

Захист від шахрайства у Великобританії



Схеми шахрайства, пов'язані з соціальними виплатами (UC) та державними послугами

Мета шахраїв — Universal Credit, Child Benefit та ін. соціальні виплати

Як працює схема:



Неліцензовані «посередники»

обіцяють «гарантовану» допомогу або аванс (Advance Payment)



Збір персональних даних

NINO, банківські реквізити, доступ до GOV.UK / One Login



Фальсифікація заявки

недостовірні дані про інвалідність, утриманців чи оренду



«Комісія» і зникнення

вилучають 40–50% отриманого авансу й зникають

ЩО ВТРАЧАЄ ЖЕРТВА

40–50%

отриманого авансу шахраї забирають як «комісію» — а борг перед DWP лишається на жертві.

МОДУЛЬ 1

Advance Payment Fraud — покроково

Кейс

1

Первинний контакт оголошення в соцмережах: «£1,500–3,000 безповоротно за 24 години»

2

Передача даних жертва віддає NINO та реквізити Monzo / Lloyds «для перевірки»

3

Фальсифікована заявка шахраї подають фейкову заявку на UC і запитують негайний аванс

4

Присвоєння коштів DWP платить £2,100 → шахраї вимагають £1,000 «комісії» на Revolut

5

Правові наслідки DWP виявляє підробку та виставляє жертві борг на повні £2,100

Кваліфікація та нові повноваження

Юридична кваліфікація



Social Security Administration Act 1992

ss. 111A, 112 — незаконне отримання виплат за неправдивими даними



Fraud Act 2006 (s. 2)

шахрайство шляхом неправдивого представлення фактів



Наслідки для потерпілого

Overpayment Recovery; Administrative Penalty 50% (£350—£5,000); Prosecution

Нові повноваження DWP (2025–2026)



Public Authorities (Fraud, Error and Recovery) Act 2025

Новий британський закон (прийнятий 02.12.2025), який розширює повноваження DWP щодо боротьби з шахрайством, помилками у виплатах і поверненням переплат.



Eligibility Verification Notices (EVN)

DWP може зобов'язати банк перевірити рахунки одержувачів виплат на ознаки порушення умов і повідомити про збіги — без передачі виписок.



Direct Deduction Orders

Якщо людина не виходить на контакт щодо погашення підтвердженої переплати, DWP зможе списати кошти прямо з банківського рахунку без рішення суду (з жовтня 2026).

Практичний висновок: механізм стягнення переплати тепер жорсткіший — тим важливіше не передавати свої дані посередникам.

Що робити потерпілому

1

Повідомити DWP → **Journal + 0800 854 440**

- 1) Заявити, що claim подано без вашого відома, вимагати зупинити виплати і не) стягувати advance з вас.
- 2) Змінити пароль до Gov.UK account, попередити зміну банківських реквізитів шахраєм.

2

Подати звіт до Report Fraud

→ **0300 123 2040** або **reportfraud.police.uk**

Офіційно зареєструвати злочин і отримати **crime reference number**. Це додатковий доказ для DWP, що ви — жертва identity fraud, а не боржник.

3

Звернутися до банку → **159**

(Stop Scams UK — з'єднає з вашим банком напряму)
Заблокувати картку, зупинити переказ, захистити рахунок.

4

Додатково:

- змінити паролі: Gov.UK, email, банківському App;
- увімкнути 2FA скрізь, де можливо;
- зберегти всі докази (скріни повідомлень, номери телефонів, електронні листи).



Чому важливо повідомляти?

Банк — єдиний, хто може **зупинити рух грошей у реальному часі**.

DWP — щоб шахрай не встиг **змінити реквізити для наступної виплати** чи подати **фейкові зміни в claim**.

Action Fraud — не зупиняє нічого, але дає **юридичний документ**, на який спираються всі інші установи у подальшому (банк, DWP, страхова, суд).

ЕНЕРГЕТИКА ТА КОМУНАЛЬНІ ПОСЛУГИ

Шахрайство навколо енергопослуг та виплат на оплату рахунків.

Як працює схема:



Фішинг від імені Ofgem і постачальників

British Gas, Octopus, EON ...: «оформити субсидію» чи «повернути переплату»



Фальшиві інспектори лічильників

вимоги сплатити «негайну заборгованість» (Smart Meter)



Загроза відключення

тиск відключенням або лічильником з передплатою (Prepayment Meter)



Cost of Living Payments та Energy Bills Support Scheme — закриті (з 2024 р.).

