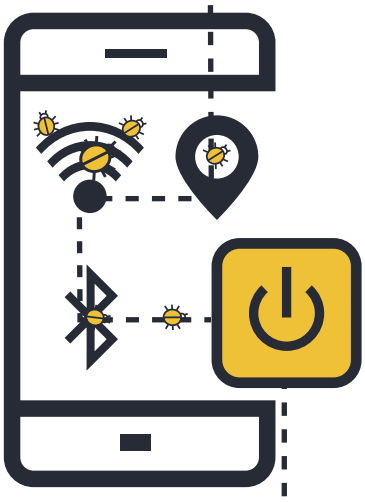
3 Здійснивши платіж, виходьте з облікового запису на сайті

- **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.

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

ШКІДЛИВЕ ПЗ ДЛЯ МОБІЛЬНОГО БАНКІНГУ

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.

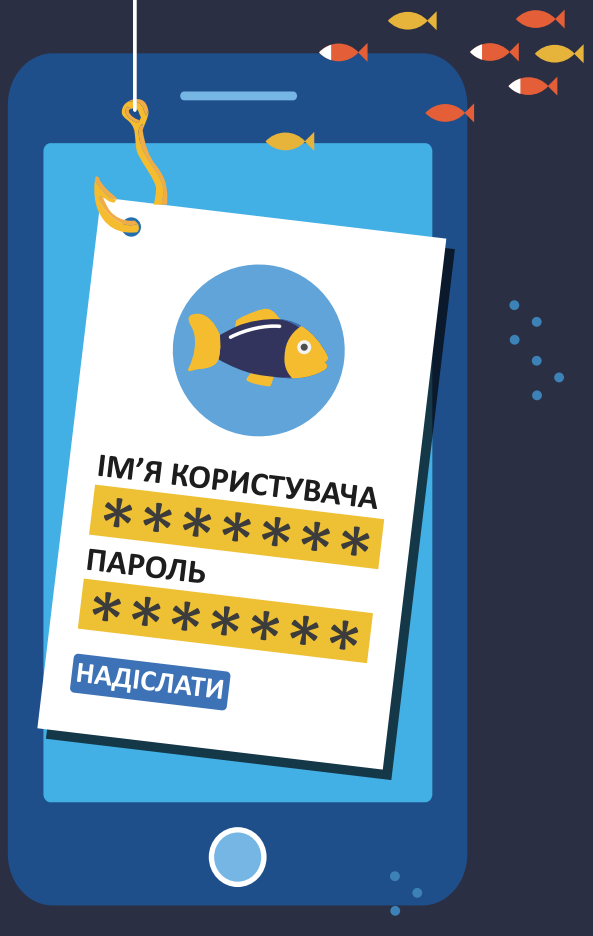
EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware

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?

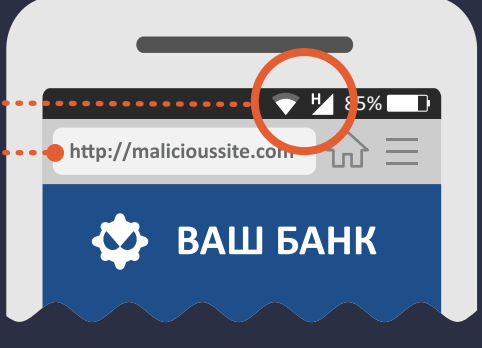
ФІШИНГОВІ АТАКИ: Розповсюджуються через електронну пошту, текстові повідомлення, соціальні медіа та виманюють персональну інформацію, удаючи з себе звернення від легітимних компаній, яким користувачі довіряють.

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.

