



National Bank  
of Ukraine

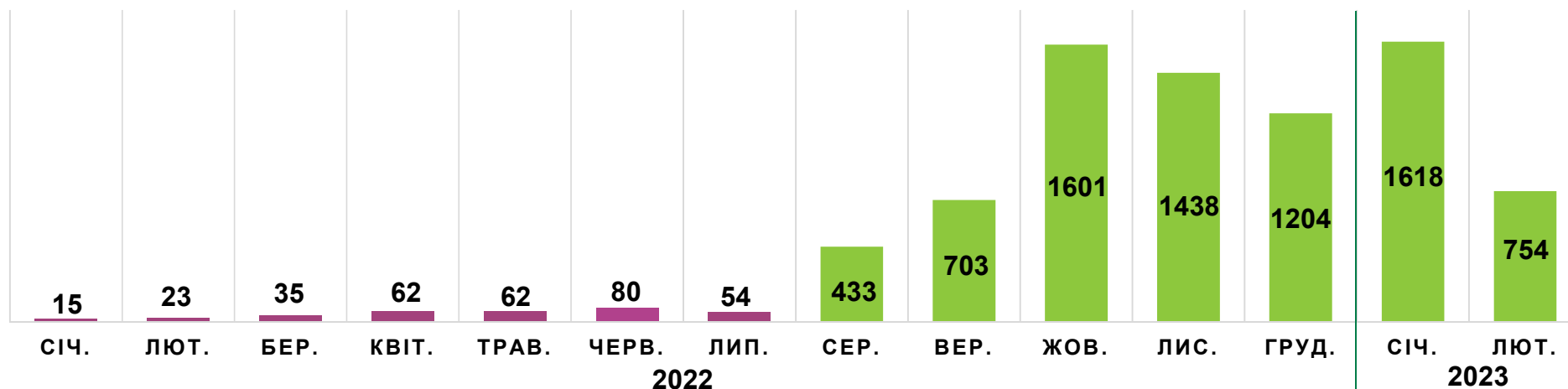
## Протидія кібершахрайству у фінансовій сфері

Київ, 2023



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

### Кількість виявлених фішингових доменів



Використання моніторингу брендів (без збагачення)

Використання моніторингу брендів  
Використання механізмів проактивного пошуку шкідливих доменів  
Отримання репортів від учасників інформаційного обміну

\* статистичні дані станом на 15.02.2023

# Приклади фішингових сайтів

## Приват інвест

Головна сторінка

privat-inv.com/ref/pi002?sub1=c043fntfvmirdae&sub4=10618&sub5=0

ПриватБанк

Цю сторінку дивляться 113 особи У проєкті залишилося 13 вільних місць

**«Приват» відкривається для приватних інвесторів**

Національні ресурси — джерело доходу кожного українця

11%

Увімкніть звук

Почніть заробляти з «Приват»

Ім'я

Прізвище

Електронна пошта

+49 1512 3456789

ХОЧУ ОТРИМУВАТИ ДОХІД ВІД НАЦІОНАЛЬНИХ РЕСУРСІВ

Я даю згоду на збір адреси мого електронної пошти з метою отримання комерційних пропозицій, які, на мого думку, будуть цікавими для мене. Збір даних комерційної галузі, детально описані в наших Умовах користування | Політиці конфіденційності.

## Благодійний фонд

Если вам нужна помощь | Благ

Не конфіденційний pomogaem.space

БЛАГОДІЙНИЙ ФОНД ПОМОГАЄМ

Про фонд Звіти help

ПОТРЕБУЮ ДОПОМОГИ ДОПОМОГИ

Вам нужна помощь? В ПОМОГАЕМ

**Благодійний фонд «Помогаєм» надає допомогу:**

- важкохворим дітям і дітям з інвалідністю;
- «відмовників» (кинутим новонародженим дітям) і дітям-сиротам;
- приймочним сім'ям та дитячим будинкам сімейного типу;
- медичним установам;
- сім'ям у складних життєвих обставинах;
- багатодітним сім'ям;
- малозабезпеченим сім'ям;
- багатодітним сім'ям переселенців;
- сім'ям, які пережили пожежа, потоп, втрату житла;
- одиноким матерям / батькам;
- вагітним жінкам і жінкам з новонародженими дітьми в складних життєвих обставинах.

