ШІ на службі аферистів: збитки українців від шахрайства сягнули 1,4 мільярда

Читать на русском Read in English

ШІ на службі аферистів: збитки українців від технологічного шахрайства сягнули 1,4 мільярда

За перші п'ять місяців 2026 року фінансове шахрайство в Україні, особливо операції з банківськими рахунками, стало помітно технологічнішим і більш адресним. Зловмисники дедалі активніше застосовують штучний інтелект для генерації фейкових дзвінків, листів, підроблених вебресурсів і шахрайських пропозицій, які стає все складніше відрізнити від автентичних.

Основна зміна полягає в тому, що ШІ дозволив шахраям значно розширити вже відомі методи — соціальну інженерію, фішинг, фальшиві дзвінки «від банку» чи псевдоблагодійні збори. Про це OBOZ.UA розповіла заступниця голови правління Глобус Банк Анна Довгальська.

«Штучний інтелект лише посилює небезпеку. Завдяки йому повідомлення стають переконливішими, дзвінки — реалістичнішими, а самі атаки — набагато швидшими», — прокоментувала банкірка.

Завдяки ШІ зловмисники можуть персоналізувати атаки, використовуючи відкриті дані з соцмереж, месенджерів, робочих профілів чи публічних світлин. У повідомленнях часто згадують місце роботи людини, ім'я керівника, недавні поїздки чи звичні сервіси, якими вона користується.

Цікаво, що загальна кількість шахрайських операцій із платіжними картками у 2025

році зменшилася на 5% і становила 256 тис. випадків (дані Національного банку України). Водночас:

- сума збитків зросла майже на чверть і сягнула 1,4 млрд грн;
- середній розмір однієї шахрайської операції збільшився на 30% — до 5536 грн;
- 83% усіх шахрайських транзакцій здійснювалися через інтернет;
- 90% збитків були спричинені саме соціальною інженерією.

Які схеми шахрайства найчастіше застосовують

Найпоширенішою залишається схема дзвінків і повідомлень нібито від представників банків, операторів зв'язку чи державних органів. У таких випадках людину намагаються налякати:

- «підозрілою операцією»;
- блокуванням рахунку;
- необхідністю «терміново врятувати кошти».

Суть маніпуляції — суто психологічний тиск. Під впливом страху жертви самі передають реквізити карток, CVV-коди чи паролі з SMS.

Окремою загрозою став AI-фішинг. Шахраї створюють фальшиві сайти банків, маркетплейсів, служб доставки та благодійних фондів, які майже не відрізняються від оригіналів. За словами Довгальської, понад 80% сучасних фішингових листів уже містять ознаки використання штучного інтелекту.

Банкірка також звернула увагу на поширення технологій deepfake. Зловмисники можуть імітувати голос і відео реальних людей, використовуючи короткі аудіозаписи з соцмереж або месенджерів.

«У найпростіших випадках людині телефонують від імені родича чи знайомого й просять терміново переказати гроші. У складніших схемах можуть підробити голос керівника компанії та вимагати негайного платежу», — пояснила Довгальська.

За оцінками експертів, у деяких атаках із використанням ШІ рівень переходів за

фішинговими посиланнями може досягати 54%, тоді як у звичайному масовому фішингу цей показник становить лише близько 2,7%.

Як уберегтися від ШІ-шахрайства

Українцям радять дотримуватися кількох простих правил цифрової безпеки. Головна мета шахраїв — змусити людину самостійно передати доступ до коштів або підтвердити операцію. Щоб знизити ризики, варто:

- нікому не повідомляти CVV-код, PIN-код, одноразові паролі з SMS та дані для входу в онлайн-банкінг;
- не переходити за підозрілими посиланнями з SMS, месенджерів чи електронної пошти;
- уважно перевіряти адресу сайту перед введенням даних картки;
- користуватися лише офіційними застосунками з App Store або Google Play;
- завершувати розмову, якщо «співробітник банку» вимагає термінових дій або переказу коштів;
- перевіряти прохання про переказ грошей через інший канал зв'язку, навіть якщо воно надійшло від знайомої людини;
- увімкнути двофакторну автентифікацію для банківських застосунків, пошти та месенджерів;
- ідентифікувати SIM-картку у свого мобільного оператора, щоб зменшити ризик викрадення фінансового номера.

Довгальська наголошує, що головними інструментами шахраїв залишаються поспіх і психологічний тиск. Якщо людину лякають блокуванням рахунку, втратою грошей або змушують діяти «негайно», варто зупинитися та перевірити інформацію.

Теги: искусственный интеллект | Аферисты | Аферисти | Шахраї | Мошенники

Максим Левченко

ВИПУСКОВИЙ РЕДАКТОР

21 травня 2026 г., 17:34 Переглядів: 1973 Коментарі: 1

Коментарі: