Шахрайські та фішингові сайти

Аналіз, тренди та рекомендації для клієнтів, 2022/2023

Дайджест платіжного шахрайства

Лютий 2023

У 2022 р. Асоціація «ЄМА» у співробітництві з чеським підрозділом компанії ThreatMark (США) заблокували на рівні реєстраторів 568 активних фішингових та шахрайських сайтів в українському сегменті Інтернет, націлених проти споживачів фінансових послуг.

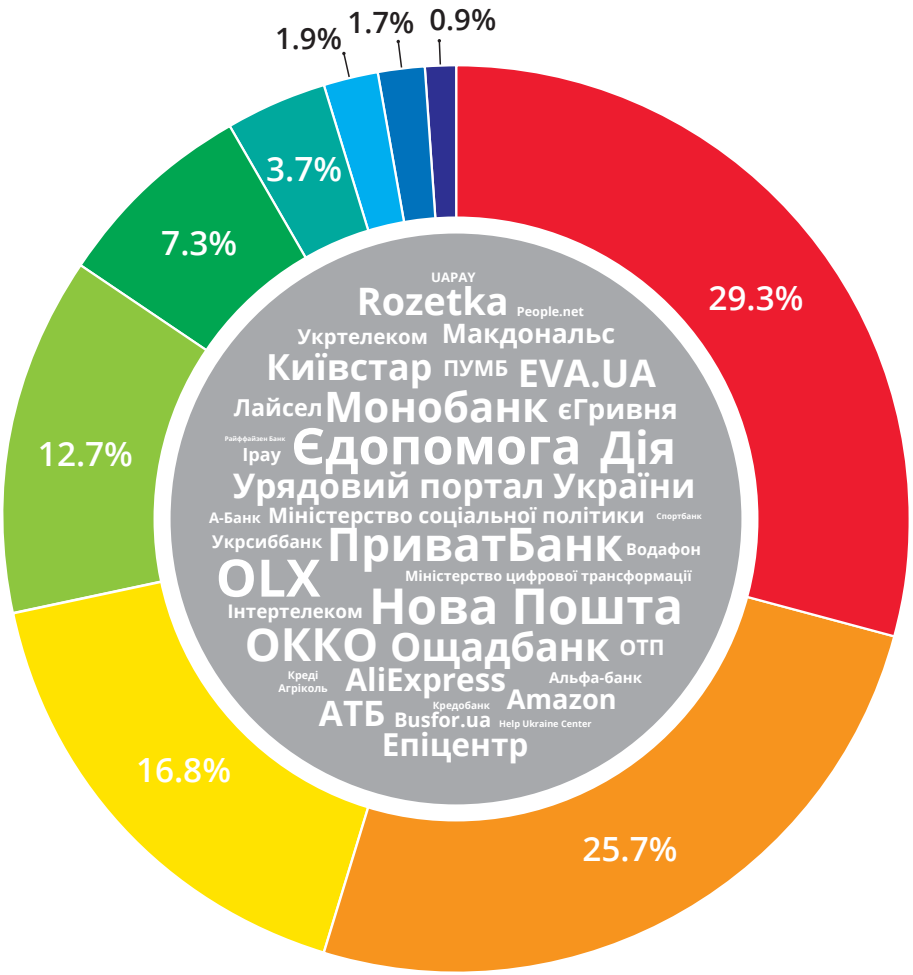
Для порівняння у 2021 р. Асоціацією «ЄМА» було заблоковано 215 доменів.

