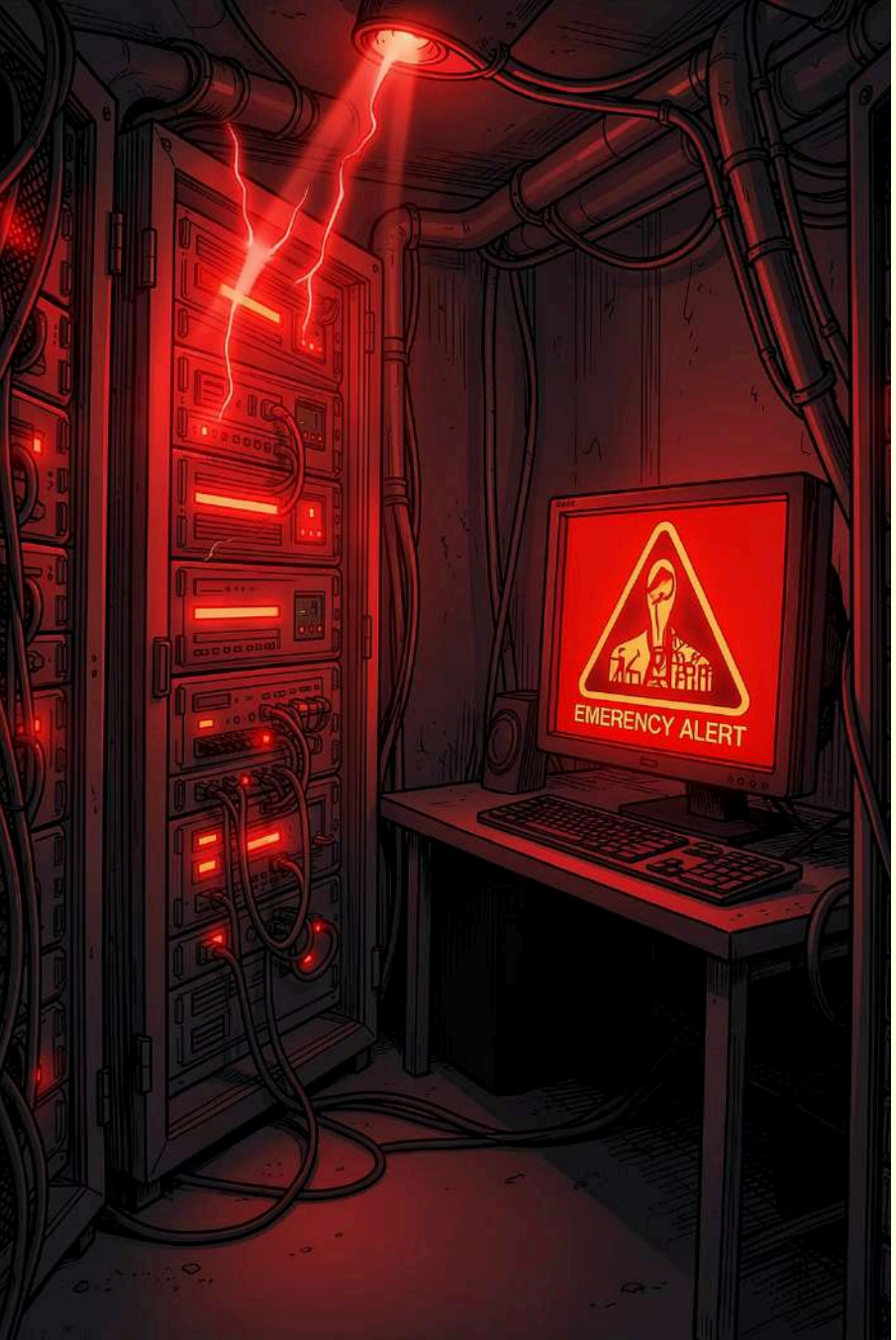
Кібератаки на «Дію»

Витоки персональних даних

Від збою сервісу – до ризику приватності. Що сталося, чому це важливо і як захистити себе.





Хвилини, коли державний сервіс «зупинився»

Що сталося

Кібератака російських хакерів спричинила призупинення роботи основних систем Міністерства юстиції України.

Хто повідомив

Про порушення в роботі офіційно повідомив портал державних послуг «Дія» – головний цифровий інтерфейс громадян з державою.

Made with GAMMA

Ключовий поворот: дані чи доступ?



ОФІЦІЙНА ПОЗИЦІЯ

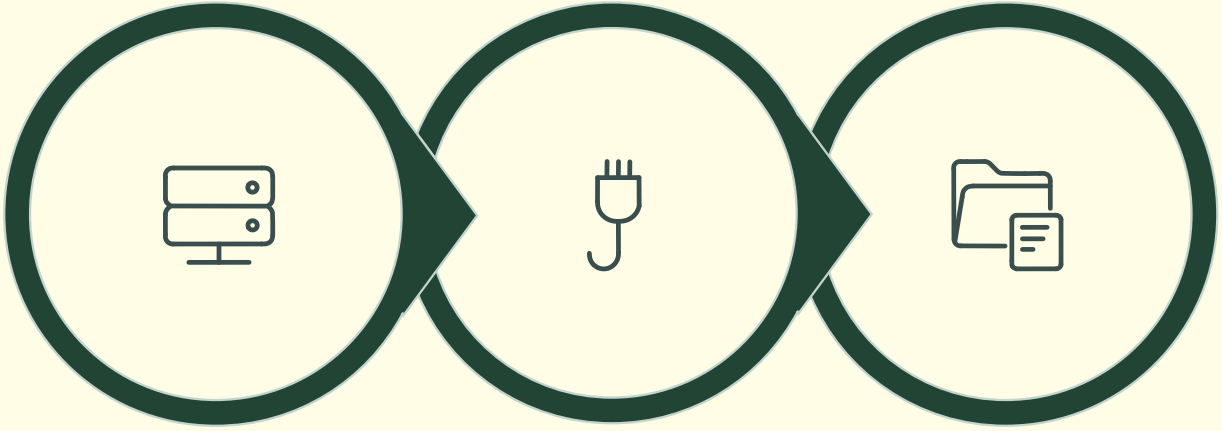
Влада запевнила: витік даних не підтвердився

«Дія» технічно **не зберігає** особисті дані користувачів — сервіс лише підтягує їх із державних реєстрів у режимі реального часу.

Ризик стосувався не бази даних, а **доступності інфраструктури** — тобто можливості користуватися сервісом.

Made with GAMMA

Втеча в інфраструктуру: роль «HAIC»



Атака HAIC

Проникнення в Мін'юст

Ризик даних

Атаку пов'язали з державним підприємством **«Національні інформаційні системи» (HAIC)**. Після зламу HAIC зловмисники «вийшли в інфраструктуру з даними» Мін'юсту – це класичний приклад атаки через **ланцюжок постачання**.

Made with GAMMA

Що таке персональні дані — і чому їх шукають



Що це таке

Будь-яка інформація, що може **ідентифікувати людину**: ПІБ, адреса, паспортні дані, ІПН, номер телефону.



Шахрайство

Викрадені дані використовують для **фінансового шахрайства** та оформлення кредитів на чуже ім'я.



Крадіжка особистості

Зловмисники **видають себе за жертву** в соцмережах, месенджерах та держсервісах.



Спам і кібербулінг

Контакти потрапляють у бази для **масових розсилок**, маніпуляцій та психологічного тиску.

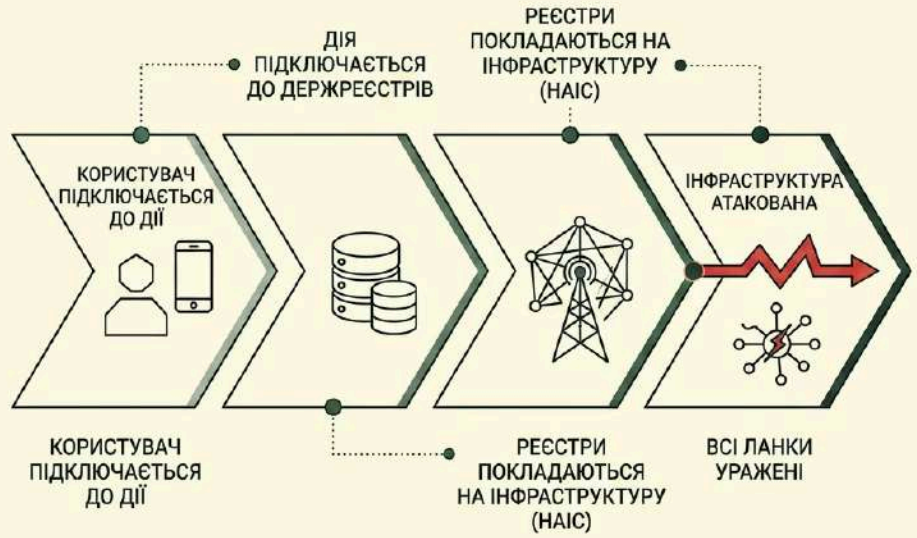
Made with GAMMA

Витоки — це «ланцюжок», а не одна помилка

Як влаштована «Дія»

Сервіс працює через **підключення до держреєстрів**. Збій або злам у будь-якій ланці цього ланцюжка впливає на цілісність усього процесу.

