**Як виявити шахрайство**

Один із найкращих способів захисту від шахрайства – це знати, на що слід звернути увагу, щоб виявити факт шахрайства. Ось на що вам слід звернути увагу та що робити:

● **Перевірте будь-який несподіваний контакт:** отримуючи незнайомі телефонні дзвінки, звичайні чи електронні листи, переконайтеся, що ви знаєте компанію чи особу, з якою спілкуєтеся. Ви можете переглянути контактні дані в офіційних документах або на їх веб-сайті, щоб перевірити, що до вас звертається особа на законних засадах.

● **Адреса електронної пошти**. Якщо ви отримали електронний лист, розгорніть верхню панель повідомлення та подивіться, від кого саме він надійшов. Може бути вказано, що це від Управління ліцензій на телебачення, але якщо ви клацнете або наведете курсор на ім’я, може виявитись щось інше. Якщо це шахрайство, то вихідна адреса може не збігатися з іменем відправника, мати помилки, випадкові числа або бути від одного з ваших контактів, який був зламаний.

● **Текстові повідомлення (СМС)** – сучасні шахраї підроблюють свої номери під такі, яким ви довіряєте, наприклад номер вашого банку. Шахрайське CМC може навіть з’явитися в тій самій кореспонденції, що й звичайні текстові повідомлення, які ви отримували раніше. Це відомо як «підробка номера». Про всяк випадок не натискайте посилання в СМС і не бійтеся звертатися безпосередньо до компанії, щоб перевірити, чи це справжнє повідомлення.

● **Якщо це звучить занадто добре, щоб бути правдою, зазвичай так і є.** Наприклад, відпочинок набагато дешевший, ніж ви очікували.

● **Особисті дані, повні PIN-коди та паролі** – це те, що жодна законна компанія не запитає у вас.

● **Швидкі рішення** - якщо вас змушують приймати рішення на місці, будьте обережні. Шахраї не хочуть, щоб ви мали час подумати про це. Будь-яка законна компанія, яка зателефонує вам, не буде проти, якщо ви передзвоните їй пізніше. Дзвоніть на номер телефону, який ви знайдете в листах від компанії або на зворотному боці картки.

**2.** **Види шахрайства**

Шахраї використовують різну тактику: від стуку у ваші двері до несподіваного електронного листа чи телефонного дзвінка.

Інтернет і розвиток цифрових комунікацій відкрили для шахраїв інші способи полювати на вас і красти інформацію. Можливо, ви стикалися з найпоширенішим типом шахрайства –спамом, у якому говориться, що вам надішлють гроші, або видають себе за представника HMRC чи вашого банку.

Однак, хоча деякі види фальшивих листів можна досить легко помітити та уникнути, інші є набагато складнішими та їх важко виявити.

**Поширені види шахрайства,** що діють останім часом**:**

*\* Будь ласка, зауважте: цей список не включає всі можливі шахрайства, все ще можуть бути інші.*

● [[**Шахрайські**](https://cfa.nhs.uk/resources/downloads/fraud-awareness/covid-19/COVID-19_SMS_and_Text_Message_Scams.pdf) **СМС щодо Covid**](https://cfa.nhs.uk/resources/downloads/fraud-awareness/covid-19/COVID-19_SMS_and_Text_Message_Scams.pdf) – шахрайство, яке було активним під час карантину, почало з’являтися знову. Ви отримуєте СМС на свій мобільний, яке повідомляє, що ви контактували з хворим на COVID і повинні натиснути посилання, яке потім запитає про ваші дані. Це шахрайство, інакше воно було б пов’язане з державним веб-сайтом.

[●](https://www.which.co.uk/news/article/beware-of-this-scam-text-offering-you-fake-government-energy-bill-support-aNkqp4d5ugIM) **[Шахрайство зі знижкою за електроенергію/газ](https://www.which.co.uk/news/article/beware-of-this-scam-text-offering-you-fake-government-energy-bill-support-aNkqp4d5ugIM)** – СМС на вашому мобільному говорить про те, що ви маєте право на знижку за пальне, тож клацніть посилання. Це шахрайство. Посилання вимагає ваших даних і не має нічого спільного з вашим власним постачальником енергії. Якщо ви отримали таке СМС, спершу зверніться до свого постачальника. Будь-яка справжня знижка буде зроблена через державну установу або безпосередньо від вашого постачальника.

Дізнайтеся більше про те, як уникнути енергетичного шахрайства та повідомити про нього [тут.](https://www.ofgem.gov.uk/avoid-and-report-energy-scams)

● [**Шахрайство з СМС від родича**](https://www.which.co.uk/news/article/notorious-hi-mum-and-dad-scam-spreads-from-whatsapp-to-text-message-an7N34c0gVbP)  – СМС на вашому мобільному телефоні, яке виглядає так, ніби воно надійшло від вашої доньки/сина/онуки/онука, де говориться, що їхній мобільний телефон пошкоджено або зламано, тому вони пишуть з «телефона друга». Шахраї просять вас надіслати 800 фунтів за новий телефон на вказаний нижче рахунок (рахунок шахраїв). Якщо ви отримали подібне СМС, спочатку зателефонуйте вашому родичу та переконайтеся, що це правда.