Будь-яка «нова виплата Cost of Living» у 2025–2026 — це шахрайство.

3 масштабних схем зараз діє Warm Home Discount — £150.

Фальшиве повернення коштів від електропостачальника

Фішинг (phishing) — це вид шахрайства, при якому зловмисники намагаються обманом змусити людину поділитися конфіденційною інформацією (паролями, даними банківських карток, PIN-кодами), видаючи себе за відомі та надійні організації.

1 Фішинговий гачок: SMS від «Octopus Energy: вам компенсація £350 — перейдіть за посиланням»

2 Крадіжка даних: посилання веде на копію сайту; жертва вводить картку та CVV

3 Соціальна інженерія: за 15 хв дзвонить так звана «служба безпеки банку» (Caller ID Spoofing) про «підозріле списання»

4 Крадіжка коштів: переконують перевести на «безпечний рахунок» (Safe Account) → викрадають £4,200

Юридична кваліфікація



Fraud Act 2006 (s. 2)- шахрайство шляхом неправдивого представлення фактів — основна кваліфікація фішингу.

Коли шахрай телефонує чи пише від імені British Gas, EDF, Octopus чи іншого постачальника й вимагає «оплатити борг», щоб уникнути відключення, — це кримінальне шахрайство шляхом неправдивого представлення, за яке загрожує до 10 років ув'язнення.



Computer Misuse Act 1990- несанкціонований доступ до комп'ютерних систем і банківських даних.

Якщо шахрай через фішинговий лист чи фейковий сайт «постачальника» отримав доступ до вашого онлайн-акаунту, банківського застосунку чи облікових даних smart meter — це окремий злочин несанкціонованого доступу, який додається до основного звинувачення.



Electricity Act 1989 / Gas Act 1986 + Rights of Entry Act 1954

миттєве відключення неможливе; загроза «негайного відключення» суперечить закону.

Жоден справжній постачальник не може відключити вам газ чи електрику «сьогодні» або «за годину»: за законом потрібен ордер мирового судді (magistrates' court warrant) і мінімум 7 днів письмового попередження, тож будь-яка погроза «негайного відключення» по телефону = 100% scam!

Що робити потерпілому

1

Переслати фішинг

SMS → 7726 / E-mail → report@phishing.gov.uk

Деталі: Переслати фішинг — підозрілу SMS про «борг за газ/світло» перешліть безкоштовно на номер 7726 (літери SPAM на клавіатурі), а фішинговий email — на report@phishing.gov.uk; це передасть шахрая до NCSC (National Cyber Security Centre - Національний центр кібербезпеки) для блокування номера/сайту, **але вашу справу не розслідує.**

2

Передали банківські дані

Телефонувати до банку — 159 (Stop Scams UK)

Деталі: якщо ви ввели дані картки чи online banking на фейковому сайті «постачальника» або назвали їх по телефону, негайно телефонуйте — вас з'єднають напяму з вашим банком, щоб заблокувати картку і зупинити спробу списання, поки шахрай не встиг ними скористатися.

3

Втрачено кошти

Action Fraud 0300 123 2040 → crime reference number

Деталі: якщо гроші вже зписано з рахунку (ви оплатили «борг» чи переказали на «безпечний рахунок»), телефонуйте в Action Fraud і обов'язково отримайте crime reference number — без нього банк не запустить процедуру відшкодування, а страхова та DWP не визнають вас офіційно жертвою злочину.

4

Спір з постачальником

Energy Ombudsman — лише спори з реальним постачальником.

Пояснення: Energy Ombudsman розглядає лише скарги на реального постачальника (British Gas, Ocorpus тощо), тому туди звертайтеся, якщо виникли проблеми саме з постачальником-постачальником (неправильний борг у білінгу, відмова визнати шахрайство третьої особи); проти самого шахрая Ombudsman нічого зробити не може.



APP fraud / PSR

Якщо ви самі переказали гроші на «безпечний рахунок» — це авторизований платіж (Authorised Push Payment / APP fraud).

Банк зобов'язаний розглянути відшкодування за правилами PSR —більш детально Модуль 6.

Пояснення: коли ви **самі** натиснули «переказати» (Authorised Push Payment), з 7 жовтня 2024 року діють нові правила Payment Systems Regulator: банк зобов'язаний розглянути заяву протягом 5 робочих днів і відшкодувати до **£85 000**, якщо ви не діяли з грубою недбалістю; це головна юридична підстава вимагати гроші назад.

Благодійність та гуманітарна допомога

Фейкові благодійні збори та краудфандинг.

Суть схеми та ризики:



Незареєстровані «благодійні» організації

фейкові краудфандингові кампанії — GoFundMe, JustGiving, соцмережі



Копіювання реальних історій

постраждалі від війн чи катастроф — для емоційного тиску



Підроблені реквізити

фальшиві Registered Charity Number та QR-коди на вуличних зборах



Вивід коштів

на приватні банківські або криптовалютні рахунки організаторів



ЧЕРВОНИЙ ПРАПОРЕЦЬ

Тиск терміновістю збору + реєстраційний номер, що не збігається з офіційним реєстром.

Перевіряйте організацію лише в Charity Commission Register на GOV.UK (пошук за назвою або номером).

Фейковий гуманітарний збір

1

Публікація кампанії

сторінка «на термінову медичну допомогу дітям у зоні конфлікту»

2

Реквізити для довіри

вказується вигаданий номер реєстрації в Charity Commission

3

Збір і виведення

£18,000 через GoFundMe та прямі перекази → вивід через криптобіржу

4

Викриття

постраждалі нічого не отримують; підробку виявляють при аудиті

Юридична кваліфікація (УК)



Charities Act 2011

Фальшивий статус зареєстрованої організації; ліцензування вуличних зборів — також House to House Collections Act 1939 (частина норм Charities Act 2011 щодо публічних зборів досі не введена в дію).

Вуличні збори коштів вимагають ліцензії від місцевої ради за Police, Factories, &c. (Miscellaneous Provisions) Act 1916 — тож збирач без бейджа з номером ліцензії або з підробленою емблемою «Red Cross / Cancer Research UK» = майже завжди SCAM.



Fraud Act 2006 (s. 2)

Видавання себе за зареєстровану організацію (false representation)- S. 4 (abuse of position) .

Коли шахрай вигадує неіснуючу «благодійність» чи прикривається іменем реальної організації, щоб виманити донат, — це false representation з покаранням до 10 років; при цьому s. 4 (abuse of position) тут не застосовується, бо стосується лише реальних інсайдерів (наприклад, справжнього trustee, який краде з каси власного фонду), а не тих, хто створив фейкову «charity» з нуля.

Покроковий алгоритм

1

Перевірити організацію

ТІЛЬКИ через офіційний реєстр Charity Commission Register на GOV.UK. Далі вводите назву або charity number зі збірної листівки/сайту/GoFundMe-сторінки: якщо організації там немає, або її номер належить зовсім іншій справжній charity — це стовідсотковий скам, і жоден «красивий сайт», емоційні історії, фото з дітьми чи «підтримка блогерів» не замінюють цю перевірку.

2

Повідомити платформу

Якщо ви донатили через **GoFundMe, JustGiving, Facebook Fundraisers, PayPal Giving Fund**, першою чергою відкривайте claim саме там (кнопка «Report fundraiser» / «Contact support»), бо це найшвидший шлях повернути гроші без поліції та суду — платформа сама заморожує збір і починає внутрішнє розслідування.

3

Поскаржитися

Паралельно подавайте два звернення: у **Charity Commission** через форму «Report a serious concern» на GOV.UK (вони можуть закрити фейкову charity і заморозити рахунки), і в **Report Fraud** через reportfraud.police.uk або 0300 123 2040 (отримуєте crime reference number, який потрібен для банку, страхової та будь-яких подальших дій).



ГАРАНТІЇ ПЛАТФОРМ

GoFundMe Giving Guarantee

Якщо ви задонатили в **особистий збір** (personal fundraiser, не charity) і виявилось, що це скам, GoFundMe повертає вам до **£1000 протягом 1 року** з дати донату; для цього треба подати заявку через їхню форму «Request a refund».

JustGiving

Гарантії повернення НЕМАЄ.

Платформа не компенсує донорам втрачені кошти, натомість вона мінімізує ризик на вході: приймає збори тільки від charity, зареєстрованих у Charity Commission (або зборів на користь таких charity), тож перевірка відбувається **до** донату, а не після..

Шахрайство: онлайн-торгівля та кур'єрська доставка

Суть схеми та ризики:

Facebook Marketplace, Vinted, eBay: «покупець» надсилає підроблений скриншот оплати; або SMS від Royal Mail / Evri / DPD / DHL про «мити» за доставку £1.45–£2.99, посилання веде на копію сайту, де крадуть дані картки.



За даними UK Finance Annual Fraud Report 2026, у 2025 році в Британії зафіксовано понад 4 млн підтверджених випадків платіжного шахрайства із загальними збитками £1,28 млрд (+4% до 2024). Найпоширеніша схема за кількістю випадків серед APP-шахрайства — **purchase scams** (71% усіх APP-кейсів): фейкові оголошення на маркетплейсах і соцмережах. Найбільші збитки приносять **investment scams** — £221,5 млн (+40%).



Криптовалютні схеми — тренд зростання.

«Гарантовані» платформи для торгівлі Bitcoin/Ethereum з фейковими графіками, де жертва бачить, як її «баланс» росте, а вивести кошти неможливо.

Фейкові «AI-trading bots», які нібито заробляють 5-10% на день.

«Крипто-експерти» в TikTok, Instagram, Telegram, які ведуть у закриті групи з «сигналами».

Investment scams: будь-яка «гарантована» висока дохідність, тиск часом та пропозиції в WhatsApp/Telegram від «брокерів» — це майже завжди **SCAM**, а справжність компанії треба перевіряти лише через офіційний реєстр **FCA** (register.fca.org.uk) ще ДО переказу коштів.

Якщо гроші вже втрачено — негайно телефонуйте в банк **(159)** і в **Report Fraud (0300 123 2040)** для отримання crime reference number, після чого банк зобов'язаний розглянути відшкодування за правилами PSR (до £85 000 з жовтня 2024 р.).

МОДУЛЬ 4 · КЕЙС ТА ПРАВОВА БАЗА

Кейс: фішинг під виглядом Royal Mail / Evri та інших відомих кур'єрських служб

1

Очікування посилки

SMS: «Royal Mail: посилку затримано через несплачений збір £1.65»

2

Введення реквізитів

потерпілий вводить дані картки для сплати £1.65

3

Прив'язка токена

картку прив'язують до Apple Pay / Google Pay на пристрої шахрая

4

Крадіжка

за 2 години — серія покупок техніки на суму £3,100

Юридична кваліфікація (UK)



Consumer Rights Act 2015 захищає покупця у відносинах із професійним продавцем (trader), але НЕ поширюється на угоди між приватними особами (private sale) — ключове застереження для Marketplace.

Якщо ви купили щось у **бізнес-компанії** (фіктивний магазин або trader на eBay/Amazon) і товар виявився бракованим або не таким, як описано, закон дає право на повернення грошей, але якщо продавець — **звичайна людина на Marketplace, Vinted чи інших майданиках** (private sale), цей захист **НЕ діє**, і повертати гроші доведеться через суд або взагалі ніяк.



Consumer Credit Act 1974 (s. 75) солідарна відповідальність банку £100–£30,000 (кредитна картка).

Тобто оплата **кредитною картою** товару вартістю £100–30 000 автоматично робить банк **співвідповідальним** разом із продавцем, тож у разі шахрайства чи браку гроші повертає банк; але цей захист **не працює на 100%**, якщо ви платили дебетовою картою (там є лише слабший Chargeback) або **через посередника** (PayPal, Marketplace, Klarna).

Покроковий алгоритм

1

Платити захищено

кредитна картка (захист Section 75) або PayPal Goods and Services

2

Перевіряти доставку

ВИКЛЮЧНО в офіційному додатку кур'єра за трек-номером — не за посиланням із SMS

3

При списанні — до банку

процедура Chargeback або позов за Section 75



SECTION 75 vs CHARGEBACK

Кредитна картка = Section 75

захист за законом, £100–£30,000.

Дебетова картка = лише Chargeback

добровільна схема, не закон.

Суть схем:



Нерухомість

фальшиві лендлорди, незаконна суборенда, обхід схем депозитів (TDS/DPS/MyDeposits), підробка EPC / Gas Safety.

шахраї видають себе за власників (лендлордів) чужого житла і збирають з орендарів депозити та передоплату за квартиру, яку не мають права здавати; або незаконно здають орендоване житло в суборенду без згоди справжнього власника; або беруть з орендаря депозит і не реєструють його в жодній з трьох державних схем захисту (TDS, DPS, MyDeposits), як цього вимагає Housing Act 2004, Renters' Rights Act 2025 — тож у момент виїзду просто зникають з грошима, які орендар уже не може повернути через офіційний arbitrator.