- Порушення **конфіденційності** – дані потрапили до чужих рук
- Порушення **цілісності** – дані змінені або пошкоджені
- Порушення **доступності** – сервіс недоступний



Made with GAMMA

Друга хвиля: фейкова «Дія»

🎣 Приманка

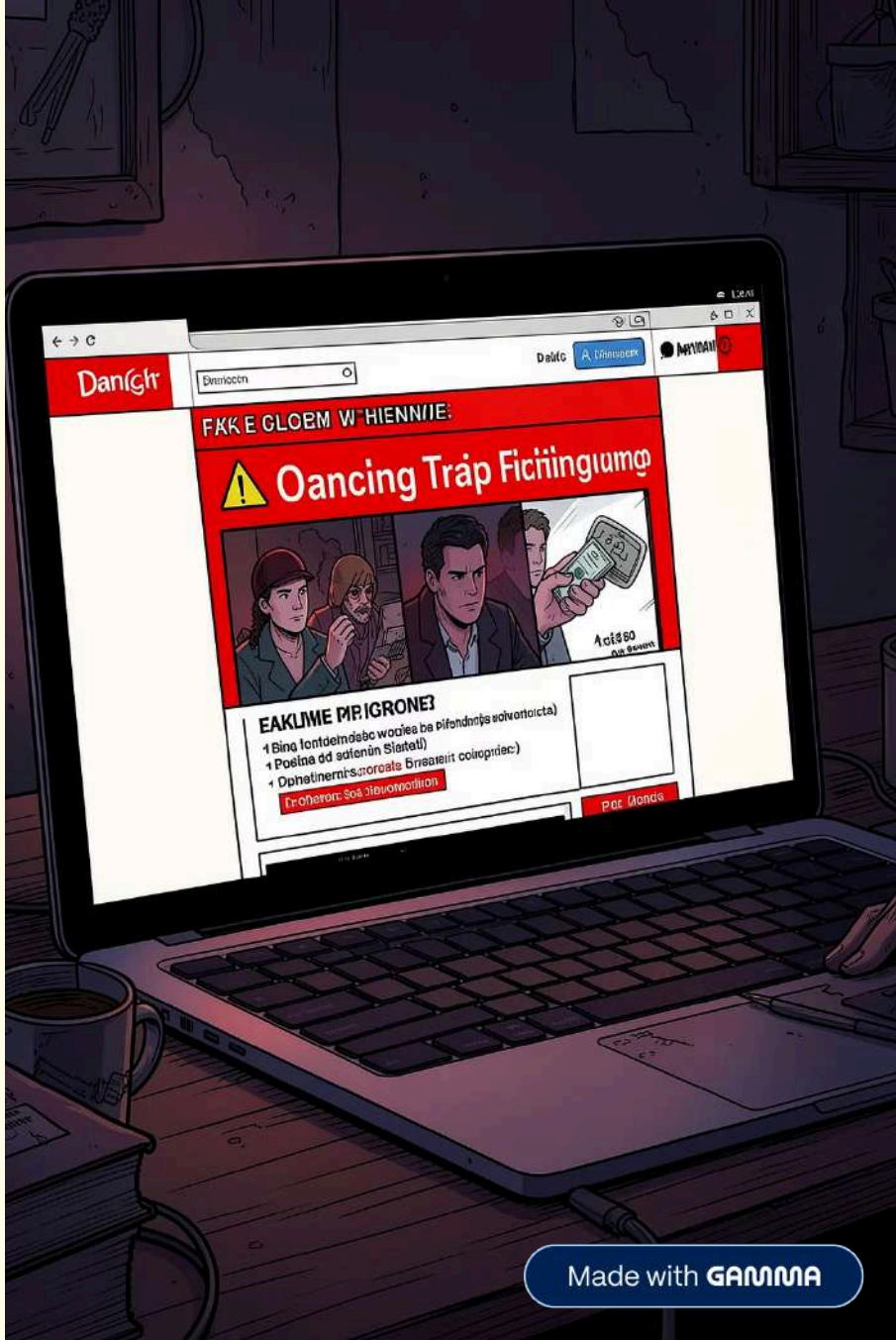
Шахраї створили ресурс із доменом, **максимально схожим** на офіційний портал Мінцифри.

📲 Дія

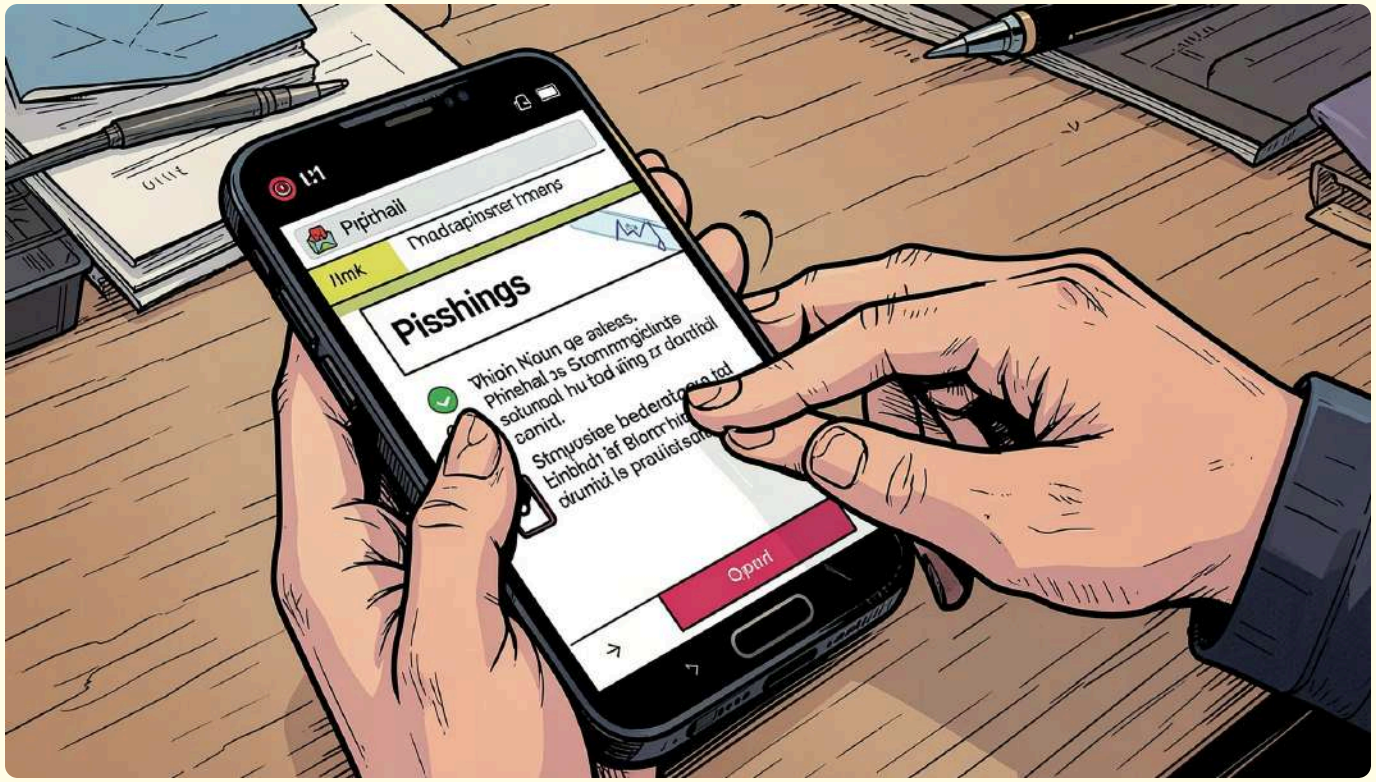
Людей просили завантажити **підроблений додаток** через браузер для отримання «доступу».

🔒 Реакція

Команда «Дії» виявила загрозу і **заблокувала** підроблену сторінку.



Як «витік» відбувається без хакерів-героїв



НАЙПОШИРЕНІШИЙ СЦЕНАРІЙ

Фішинг — зброя масового ураження

Користувача **«ведуть» на підроблену сторінку**, яка виглядає як офіційний сервіс. Там збирають логіни, паролі та персональні дані.

- Не відкривати підозрілі посилання та файли
- Завжди перевіряти адресу домену перед введенням даних
- Навіть листи «від знайомих» можуть бути небезпечними

Made with GAMMA

Три правила безпеки, які реально працюють

1

Лише офіційні джерела

Завантажуйте «Дію» лише з **App Store та Google Play**. Офіційний портал — **diia.gov.ua**. Жодних сторонніх посилань.

2

Перевіряйте самостійно

Не вводьте дані після переходів «зі стрибком». **Самостійно набирайте адресу** в браузері та перевіряйте домен.

3

Ігноруйте фішинг

Навіть якщо лист «від знайомих» — **не натискайте підозрілі посилання**. Перевірте через інший канал зв'язку.

Made with GAMMA

Кіберзахист починається з дій користувача

Системний ризик

«Дія» підтягує дані з реєстрів – збій інфраструктури створює ризики **доступності** для мільйонів користувачів.

Загроза фейків

Підроблені «Дії» зі схожими доменами – реальна зброя для **викрадення персональних даних**.

Ваша дія

Перевіряйте офіційні джерела, не довіряйте підозрілим посиланням і **дотримуйтесь кібергігієни** щодня.

Головне правило: якщо щось здається підозрілим – зупиніться, перевірте домен і зверніться до офіційних каналів «Дії».