● [**Шахрайство з криптовалютою**](https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams). Ви можете побачити рекламу криптовалюти у своєму Facebook із проханням надіслати гроші на рахунок із зазначенням, що це «хороша інвестиція». Це шахрайство. Якщо ви не впевнені, що це правда, не зв’язуйтеся з компанією.

● [**Шахрайство з кур’єром**](https://www.actionfraud.police.uk/a-z-of-fraud/courier-fraud) – ви отримуєте СМС про те, що для вас є посилка, але перед тим, як її доставити, вам треба заплатити, натиснувши на посилання. Це шахрайство, оскільки жодна справжня кур’єрська компанія не вимагає оплати.

● [**Шахрайство з HMRC**](https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-and-customs-examples#:~:text=Do%20not%20reply%20if%20you,gov.uk%20then%20delete%20it.) – CМС, дзвінки та електронні листи від “HMRC” є шахрайством. Цей відділ може лише писати вам поштою і ніколи не дзвонить, не пише СМС або email.

● [**Шахрайство з телевізійною ліцензією**](https://www.tvlicensing.co.uk/faqs/FAQ288) – ви отримуєте електронний лист про те, що ви повинні оплатити ліцензію на телебачення і клацнути посилання, щоб здійснити оплату. Якщо вам не пора платити або навіть якщо це справжній електронний лист, він надасть ваш власний контрольний номер. Якщо контрольного номера немає та в адресі електронної пошти є помилка у слові «ліцензія», це шахрайство,

● [**Щахрайські дзвінки загального характеру**](https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams) – якщо вам дзвонять на мобільний або стаціонарний телефон, але ви не впізнаєте номер або він анонімний, то радимо не приймати дзвінок. Ви також можете блокувати шахрайські дзвінки на своєму мобільному телефоні. Більшість провайдерів стаціонарного зв’язку мають «послугу блокування», то ж до вас надходитимуть лише справжні дзвінки.

**●** [**Шахрайство з розіграшем призів**](https://consumer.ftc.gov/articles/fake-prize-sweepstakes-lottery-scams#:~:text=You%20get%20a%20call%2C%20email,information%20to%20get%20the%20prize.). Якщо ви отримуєте поштою листа, такого як «розіграш призів», у якому повідомляється, що ви виграли (наприклад) 20 000 фунтів і повинні надіслати 20 фунтів, щоб отримати приз, — це безперечно шахрайство. Подрібніть лист, а потім викиньте його.

● [**Шахрайство**](https://www.which.co.uk/consumer-rights/advice/doorstep-scams-and-how-to-avoid-them-aWers5g8JA3V) **на порозі** – ще один вид шахрайства, коли хтось стукає у ваші двері і запитує, чи хочете ви, щоб на вашій території були проведені роботи. Наприклад, роботи в саду, прибирання під’їзду тощо. Або вони намагаються вам щось продати. Якщо до вас приходять, скажіть, що вас не цікавлять їхні послуги, і попросіть їх піти.

**3. Як захиститися від шахрайства**

Наступний крок до уникнення шахрайства — це знати, як захистити себе. Хоча деякі з цих порад є корисними взагалі, багато з них спрямовані на вашу безпеку в Інтернеті.

● **Ніколи не надавайте особисту інформацію**. Це може бути використано для викрадення вашої ідентичності та доступу до рахунків. Ніколи нікому не повідомляйте свій повний PIN-код або пароль. Ваш банк попросить вас скористатися сканером для читання карток або назвати кілька цифр вашого пароля, якщо він потрібен.

● **Переконайтеся, що всі ваші рахунки мають надійні паролі**. Не використовуйте той самий пароль для кількох рахунків і регулярно змінюйте їх.

**● Не робіть авансових платежів,** доки не переконаєтеся, що компанія, з якою ви маєте справу, є законною.

● **Якщо у вас є сумніви щодо фінансової компанії,** перевірте [реєстр регульованих компаній FCA](https://register.fca.org.uk/s/). Якщо вони не в реєстрі, не майте з ними справи.

● **Якщо у вас є сумніви щодо будь-якої іншої компанії,** ви можете знайти її на сайті [Companies House](https://www.gov.uk/government/organisations/companies-house), щоб дізнатися про їхню історію або пошукати відгуки в Інтернеті.

● **Використовуйте безпечні та захищені Wi-Fi-з’єднання** та уникайте публічних Wi-Fi. Ваше стандартне з’єднання 3G або 4G часто безпечніше, ніж у кав’ярні чи ресторані.

**4. Що робити, якщо ви стали жертвою шахраїв**

Якщо ви вважаєте, що вас ошукали, ось що вам слід зробити:

1. Негайно припиніть надсилати гроші. Якщо платіж налаштовано як прямий дебет, зв’яжіться зі своїм банком, щоб негайно його припинити.

2. Якщо ви стали мішенню шахраїв, навіть якщо ви не стали їх жертвою, повідомте про це на лінію підтримки споживачів Citizens Advice за номером **0808 223 1133** та скористайтеся [онлайн-інструментом для заяви](https://ssl.datamotion.com/form.aspx?co=3438&frm=scam&to=scamsaction).

Якщо ви вважаєте, що стали мішенню шахраїв, вам слід зібрати якомога більше інформації для доповіді та розслідування. Щоб дізнатися більше про те, як повідомити про шахрайство, відвідайте веб-сайт [Citizens Advice](https://www.citizensadvice.org.uk/consumer/scams/reporting-a-scam/).