Працевлаштування та візи

Продаж недійсних Certificate of Sponsorship (COS), «гарантовані візи», залучення до схем «грошових мулів» через відкриття/передачу рахунків Monzo / Revolut. Особливо гостра тема — care worker візи.; хвиля care worker віз 2023–2025.

Схема «грошовий мул» через банк

Потерпілий, 22 роки, знайшов у Telegram-групі вакансію «Remote Data Entry», £2 500/міс, «без англійської». «Роботодавець» пояснив: «Клієнти переказуватимуть тобі гроші, ти переказуватимеш 90% у крипті, 10% лишаєш собі». Через три тижні Monzo заблокував рахунок. Виявилося: гроші, що надходили, — від жертв інших шахрайств.

Молодого чоловіка НЕ звинуватили у злочині (він був жертвою), але на його ім'я занесли мітку CIFAS (Misuse of Facility) на 6 років. Ця мітка напругу блокує: відкриття будь-якого банківського рахунку, кредити, страхові розстрочки, перевірки при працевлаштуванні. Опосередковано ускладнює оренду житла (через tenancy referencing). Потерпілий не міг відкрити навіть простий поточний рахунок протягом 2 років, поки не оскаржив мітку через Financial Ombudsman.

Юридичний ризик: використання власного рахунку для транзиту чужих коштів кваліфікується як money laundering (POCA 2002, ss. 327–329) — до 14 років ув'язнення. Навіть невільна жертва отримує мітку CIFAS. Її можна оскаржити (SAR → банк → CIFAS/FOS), але це займає місяці.

Схема шахрайства з візовими спонсорствами у секторі care work за Skilled Worker visa

У 2022–2024 роках, після включення посади care worker до Shortage Occupation List, десятки тисяч мігрантів стали жертвами організованої схеми: ліцензовані care agencies або їхні посередники незаконно стягували з іноземних працівників **£8 000 – £15 000** за Certificate of Sponsorship (CoS), хоча закон прямо це забороняє. Після прибуття в UK з'ясовувалося, що реальних робочих годин немає, компанія-спонсор існує лише формально, або її ліцензію вже відкликано — Home Office у 2024–2025 роках позбавив ліцензій **понад 470 роботодавців** у секторі соціальної допомоги. Наслідок для мігранта — правовий вакуум: 60 днів на пошук нового спонсора, інакше — статус overstayer і депортація.

У жовтні 2025 року розслідування **BBC Panorama** зафіксувало продаж CoS коventрійською агенцією за £15 000 готівкою, після чого Home Office офіційно підтвердив, що такі дії підпадають одночасно під три кримінальні статті: Fraud Act 2006 (s. 2) — до 10 років, Immigration Act 1971 (s. 25) — до довічного ув'язнення (з 28.06.2022 за Nationality and Borders Act 2022; раніше — 14 років), Proceeds of Crime Act 2002 (ss. 327–329) — до 14 років.

CIFAS (Credit Industry Fraud Avoidance System) — це найбільша британська некомерційна база даних із запобігання шахрайству, яка об'єднує понад **700 організацій**: усі великі банки, будівельні товариства, страхові компанії, телеком-оператори, кредитні брокери, деякі роботодавці та державні органи (включно з DWP і HMRC). Учасники обмінюються між собою даними про підозрілу активність — і саме тут з'являється «мітка».

Що таке «мітка CIFAS» (CIFAS marker)
Це запис у базі National Fraud Database про людину, чий дані пов'язані з шахрайством — **як жертви, так і виконавця**. Мітку ставить банк або інша організація-учасник, коли фіксує підозрілу активність. Після цього **всі інші організації бачать її при будь-якій перевірці особи**: коли ви відкриваєте рахунок, берете кредит, оформлюєте страховку, іпотеку, договір на телефон, а іноді і при tenancy referencing чи працевлаштуванні у фінансовому секторі.

ТОП-3 СХЕМИ ОРЕНДНОГО ШАХРАЙСТВА В АНГЛІЇ

СХЕМА 1

Фантомна оренда

Як виглядає:

- Оголошення на Facebook, OpenRent або Gumtree про квартиру помітно нижче ринкової ціни; гарні фото (часто вкрадені з іншого оголошення).
- «Лендлорд за кордоном» (або інший привід) уникає перегляду й просить holding deposit «щоб зарезервувати».
- Після переказу — квартира «раптово недоступна», лендлорд зникає.

