НОТАРІАЛЬНА
ПАЛАТА УКРАЇНИ

Комісія Нотаріальної палати України
з питань інформатизації, цифрової трансформації
та запобігання кіберзлочинності

Інформаційний лист
Щодо актуального стану кіберзагроз для нотаріальної спільноти

Шановні колеги,

Державне підприємство «НАІС» оприлюднило Підсумковий звіт з кібербезпеки за ІІ півріччя 2025 року, у якому детально описано поточний стан кіберзагроз для інфраструктури державних реєстрів.

Комісія НПУ з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності проаналізувала цей звіт і вважає за необхідне звернути вашу увагу на ключові висновки, що безпосередньо стосуються щоденної роботи нотаріусів.

*Ознайомитись зі звітом НАІС повністю можна за посиланням: **https://is.gd/zvit_nais_2026_cyber***

Що важливо знати

Звіт підтверджує те, про що Комісія попереджала раніше: **зловмисники цілеспрямовано атакують саме нотаріусів і державних реєстраторів**.

Угруповання, яке отримало назву UAC-0173 («Black Notary»), здійснює кібератаки саме з метою отримання прихованого доступу до робочих місць нотаріусів – для внесення несанкціонованих змін до державних реєстрів. Атаки мають комерційний характер і виконуються на замовлення.

Методи атак не є випадковими – вони ретельно сплановані, постійно вдосконалюються і використовують штучний інтелект для створення переконливого контенту. **Нехтувати правилами кібергігієни та кібербезпеки неприпустимо.**

Головний вектор атак – електронна пошта

За даними звіту НАІС, основним інструментом зловмисників залишається фішинг через електронну пошту. Листи майстерно імітують офіційні запити від судів, СБУ, НБУ, Міністерства юстиції, реєстраційних органів. Вони містять архіви або посилання, після відкриття яких зловмисники отримують повний прихований доступ до вашого комп'ютера і, відповідно, до реєстрів.

Приклади тем реальних шкідливих листів, зафіксованих у звітному періоді:

- «Запит судових документів»
- «Електронна вимога СБУ України»
- «Відділ Фінансового Моніторингу – ПриватБанк»
- «Щодо питань державної реєстрації ЮО та ФОП»

- «Зміни стосовно реєстрації ЮО та ФОП»
- «Протокол про адміністративне правопорушення»
- «Бойове розпорядження»

П'ять простих запитань, які захистять вас від фішингу

Перш ніж відкрити вкладення або перейти за посиланням у листі – **зупиніться і дайте собі відповідь**:

1. **Чи очікував(ла) я цей лист?** Якщо лист прийшов несподівано – це вже привід для підвищеної уваги.
2. **Чи знайомий мені відправник?** Перевірте адресу електронної пошти повністю, а не лише ім'я відправника.
3. **Чи надходили від цього відправника листи в такому форматі раніше?** Якщо державний орган вперше надсилає вам архів або просить «терміново відкрити файл» – це підозріло.
4. **Чи є у листі ознаки тиску або терміновості?** Фрази на кшталт «негайно», «протягом 24 годин», «невідкладно» – класичні прийоми маніпуляції.
5. **Що буде, якщо я просто не відкрию цей файл зараз?** У переважній більшості випадків – нічого. Справжній офіційний запит завжди можна уточнити.

У будь-якому сумнівному випадку не поспішайте. Зверніться до колег або безпосередньо до Комісії. Запитати – це не ознака некомпетентності, це ознака відповідальності.

Ресурси для самонавчання

Комісія НПУ з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності розмістила на вебсайті Нотаріальної палати України достатню кількість матеріалів для самостійного підвищення рівня кіберобізнаності.

За посиланням **https://npu.ua/palata/komisii/cyber/** ви знайдете практичні рекомендації, інструкції та актуальні попередження про загрози.

Також нагадуємо про рекомендації Комісії, які нещодавно доводились до відома нотаріусів через голів відділень НПУ. Якщо ви їх не отримали – зверніться до голови вашого регіонального відділення або безпосередньо до Комісії.

Кібербезпека нотаріуса – це не лише захист власного комп'ютера. Це захист прав ваших клієнтів, цілісності реєстрових даних і довіри до інституту нотаріату в цілому.
Будьте уважні. Діліться цією інформацією з колегами.

З повагою,
Голова Комісії НПУ з питань інформатизації,
цифрової трансформації та запобігання кіберзлочинності
Наталія КОЗАЄВА