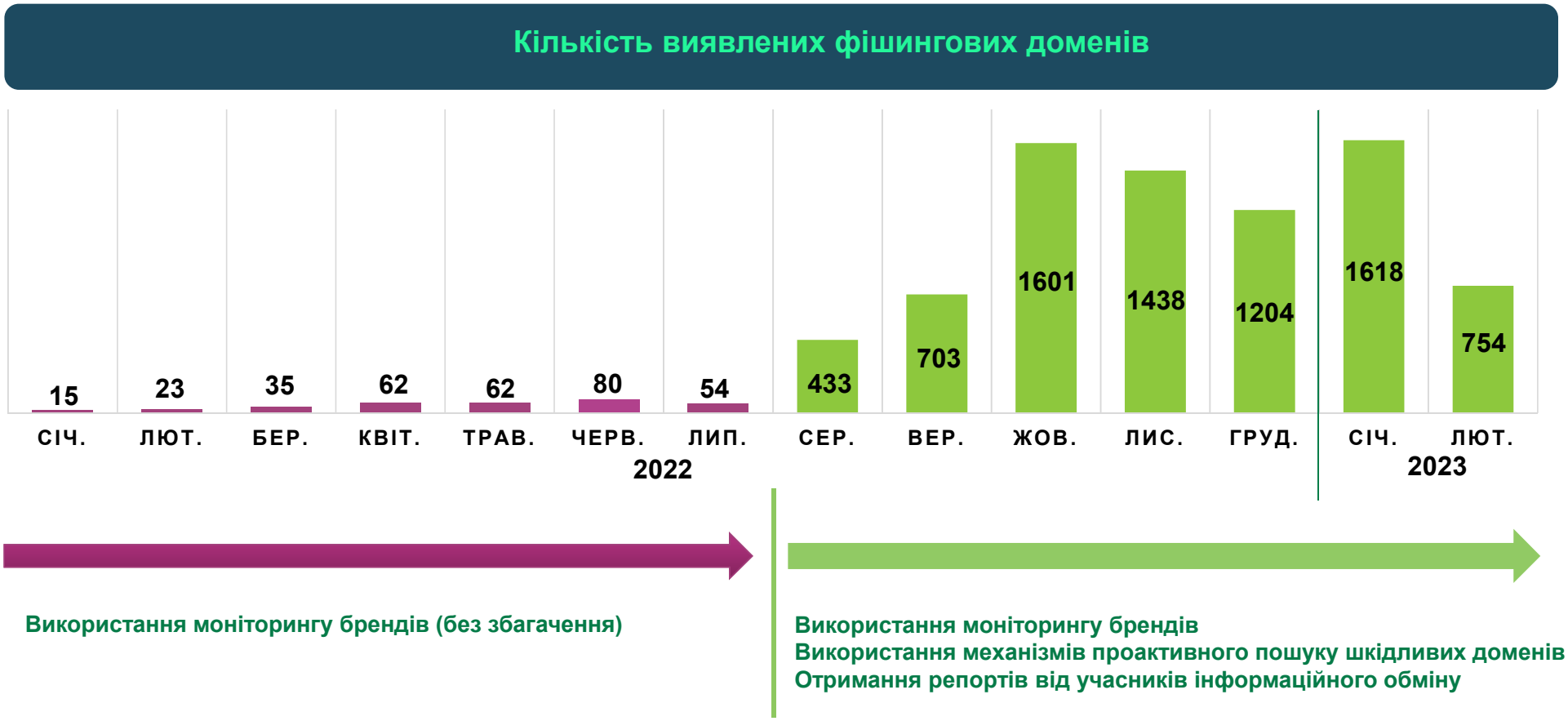
National Bank of Ukraine

Протидія кібершахрайству у фінансовій сфері

Київ, 2023

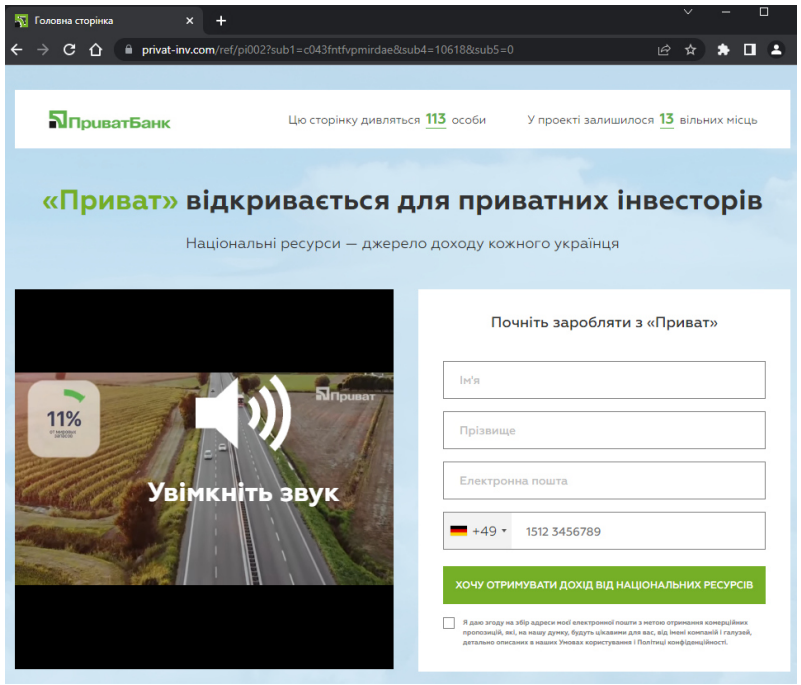
Статистична інформація щодо виявлених фішингових доменів пов'язаних із фінансовим шахрайством



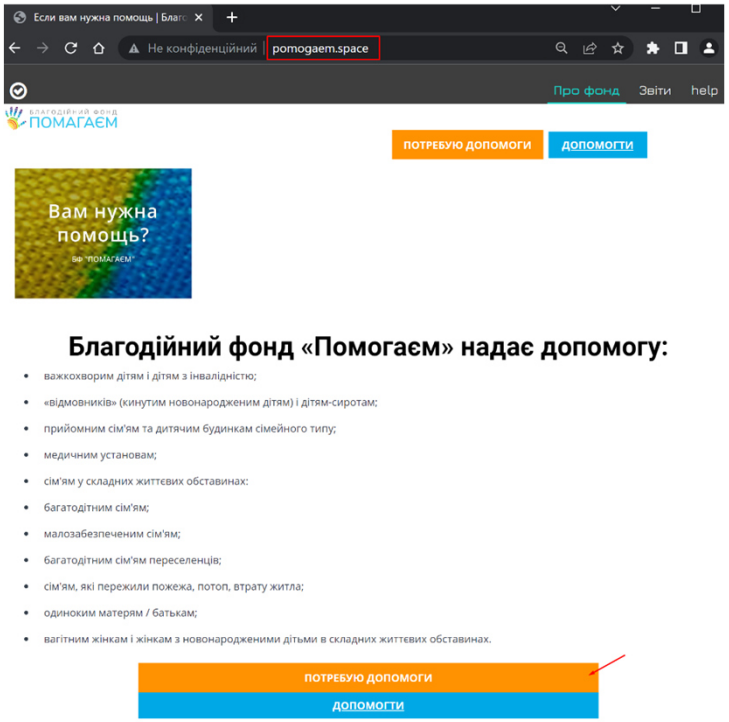
* статистичні дані станом на 15.02.2023

Приклади фішингових сайтів

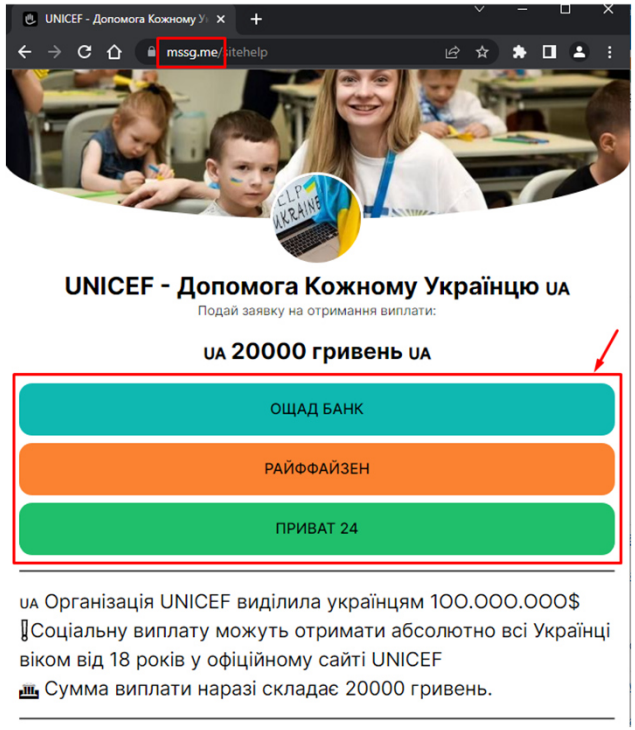
Приват інвест



Благодійний фонд



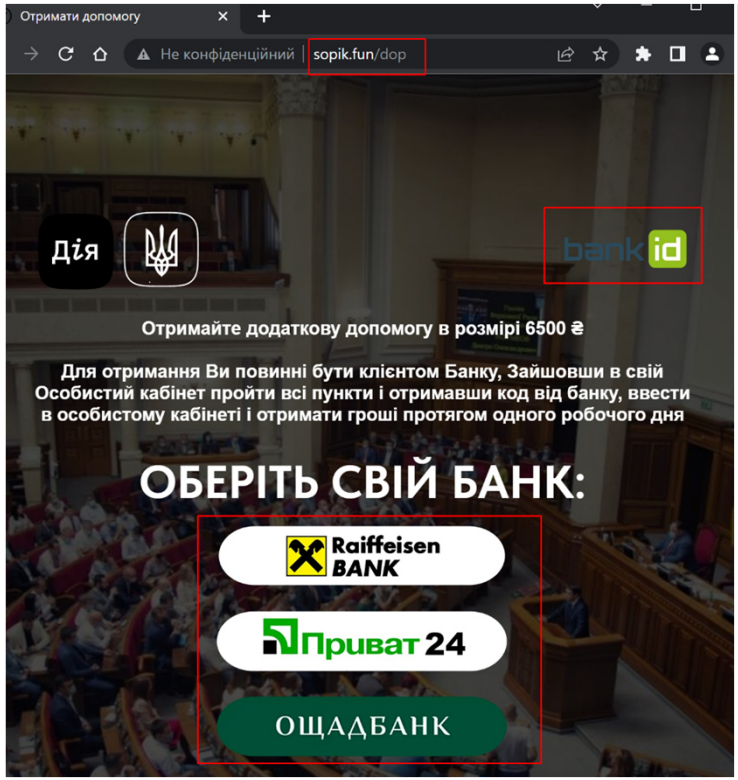
Міжнародна допомога UNICEF



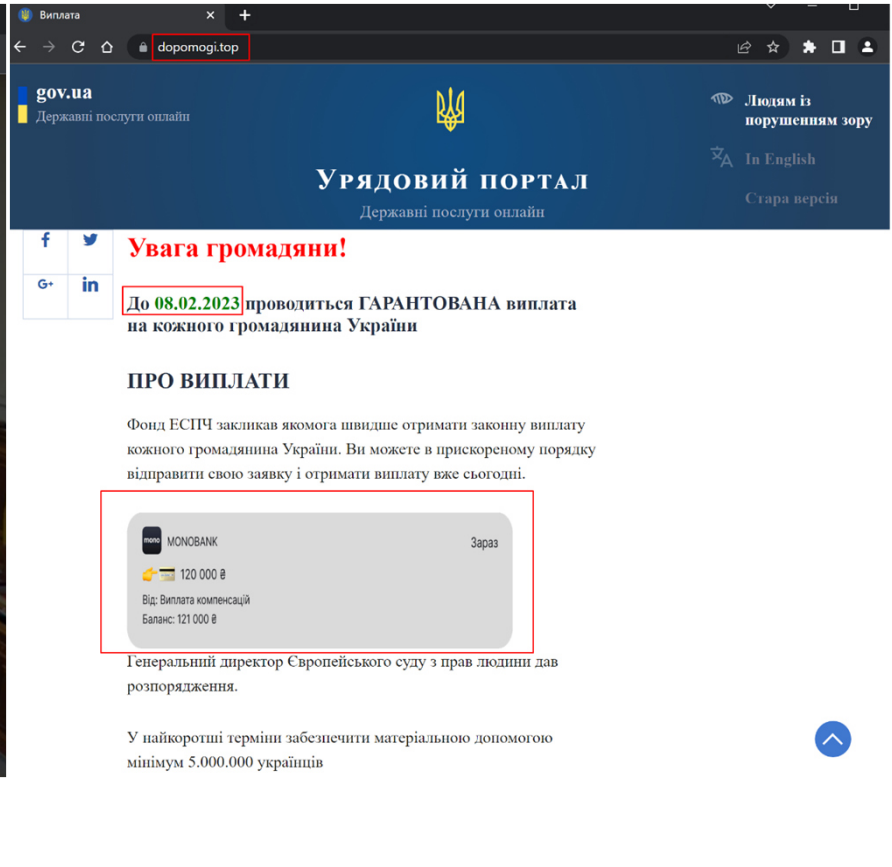
Приклади фішингових сайтів

ЄДопомога

Портал Дія

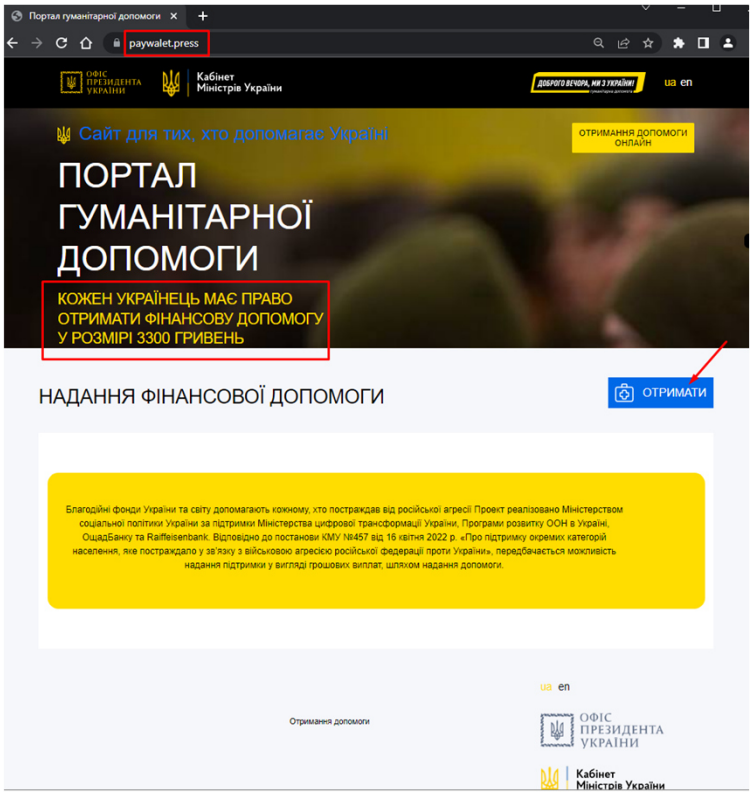


Урядовий портал

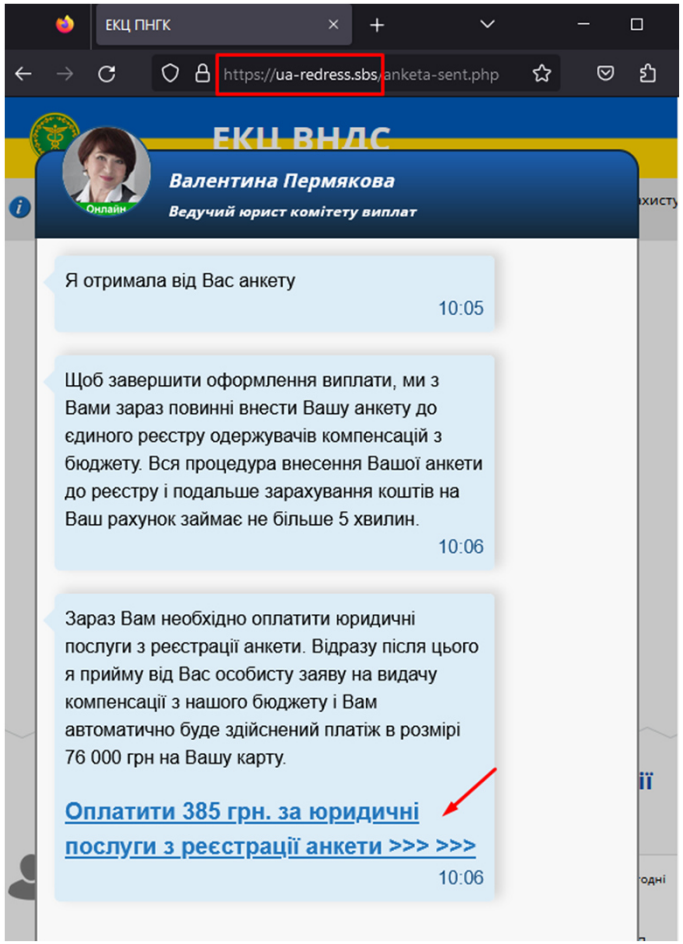


Приклади фішингових сайтів

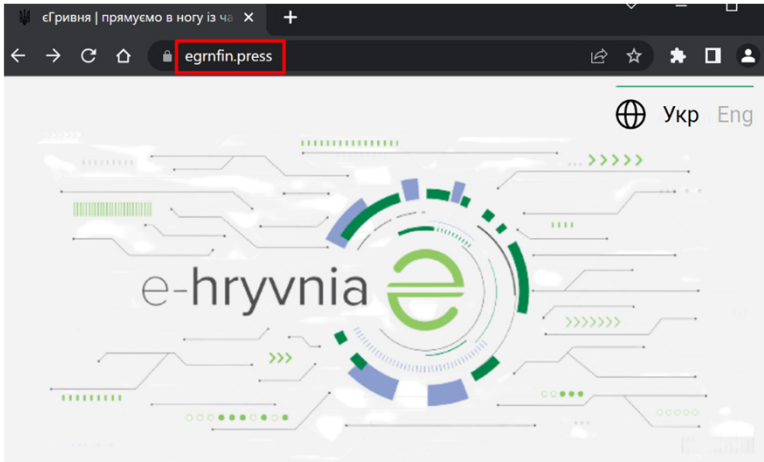
Портал гуманітарної допомоги



Компенсації

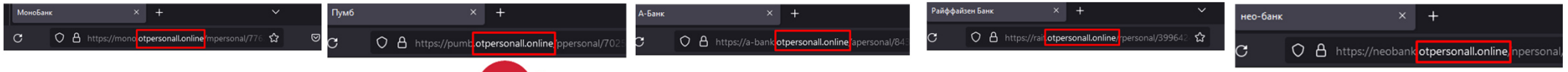


Є-гривня

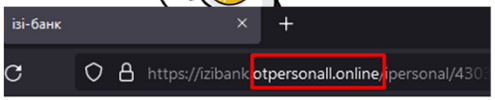


НБУ та Міністерства цифрової трансформації України презентував проєкт концепції е-гривні – вона зможе ефективно виконувати звичайні функції грошей