- Найчастіше як приманку шахраї використовують грошові виплати від держави, міжнародних організацій, відомих українських компаній та банків.
- Зростання кількості фішингових сайтів пов'язане з дедалі більшим поширенням схеми виманювання у банківських клієнтів облікових записів до онлайн-банкінгу, після чого з їх карткових рахунків знімаються гроші та на їх ім’я оформлюються онлайн-кредити.
- В 2022 р. зросла кількість виявлених фейкових застосунків у Google Play та App Store, більшість з яких рекламуються як застосунки для реалізації залишків палива за низькими цінами та застосунки для отримання грошової допомоги від держави та міжнародних організацій. Також збільшилася кількість фейкових банківських чат-ботів у Telegram, що виманюють карткові реквізити та облікові записи до онлайн-банкінгу.
- Фішинг залишається найбільш масовою загрозою для українських користувачів Інтернет, і його масштаби неухильно зростають. Саме фішингові сайти становлять 88% заблокованих ресурсів кібермародерів. Решта 12% припадають на шахрайські інтернет-крамниці, шахрайські схеми заробітку, шахрайство з «інвестиціями» та наданням послуг, в результаті яких у громадян виманюються гроші, та сайти зі шкідливим ПЗ.

Ландшафт онлайн-шахрайства під час війни

Кібермародери теж люблять бренди. Паливна субсидія від ОККО, приз 5000 гривень від Київстар, грошова субсидія розміром 3000$ від АТБ... – під приводом роздачі великих грошей від імені відомих українських компаній кібермародери виманюють у громадян гроші, реквізити платіжних карток та облікові записи до онлайн-банкінгу.

Найулюбленіші бренди кібермародерів у 2022 р.: **єДопомога, Дія, ПриватБанк, Ощадбанк** та **OLX**.



- Фішингові банківські сайти
- Афери з компенсаціями та виплатами громадянам
- Фішингові платіжні сайти, P2P, обмінники та поповнення мобільного рахунку
- Фейкові опитування, лотереї та розіграші
- Шахрайські інтернет-крамниці
- Фішингові сайти маркетплейсів та поштових операторів
- Заробіток та працевлаштування
- Пастки для кріптанів, інвесторів та беттерів
- Шахрайство з наданням послуг

Заблоковано!

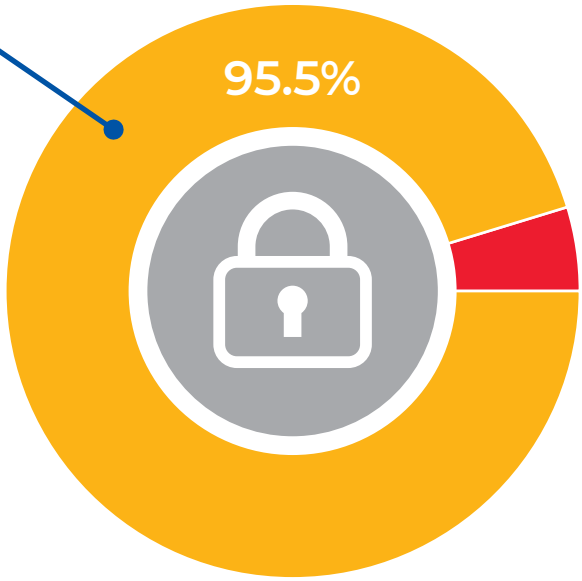
568
сайтів

У 2022 р. Асоціація «ЄМА» ідентифікувала та заблокувала 568 шахрайських сайтів, що виманюють облікові записи, карткові реквізити та гроші у громадян України.