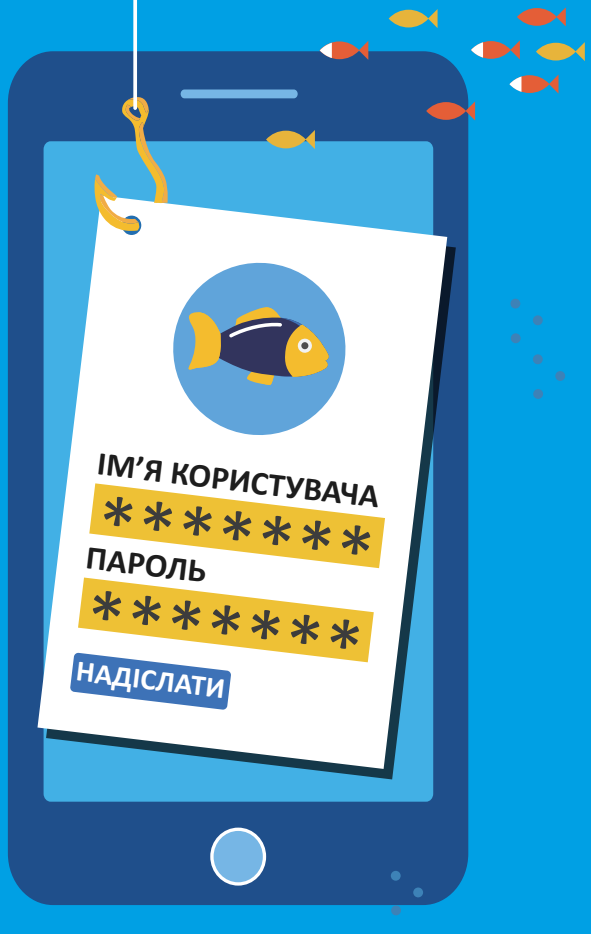


ЗМЕНШЕНИЙ РОЗМІР ЕКРАНУ ПРИСТРОЮ — це загальний обмежувальний чинник. Браузери для мобільних пристроїв показують інтернет-адреси в обмеженому екранному просторі, через що важко перевірити справжність домену.

БЕЗЗАСТЕРЕЖНА ВІРА КОРИСТУВАЧІВ у приватність мобільного пристрою.

ВЕБ-ЗАГРОЗИ

ПЕРШ НІЖ ЩОСЬ НАТИСНУТИ, ДВІЧІ ПОДУМАЙТЕ



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

МОБІЛЬНЕ ПЗ, ЩО
ВИМАГАЄ ВИКУП

СКАЖИ “ПРОЩАВАЙ” СВОЇМ ОСОБИСТИМ ФАЙЛАМ

Мобільне ПЗ, що розроблене з метою вимагання, утримує ваш мобільний пристрій та дані в заручниках, вимагаючи певну суму грошей. Цей тип шкідливого ПЗ блокує екран вашого пристрою або ж не дозволяє користуватися певними файлами та функціями.

ЯК ВОНО ПОШИРЮЄТЬСЯ?

Під час відвідування скомпрометованих веб-сайтів.

Під час завантаження фальшивих версій справжніх застосунків.

Під час відкриття шкідливих посилань або вкладень, що містяться в фішингових електронних листах.

ЯКІ ВІД ЦЬОГО РИЗИКИ?

Можливо, вам доведеться скинути свій пристрій до заводських налаштувань, втративши всі дані.

Нападник може отримати повний доступ до вашого пристрою і поділитися вашими даними з третіми особами.

МОБІЛЬНЕ ПЗ, ЩО
ВИМАГАЄ ВИКУП

ЩО З ЦИМ РОБИТИ?

Періодично робіть резервні копії своїх даних та оновлюйте всі свої застосунки й операційну систему.

Намагайтесь не купувати в магазинах застосунків, що належать третім особам

Якщо є така можливість, встановіть застосунок мобільної безпеки, який сповістить вас про компрометацію вашого пристрою.

Остерігайтесь підозрілих електронних листів та веб-сайтів чи надто привабливих пропозицій.

Нікому не надавайте прав адміністратора вашого пристрою.

Не платіть викуп. Заплативши, ви фінансуватимете злочинність і заохочуватимете злочинців до нових незаконних дій.

EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware

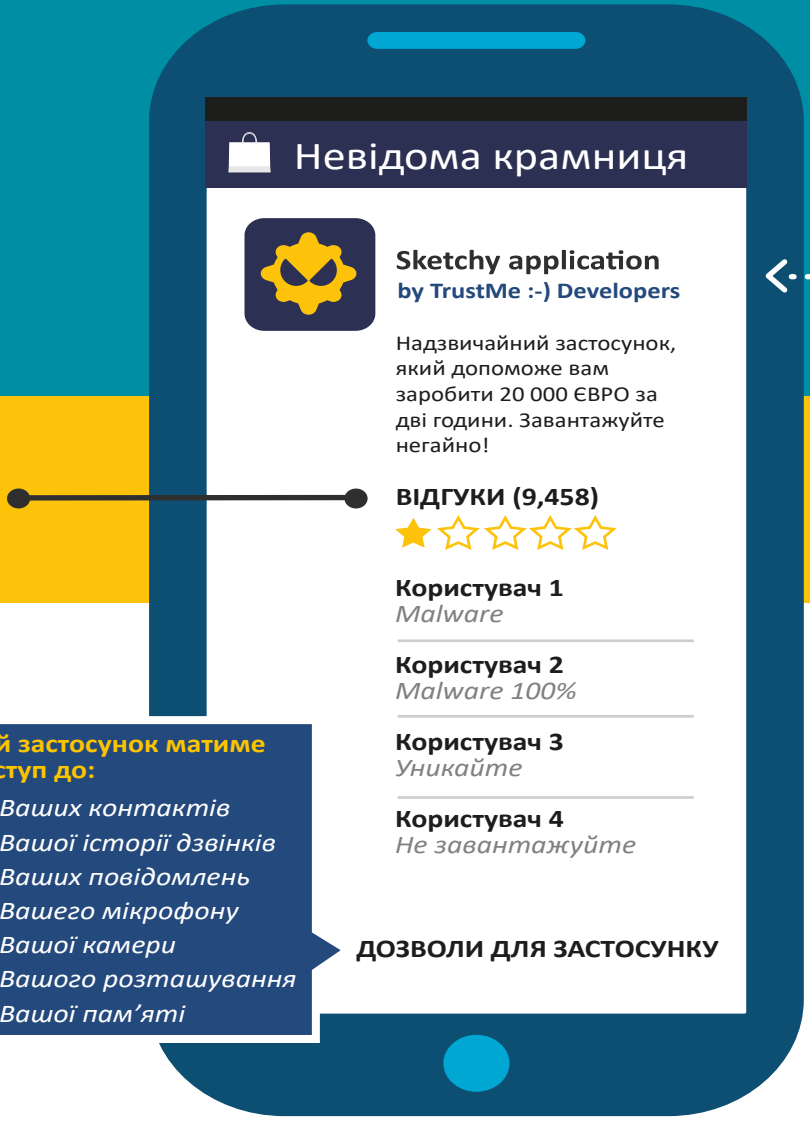
ЗАСТОСУНКИ

ПРОСТО ГРА?

Встановлюйте застосунки лише з офіційних магазинів застосунків.

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



ПРОЧИТАЙТЕ ПРО ДОЗВОЛИ ЗАСТОСУНКУ

Перевірте, до яких даних має доступ цей застосунок і чи може він передавати інформацію назовні. Чи потрібні застосунку всі ті дозволи? Якщо ні, — не завантажуйте його.

ВСТАНОВІТЬ ЗАСТОСУНОК МОБІЛЬНОЇ БЕЗПЕКИ

Він перевірить всі наявні застосунки на вашому пристрої, а також кожен новий застосунок, та повідомить вас в разі виявлення шкідливої програми.

EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware

Інформацію підготовлено за підтримки асоціації «ЄМА» та Європейськго поліцейського управління (Європол)

ПАТ «Ідея Банк”

Адреса для кореспонденції:
79008, Україна, м. Львів,
вул. Валова, 11

п/р 35195904599 в ПАТ «Ідея Банк»
МФО 336310
ЄДРПОУ 19390819
ІПН № 193908109156,
Свідоцтво платника ПДВ № 200034226

www.ideabank.ua