Приклади фішингових сайтів - сторінки банків України



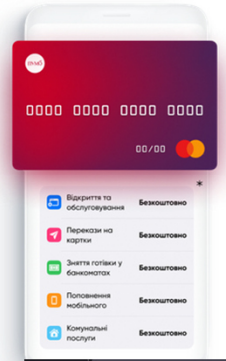
monobank | Universal Bank

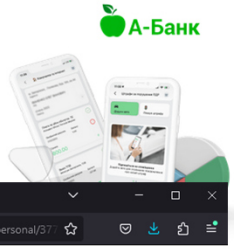


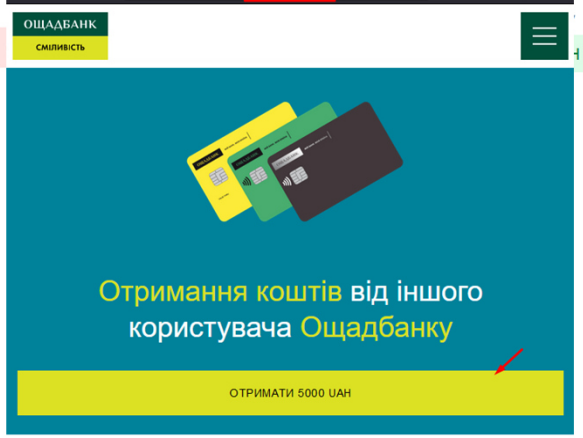
izibank

Отримання переказу

Отримати 5000 UAH

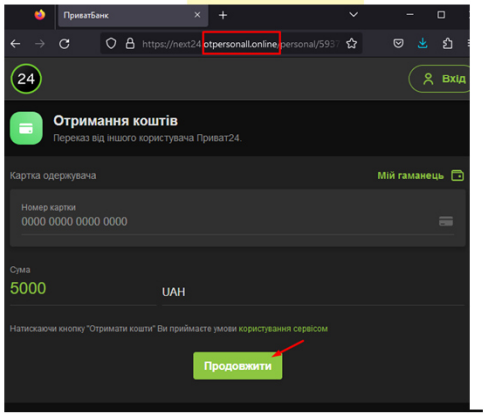






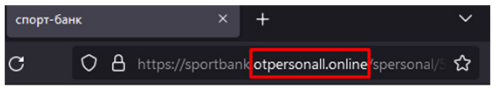
Отримання переказу

Отримати 5000 UAH



Отримання переказу

Отримати 5000 UAH



sportbank

Отримання переказу

Отримати 5000 UAH

Методи протидії

1. **Підвищення кіберобізнаності (кібергігієни) громадян України:**
   НБУ постійно займається організацією та проведенням заходів підвищення кібергігієни в банківській системі України та серед користувачів банківських послуг (https://promo.bank.gov.ua/stopfraud/ - проект Шахрай Гудбай), активно співпрацює із асоціацією ЕМА з питань платіжного шахрайства

2. **Блокування шахрайських ресурсів на рівні реєстраторів, хостерів та надавачів хмарних послуг:**
   CSIRT-NBU у більшості випадків подає відповідні скарги (abuse) для блокування фішингових ресурсів. Дані звернення опрацьовуються відповідно до визначених політик, процедур, правил та час реагування в даному випадку є дуже великим (від декількох днів до декількох тижнів), даний підхід не є ефективним. Команда CSIRT-NBU постійно шукає шляхи підвищення ефективності даного підходу (налагодження прямих контактів, покращення процедур, консультації з міжнародними партнерами)

3. **Використання Google Save Browsing:**
   CSIRT-NBU в обов'язковому порядку подає відповідні скарги (abuse) для блокування фішингових ресурсів. Механізм працює тільки у браузерах Google Chrome, Firefox, Safari та додатку Instagram. Не ефективний для мобільних додатків Facebook, Telegram, Viber, тощо. Додатки використовують власні вбудовані браузери та є основними засобами розповсюдження фішингових посилань.

4. **Обмеження фішингових ресурсів на рівні надавачів телекомунікаційних послуг:**
   CSIRT-NBU розробила пропозиції щодо архітектури побудови системи протидії фішинговим сайтам. Пропозиції подані до Держспецзв'язку та РНБО. 14.09.2022 РНБО провела робочу нараду із обговорення цих питань із залученням ключових суб'єктів (НБУ, Кіберполіція, Держспецзв'язок, РНБО), представників провайдерів та ЕМА. Всі учасники підтримали використання даного підходу для протидії фінансовому шахрайству.