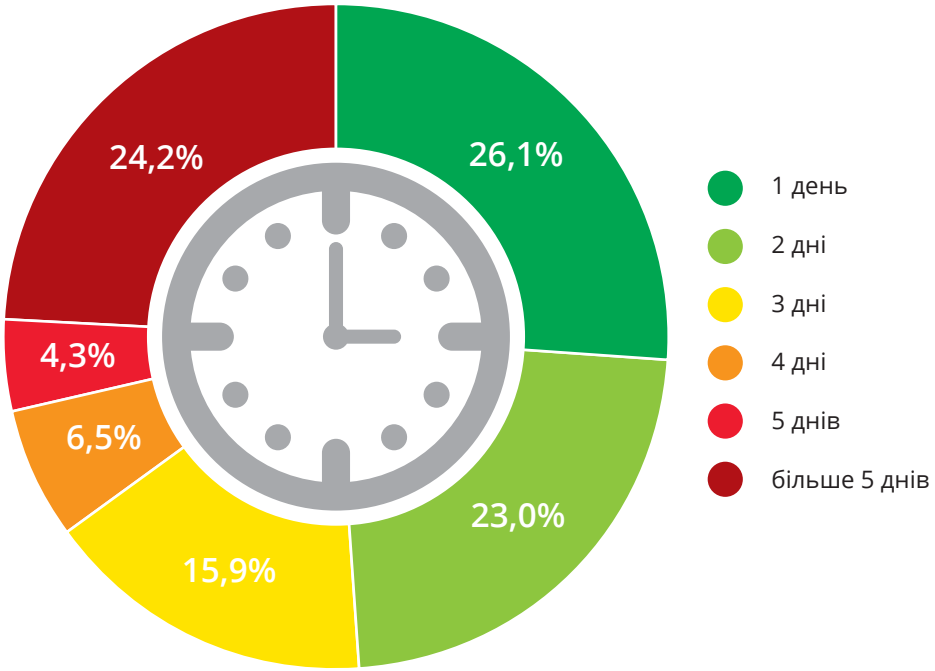
Коефіцієнт успішного блокування шкідливих ресурсів на рівні реєстратора (closure rate) склав **95,5%**.

Рекорд швидкої дії реєстратора з блокування шахрайського ресурсу – **18 хвилин**.

Максимальний час блокування сайту на рівні реєстратора склав 32 дні.



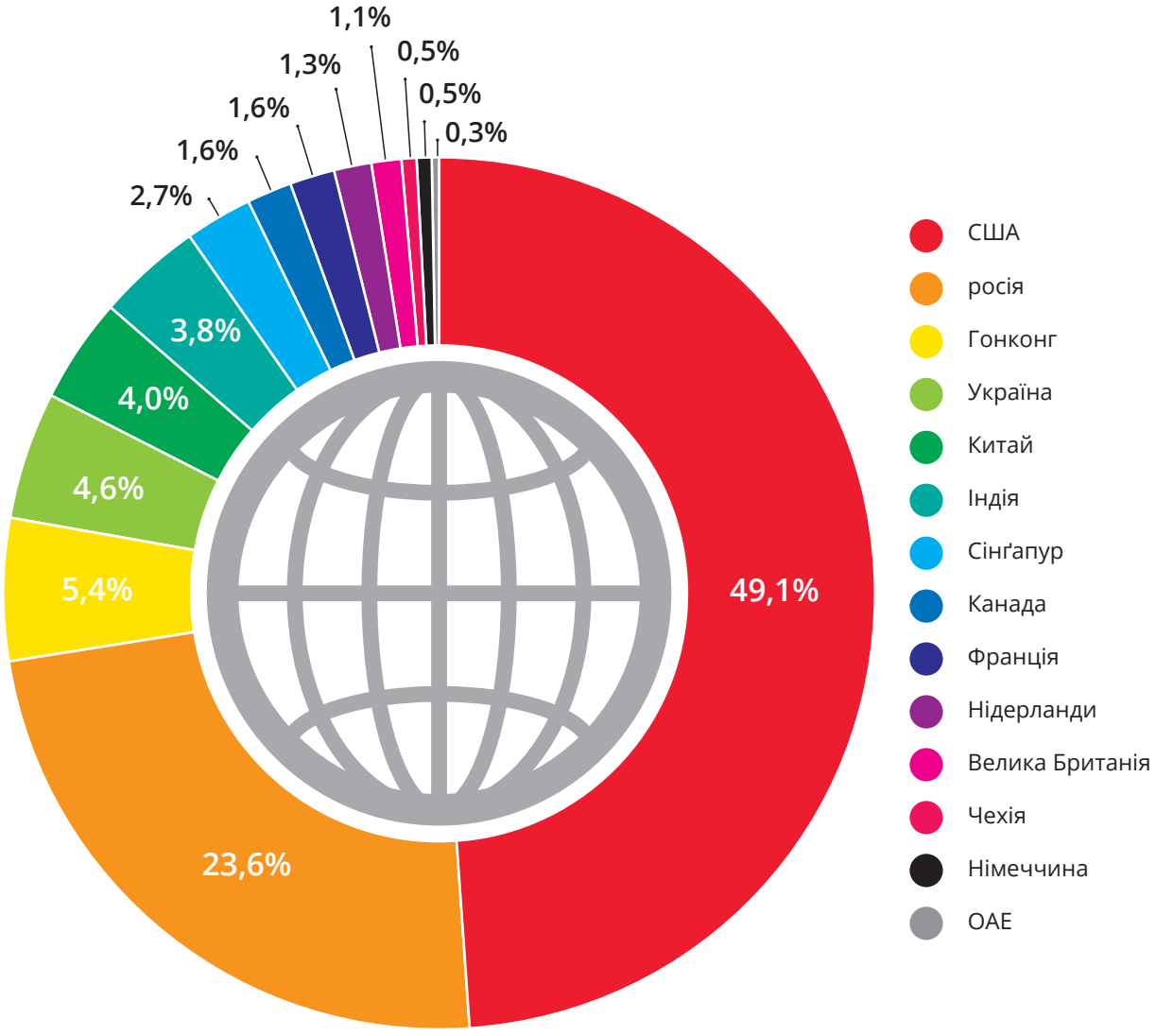
Протягом якого часу після виявлення було заблоковано шахрайський сайт