ПОТРЕБУЮ ДОПОМОГИ ДОПОМОГИ

## Міжнародна допомога UNICEF

UNICEF - Допомога Кожному

mssg.me/itehelp

UNICEF - Допомога Кожному Українцю ua

Подай заявку на отримання виплати:

ua 20000 гривень ua

ОЩАД БАНК

РАЙФАЙЗЕН

ПРИВАТ 24

ua Організація UNICEF виділила українцям 100.000.000\$  
Соціальну виплату можуть отримати абсолютно всі Українці віком від 18 років у офіційному сайті UNICEF  
Сумма виплати наразі складає 20000 гривень.

# Приклади фішингових сайтів

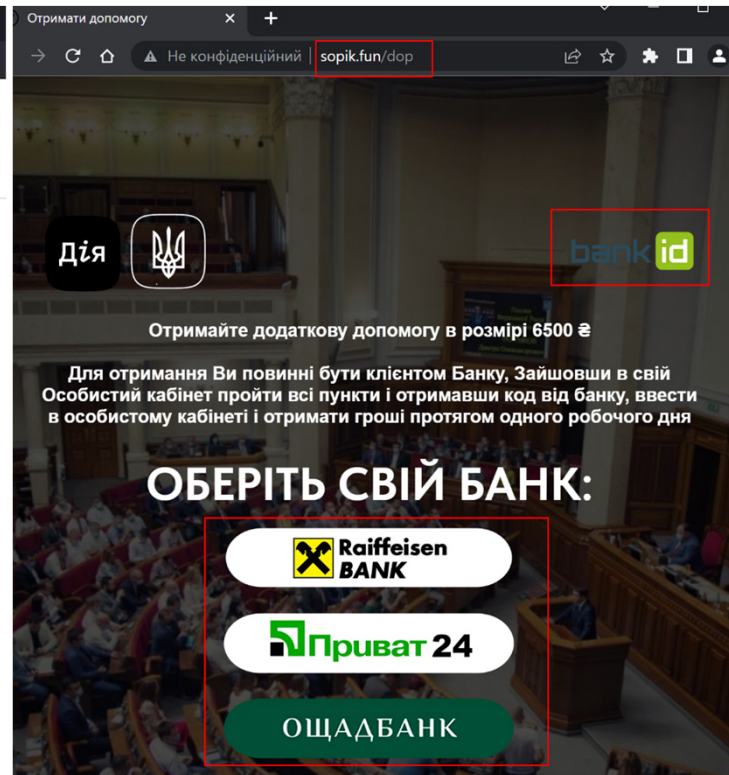
## ЄДопомога



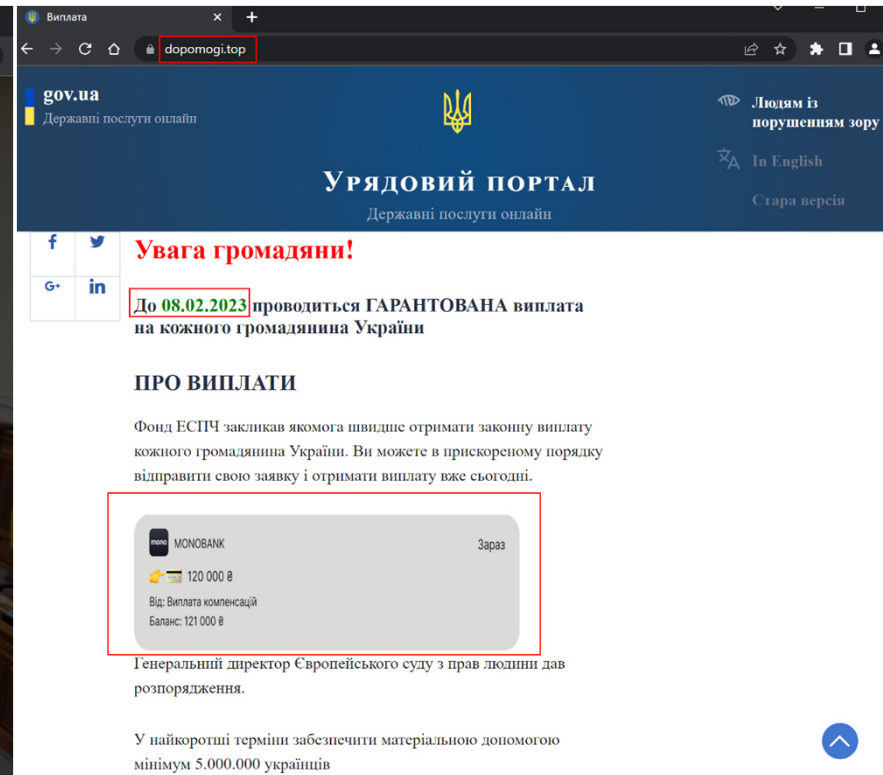
Заповніть заявку на виплату грошової допомоги від міжнародних організацій мешканцям України.

Включаючи тих, хто перебуває на тимчасово окупованих, деокупованих територіях або таких, що знаходяться в зоні активних бойових дій.

## Портал Дія



## Урядовий портал



# Приклади фішингових сайтів

## Портал гуманітарної допомоги

The screenshot shows a browser window with the URL [paywalet.press](http://paywalet.press). The page header includes the Ukrainian coat of arms and logos for the President's Office and the Cabinet of Ministers. The main heading reads "ПОРТАЛ ГУМАНІТАРНОЇ ДОПОМОГИ". A prominent yellow box contains the text: "КОЖЕН УКРАЇНЕЦЬ МАЄ ПРАВО ОТРИМАТИ ФІНАНСОВУ ДОПОМОГУ У РОЗМІРІ 3300 ГРИВЕНЬ". Below this, there is a blue button labeled "ОТРИМАТИ" and a section titled "НАДАННЯ ФІНАНСОВОЇ ДОПОМОГИ". A yellow box at the bottom contains a detailed text about the aid program, mentioning the Ministry of Social Policy and the Raiffeisenbank.

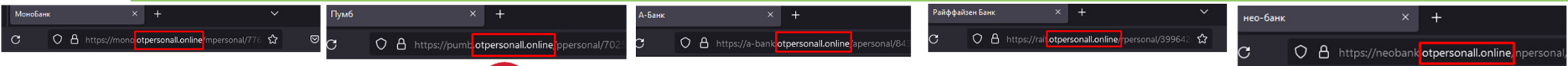
## Компенсації

The screenshot shows a browser window with the URL <https://ua-redress.sbs/anketa-sent.php>. The page features a profile for "Валентина Пермякова" (Valentina Permyakova), a "Ведучий юрист комітету виплат" (Lead lawyer of the payment committee). The main text states: "Щоб завершити оформлення виплати, ми з Вами зараз повинні внести Вашу анкету до єдиного реєстру одержувачів компенсацій з бюджету. Вся процедура внесення Вашої анкети до реєстру і подальше зарахування коштів на Ваш рахунок займає не більше 5 хвилин." Below this, it says: "Зараз Вам необхідно оплатити юридичні послуги з реєстрації анкети. Відразу після цього я прийму від Вас особисту заяву на видачу компенсації з нашого бюджету і Вам автоматично буде здійснений платіж в розмірі 76 000 грн на Вашу карту." A blue link is provided: "Оплатити 385 грн. за юридичні послуги з реєстрації анкети >>> >>>".

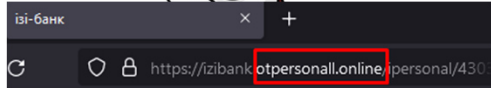
## Є-гривня

The screenshot shows a browser window with the URL [egmfin.press](http://egmfin.press). The page features a large graphic with the text "e-hryvnia" and a stylized "e" symbol. Below the graphic, there is a text block: "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

ОЩАДБАНК  
СПИВІВІСТЬ

Отримання коштів від іншого користувача Ощадбанку

ОТРИМАТИ 5000 UAH



Отримання переказу  
Отримати 5000 UAH

24

Отримання коштів  
Переказ від іншого користувача Приват24.

Карта одержувача Мій гаманець

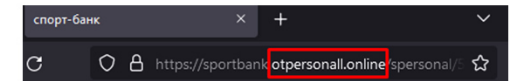
Номер картки  
0000 0000 0000 0000

Сума  
5000 UAH

Натискаючи кнопку "Отримати кошти" Ви приймаєте умови користування сервісом

Продовжити

NEOBANK  
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 браузерях 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 на 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 60M.