Існуючий міжнародний досвід

У 2020 році розпочали боротьбу із фішинговими сайтами, що націлені та викрадення особистих даних, банківської інформації та облікових записів. Блокування відбувається на рівні операторів телекомунікаційних послуг Польщі. Підписано угоду за участі Міністерства Цифрової трансформації, NASK (CERT-PL) та надавачів телекомунікаційних послуг. Провайдери приймають участь на волонтерських засадах та завжди можуть відмовитися від участі.

У 2015 році впровадили SWITCH DNS Firewall, що реалізований із використанням методу DNS Response Policy Zones (RPZ). Першочергово обслуговували клієнтів SWITCH, на даний момент надають сервіс на договірних засадах.

У 2017 році впровадили Protective Domain Name Service (PDNS). PDNS було створено, щоб перешкоджати використанню DNS для розповсюдження та роботи шкідливих програм. Його створив Національний центр кібербезпеки (NCSC), а впроваджує Nominet. Реалізований із використанням методу DNS Response Policy Zones (RPZ). Клієнтами є державні організації. Список фільтрації налічує близько 60М.

https://cert.pl/en/posts/2020/03/malicious_domains/
https://www.switch.ch/dns-firewall/
https://www.ncsc.gov.uk/information/pdns

Очікуваний ефект

За результатами впровадження даного підходу, реалізації швидких процедур внесення шкідливих доменів до переліку, а також підключення ключових провайдерів до системи будуть реалізовані наступні функції забезпечення кібербезпеки:

Попередження

- зменшення кількості фінансового шахрайства
- зменшення кількості скомпрометованих облікових записів (фінансових установ, тощо)