Країни походження реєстраторів

Основними країнами походження реєстраторів є США (49,1%) та росія (23,6%), що відповідає світовому тренду.

57,8% шахрайських ресурсів використовують зворотній проксі для сайту від американського сервісу Cloudflare, який допомагає бізнесу захистити свій сайт від атак, а шахраям – заховати свого реального хостинг-провайдера, щоб затягнути блокування шахрайського ресурсу.



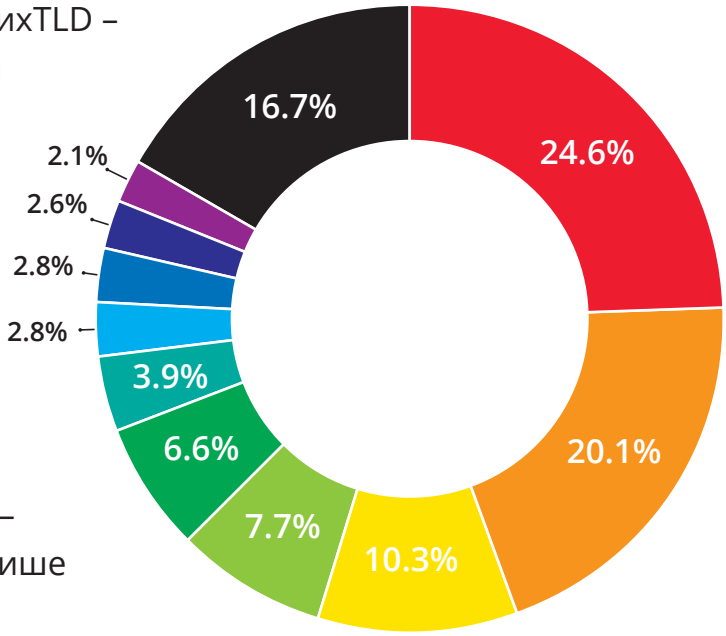
Надзвичайно, але факт: Найбільш абузостійким реєстратором та хостером шахрайських ресурсів, тобто таким, що **не реагує** на «абузи» (скарги), став не російський сервіс, а вітчизняний – **Хостинг-Україна**. 242 скарги, що були направлені до Хостинг-Україна у 2022 році, залишилися без відповіді та реакції з боку сервісу.