Червоний прапорець: гроші просять ДО того, як ви побачили квартиру своїми очима.

ЯК УНИКНУТИ

Не платіть жодного пенса, поки не подивилися житло особисто і не підписали договір.

СХЕМА 2

Фейковий агент / «подвійна здача»

Як виглядає:

- Правдоподібне «агентство» рекламує РЕАЛЬНУ квартиру, показує її вам особисто.
- Використовує справжнє ім'я власника (перевірка Land Registry не рятує) і фальшиве членство Propertymark.
- Просить оренду за 6 місяців наперед + великий депозит.
- У день заселення — немає ключів; на ту саму квартиру приходять ще 10–20 орендарів.

Червоний прапорець: вимагають велику передоплату (місяці наперед) або депозит понад 5 тижнів.

ЯК УНИКНУТИ

Депозит МАКСИМУМ 5 тижнів оренди (за законом), holding deposit — максимум 1 тиждень; більше — ознака шахрайства.

СХЕМА 3

Депозит «повз схему»

Як виглядає:

- Приватний лендлорд бере депозит готівкою чи переказом «на руки», не вносить його в державну схему захисту (DPS, TDS або MyDeposits).
- У день виїзду — знаходить фейкові «пошкодження» і відмовляється повертати депозит.
- Іноді «лендлорд» — насправді суборендар, який здав чужу квартиру без дозволу власника.

Червоний прапорець: лендлорд не дає письмового підтвердження, у якій схемі зберігається депозит.

ЯК УНИКНУТИ

Протягом 30 днів після заселення перевірте депозит на сайті DPS / TDS / MyDeposits за адресою; якщо його там немає — суд і компенсація 1–3 депозити.



Не платіть до перегляду й підписання. Holding deposit ≤ 1 тиждень, депозит ≤ 5 тижнів (Tenant Fees Act 2019); з 05.2026 передоплата оренди до підписання заборонена (Renters' Rights Act 2025).

Алгоритми захисту

Орендне шахрайство

- 1) Одразу подзвоніть у банк за 159 — зупинити переказ і відкрити справу про повернення грошей.
- 2) Повідомте про злочин у Report Fraud (0300 123 2040 або reportfraud.police.uk) і збережіть crime reference number разом з усіма скріншотами листування та оплати.
- 3) Якщо банк відмовив у поверненні — скарга до фінансового омбудсмена (0800 023 4567).

Шахрайство з візами

- 1) Негайно припиніть будь-які платежі й контакт із «консультантом» або «спонсором»; збережіть усі скріншоти листування, чеки, копії документів і реквізити, куди переказали гроші.
- 2) Заявіть у Report Fraud (**0300 123 2040** або reportfraud.police.uk) — отримайте crime reference number; якщо гроші переказали через банк, одразу подзвоніть у банк за **159**, щоб спробувати зупинити платіж.
- 3) Візьміть за потреби безкоштовну кваліфіковану консультацію з доступного переліку благодійних організацій Великобританії у сфері імміграційного права.
- 4) Перевіряйте будь-якого нового радника в офіційному реєстрі IAA (portal.immigrationadviceauthority.gov.uk).

Як діють шахраї

Суть схем: APP-фрод (Authorised Push Payment — жертва сама переказує гроші), імперсонація банків/поліції/HMRC, продаж фейкових автостраховок («Ghost Broking»), клонування голосу через AI (deepfake voice/video).

Способи обману:



Переказ під тиском

Вас переконують самому переказати гроші.

Шахрай тисне терміновістю чи страхом («грошам загрожує небезпека», «треба діяти зараз»), і ви самі переказуєте кошти зі свого рахунку — на його рахунок. Це один із найпоширеніших видів шахрайства у 2025 році. Небезпечно тим, що переказ ви робите **власноруч**, тож банк спочатку не бачить у ньому нічого підозрілого.



Дзвінок «від банку чи поліції»

Лякають і просять «перевести на безпечний рахунок».

Телефонує «співробітник банку» або «поліцейський» і каже: «На ваш рахунок здійснюється атака, терміново переведіть гроші на безпечний рахунок». Номер на екрані виглядає справжнім (підроблений), голос упевнений. Насправді жоден банк і жодна поліція **ніколи** не просять переказати гроші на «безпечний рахунок» — це завжди шахрайство.



Фальшива автостраховка

Продають недійсний автополіс.

В Instagram, Facebook чи WhatsApp пропонують автостраховку за півціни («Cheap car insurance UK»). Ви платите, отримуєте документи, що виглядають як справжні. Але поліса в базі страховика немає — його ніколи не існувало. Наслідки: при перевірці поліцією або в ДТП — штраф £300, 6 штрафних балів, конфіскація авто і повна фінансова відповідальність за ДТП.



Підроблений голос чи відео

Шахрай імітує рідних за допомогою програм.

AI тепер може скопіювати голос будь-якої людини з коротких відео у соцмережах. Вам телефонує «син», «донька» чи «онук» — голос ідеальний, у сльозах: «Я потрапив у аварію, терміново потрібні гроші». Насправді це шахрай із програмою клонування голосу. Правило: **завжди покладіть слухавку і передзвоніть родичу/близькій людині самі** на її звичайний номер.

Фальшиві інвестиції та обман через почуття

Фальшиві інвестиції

- 1 Реклама**
«вигідні інвестиції» у соцмережах
- 2 Довіра**
«менеджер» показує підроблений екран зі «зростанням» грошей
- 3 Все більше**
ви вкладаєте дедалі більше
- 4 Пастка**
щоб «вивести», просять доплатити «податок» — і зникають

Ознака: гарантована висока дохідність + неможливість вивести гроші без «додаткових платежів».

Обман через почуття

- 1 Знайомство**
«партнер» у мережі уникає зустрічей і відеодзвінків
- 2 Довіра**
тижнями завойовує ваші почуття
- 3 «Біда»**
раптом просить терміново грошей
- 4 Втрата**
ви переказуєте — шахрай зникає

Ознака: людина, яку ви ніколи не бачили наживо (уникає відеодзвінка), просить гроші. Це завжди шахрайство, без винятків.



ЩО РОБИТИ: не переказуйте одразу — зупиніться й перевірте. Подзвоніть у банк за номером 159. Банк має розглянути повернення грошей.

Коли банк поверне гроші



Банк має повернути....

якщо вас обманом змусили переказати, а ви не були грубо необережні.

З 7 жовтня 2024 року в Британії діє новий закон: банк **зобов'язаний** повернути гроші жертвам обману, коли вони самі переказали кошти під тиском шахраїв (це називається APP-шахрайство). Раніше банки могли відмовити — тепер це їхній прямий обов'язок. «Грубо необережні» означає рідкісні випадки, коли клієнт ігнорував очевидні попередження банку і всі здорові сигнали.



Скільки...

до £85 000 за один випадок.

Це максимум за одну заяву про шахрайство. Якщо ви втратили менше — повернуть повну суму. Якщо більше — банк поверне £85 000, а решту можна доспробувати повернути через фінансового омбудсмена окремо (у нього ліміт компенсації — понад £450 000, переглядається щороку).



Як швидко...

зазвичай за 5 робочих днів; складні випадки — до 35 днів.

Банк розглядає більшість заяв швидко: п'ять робочих днів — це стандарт. Якщо справа складна (великі суми, багато переказів, треба перевірити з іншим банком) — до 35 робочих днів. Довше — тільки якщо ведеться поліцейське розслідування. **Порада:** якщо банк тягне довше без пояснення — просіть письмову відповідь і подавайте скаргу омбудсмену.



Що можуть утримати...

до £100 — але не з вразливих людей.

Це «франшиза» — невелика сума, яку банк має право не повертати з кожного випадку (принцип «власна пильність клієнта»). Якщо вкрали £5000 — повернуть £4900. **Але** якщо ви належите до вразливих людей — літня людина, з інвалідністю, у тяжкій життєвій ситуації, погано володієте англійською (це стосується багатьох новоприбулих українців) — банк **не має права** утримувати ці £100. Повертають повну суму.



Що не повертають...

міжнародні перекази. Якщо банк відмовив — скарга фінансовому омбудсмену.

Закон захищає тільки перекази **всередині Британії** (Faster Payments, CHAPS). Якщо гроші пішли за кордон, у криптовалюту або готівкою — банк не зобов'язаний повертати. **Але** відмова банку — це не кінець: скаржитесь у безкоштовну незалежну службу **Financial Ombudsman Service (0800 023 4567)** — вона розгляне вашу справу заново, і приблизно у 40% випадків приймає рішення на користь клієнта.

Поради проти шахрайства з автострахуванням

1. **Купуйте страховку лише через перевірені канали.** Це офіційні сайти страхових компаній (Admiral, Aviva, Direct Line, LV=, Churchill) або великі порівняльники (Confused.com, MoneySuperMarket, Compare the Market, GoCompare). **Ніколи не купуйте через Instagram, TikTok, WhatsApp, Facebook або оголошення в українських Telegram-групах** — це головне джерело фейкових полісів у 2025 році.
2. **Перевірте поліс у базі askMID.** Через 24 години після оформлення зайдіть на **askmid.com** і перевірте, чи ваше авто в базі. Це офіційна база всіх застрахованих авто у Британії (Motor Insurance Database). Якщо вашого авто там немає — поліс фейковий. Перевірка безкоштовна і займає 30 секунд.
3. **Якщо ціна набагато нижча за ринкову — це шахрайство.** Реальна страховка для молодого водія в Лондоні коштує £1500–£3000 на рік. Якщо вам пропонують за £400–£600 — це «ghost broking». Порахуйте: справжня страхова не буде працювати собі у збиток. Правило: якщо дешевше на 40–50% від найдешевшої пропозиції на порівняльнику — це фейк.
4. **Перевіряйте «брокера» в реєстрі FCA.** Легальні страхові брокери зареєстровані у **Financial Conduct Authority**. Перевірити можна на **register.fca.org.uk** за назвою компанії або ім'ям брокера. Немає в реєстрі — не купуйте, навіть якщо сайт виглядає професійно.
5. **Ніколи не платіть готівкою чи переказом «на карту приватної особи».** Легальна страхова приймає оплату лише **на рахунок компанії** (business account) — картою або через їхній офіційний платіжний шлюз. Прохання переказати «на Revolut Івана», «family and friends» або готівкою — 100% шахрайство.



Куди звертатися

Insurance Fraud Bureau (IFB) — гаряча лінія: **0800 422 0421** (безкоштовно, анонімно, повідомити про підозрілого брокера)

Report Fraud: 0300 123 2040 — якщо ви вже стали жертвою

FCA Consumer Helpline: 0800 111 6768 — перевірити, чи брокер зареєстрований

Як обманюють українців

Способи обману



Платний «спонсор» чи віза

просять £600–1000 за «допомогу». За візу платити НЕ треба



Платна «допомога» з eVisa

оформлення eVisa та подовження — безкоштовні на gov.uk



Фейкові «консультанти»

беруть гроші, часто не маючи права давати поради



Фейкова робота і збори

«грошові мули» та фальшиві збори «на війну»



ЧЕРВОНІ ПРАПОРЦІ

- просять гроші за спонсора чи візу
- просять переказ з поміткою «family and friends» — банк не поверне
- уникають відеодзвінка

Справжній спонсор отримує £350/міс від держави — доплат не просить.

Платний «спонсор»: як це виглядає

Що відбувається

1

Оголошення

у Telegram чи Facebook: «знайду спонсора і візу за 3 дні»

2

Оплата

просять £700 і саме з поміткою «family and friends»

3

«Спонсор»

бере гроші, але житла немає

4

Відмова

Home Office блокує заявку; гроші не повертають



ЯК ПЕРЕВІРИТИ

- попросить відеодзвінок і показ житла
- справжній спонсор отримує £350/міс — доплат не просить
- шукайте спонсора лише через офіційні організації

Закон і де взяти допомогу

Що каже закон



Обман — це злочин

піддроблені документи й фейкові поради караються законом



Поради з віз — лише від дозовлених

давати візові поради без дозволу — злочин. Перевіряйте радника в реєстрі IAA

Де взяти безкоштовну допомогу

1

Безкоштовні консультації

OPORA, Citizens Advice, Law Centres, JCWI (0800 160 1004)

2

Перевірити радника

реєстр IAA: portal.immigrationadviceauthority.gov.uk

3

Якщо втратили гроші

банк — 159; Report Fraud — 0300 123 2040



ГОЛОВНЕ: eVisa і подовження UPE — безкоштовні на gov.uk. За візу платити не треба.

«Ціна свободи — вічна пильність».

Томас Джефферсон