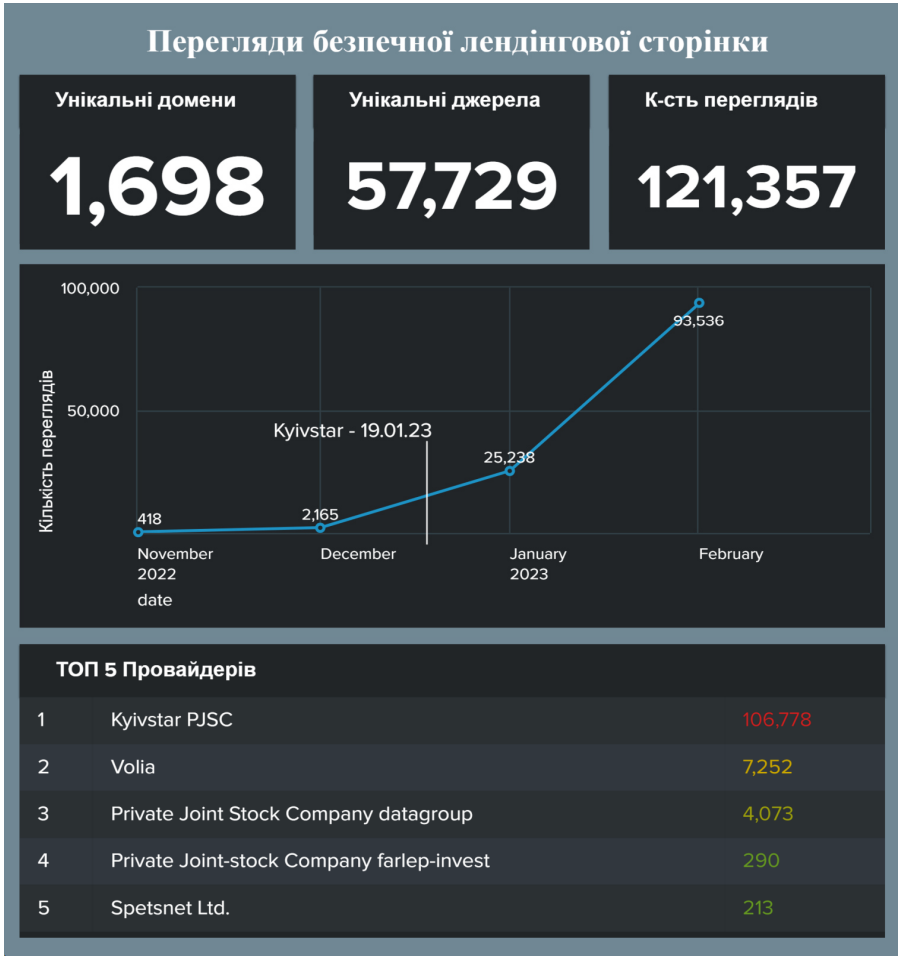
Виявлення та звітність

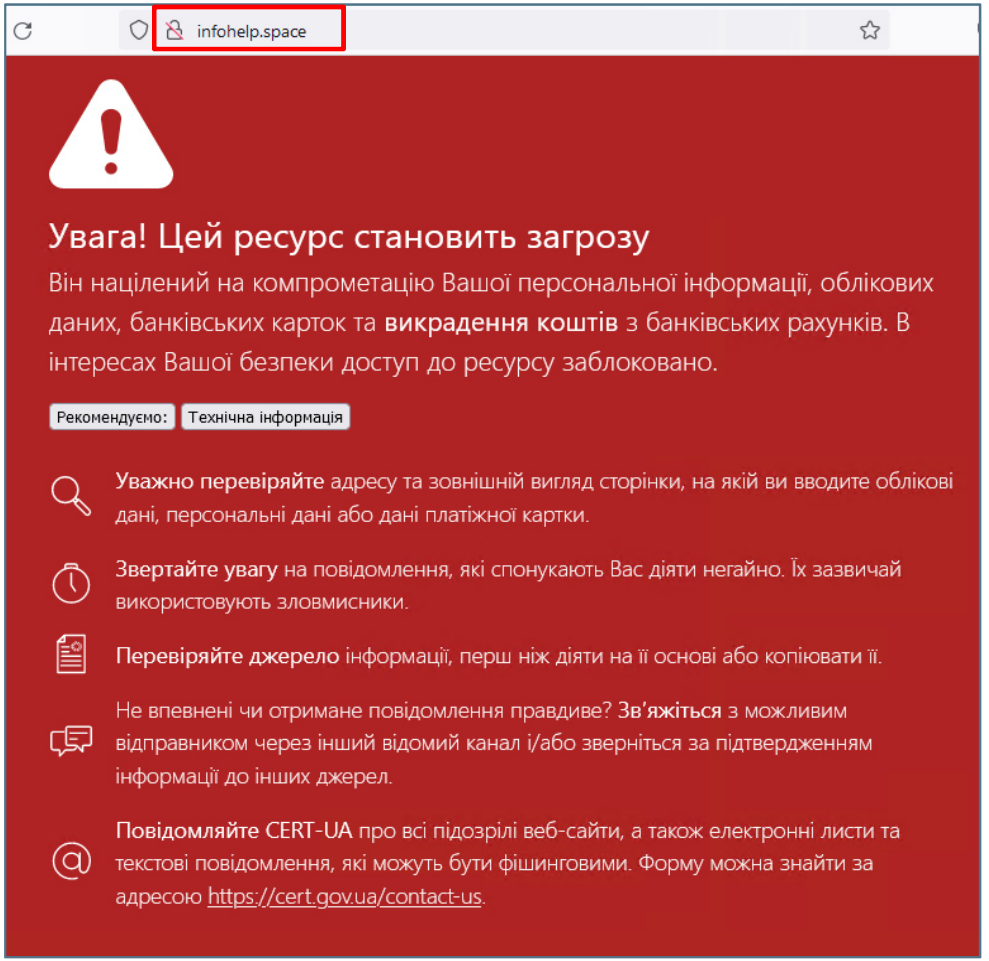
- виявлення джерел розповсюдження
- виявлення фішингових кампаній
- отримання статистичних даних щодо фішингових кампаній

Обізнаність

- інформування користувача про перехід на шкідливий ресурс (перенаправлення на безпечну цільову сторінку)

Статистика переходів на лендінгову сторінку





* статистичні дані станом на 15.02.2023

Дякую за увагу!