Топ

Топ-10 TLD

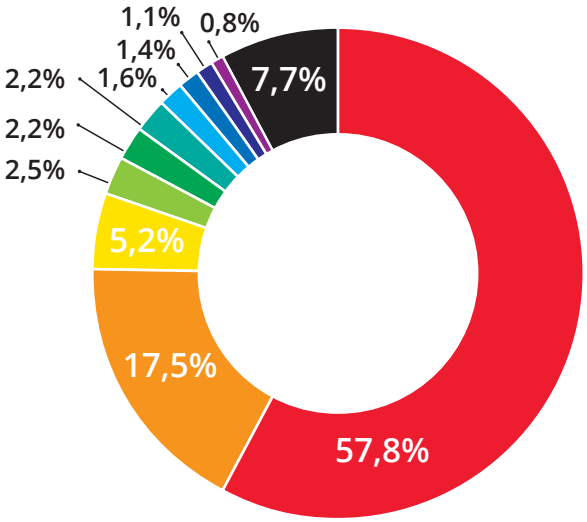
В ТОПі улюблених шахрайськихTLD – ті, на яких відсутні обмеження під час реєстрації: «топова» доменна зона **.top** (24,6%), найпопулярніша зона світу **.com** (20,1%) та універсальна доменна зона **.site**

Раніше популярна у шахраїв доменна зона **.ru** втратила свою привабливість, ставши ознакою шкідливого ресурсу, – її в 2022 р. використовувало лише 1,7% шахрайських сайтів.



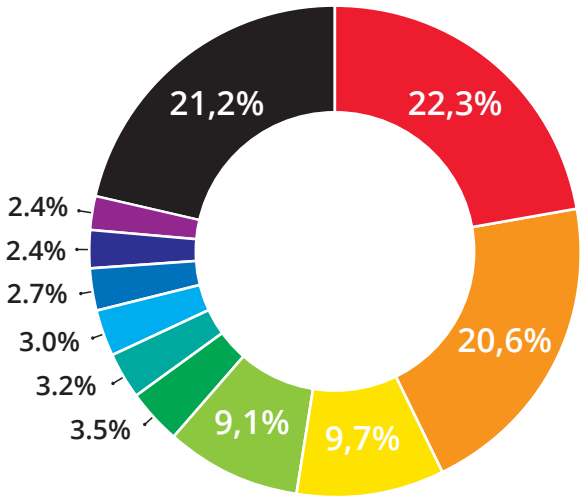
.top .com .site .me .shop
.com.ua .xyz .biz .online .net інші

Топ-10 провайдерів та сервісів публікації



Cloudflare
DigitalOcean
Hosting Ukraine
Amazon
DDOS-Guard
Hetzner Online
OVH
Fornex
Google LLC
SonderCloud
інші

Топ-10 реєстраторів



NameSilo
REG.RU
Namecheap
Sav.com, LLC
PDR LTD. D/B/A publicdomainregistry.com
Chengdu West Dimension Digital Technology Co.
Hosting Ukraine
GoDaddy
EraNet
NiceNIC

Рекомендації для громадян

- **Завжди перевіряйте веб-сайти**, якщо йдеться про гроші, карткові реквізити та облікові записи. Для перевірки використовуйте безкоштовний функціонал **CheckMyLink** (check.ema.com.ua), який за лічені секунди перевірить сайт на шахрайство та віруси.
- **Будьте пильними**, навіть завантажуючи програми з офіційних сторів – **App Store** та **Google Play**. А саме, обов'язково перевіряйте, хто є автором застосунку та чи має він відношення до реального бренду; уважно вивчайте відгуки, – нерідко саме там можна зустріти попередження щодо шахрайства. Найбезпечніше завантажувати мобільний застосунок за посиланням на офіційному сайті компанії, яка є його власником.
- Щоб відрізнити справжній чат-бот у Telegram від фейкового, використовуйте інструмент для перевірки чат-ботів на сайті **https://dovidka.info/**. Найбезпечніше переходити у чат-бот за посиланням на офіційному сайті компанії, яка є його власником.

Здолаємо шахраїв разом!

З питань аналітики та блокування шахрайських сайтів
звертайтесь до Раїси Федоровської
fera@ema.com.ua, +380 50 390 10 26

Українська міжбанківська асоціація платіжних систем «ЄМА»