[https://cert.pl/en/posts/2020/03/malicious\\_domains/](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)

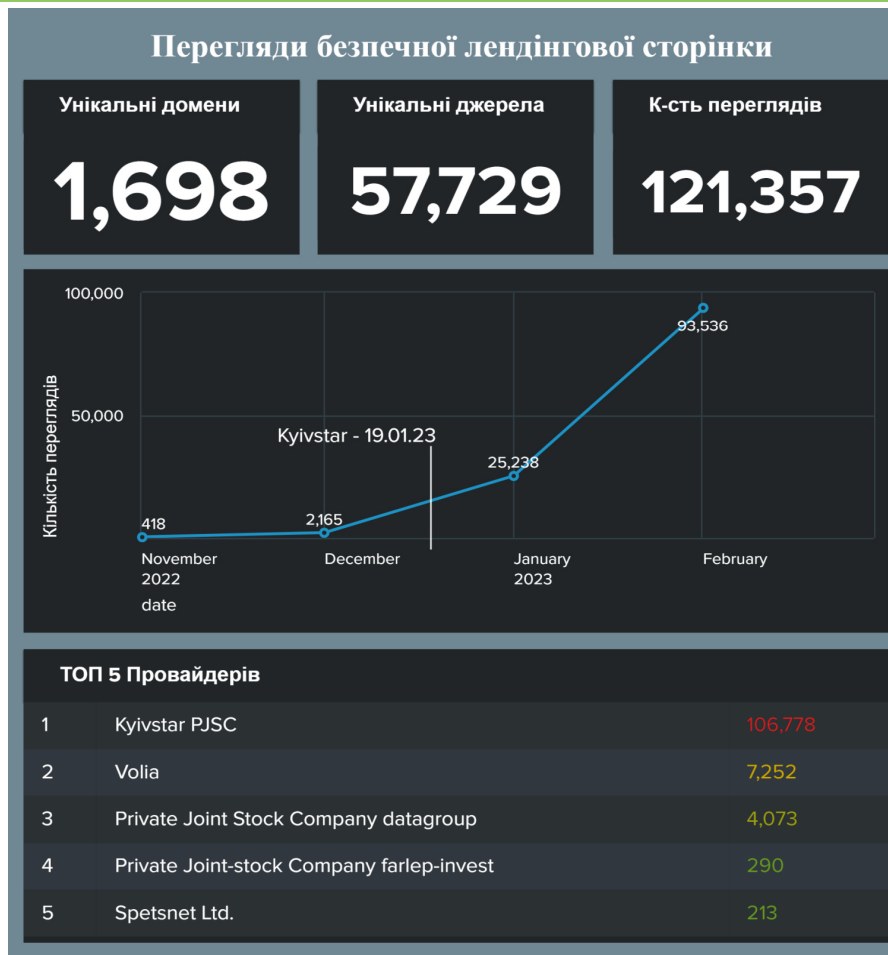
### **Виявлення та звітність**

- 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



infohelp.space

### Увага! Цей ресурс становить загрозу

Він націлений на компрометацію Вашої персональної інформації, облікових даних, банківських карток та викрадення коштів з банківських рахунків. В інтересах Вашої безпеки доступ до ресурсу заблоковано.

Рекомендуємо: [Технічна інформація](#)

- Уважно перевіряйте адресу та зовнішній вигляд сторінки, на якій ви вводите облікові дані, персональні дані або дані платіжної картки.
- Звертайте увагу на повідомлення, які спонукають Вас діяти негайно. Їх зазвичай використовують зловмисники.
- Перевіряйте джерело інформації, перш ніж діяти на її основі або копіювати її.

Не впевнені чи отримане повідомлення правдиве? Зв'яжіться з можливим відправником через інший відомий канал і/або зверніться за підтвердженням інформації до інших джерел.

Повідомляйте CERT-UA про всі підозрілі веб-сайти, а також електронні листи та текстові повідомлення, які можуть бути фішинговими. Форму можна знайти за адресою <https://cert.gov.ua/contact-us>.

\* статистичні дані станом на 15.02.2023



**Дякую за увагу!**