



beforeitrugs

FOR PARENTS, SCHOOLS AND WORKPLACES

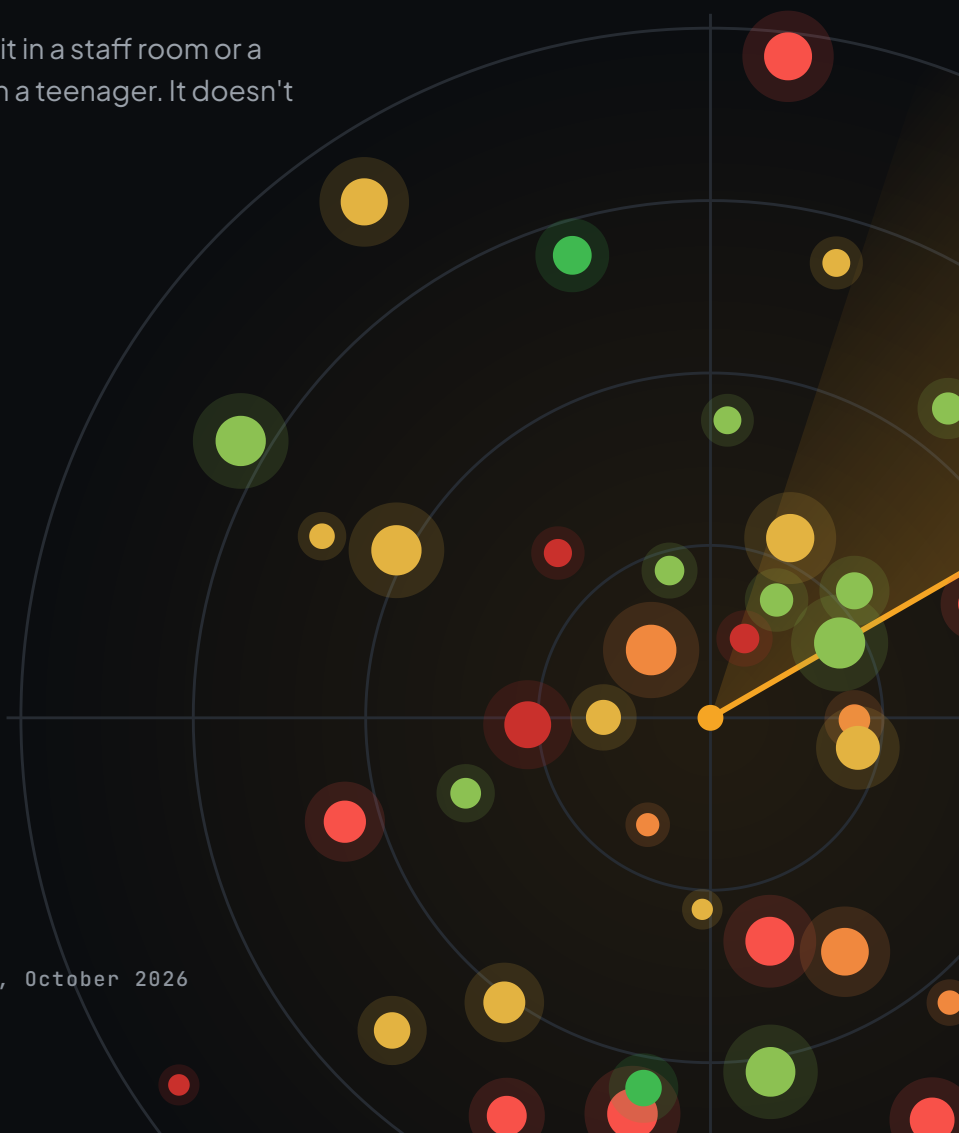
Crypto Scam Awareness Pack

The five crypto scams hitting people in the UK,
how to spot them, and where to report them

Plain English, no jargon. Print it, share it in a staff room or a parents' evening, or go through it with a teenager. It doesn't ask anyone to buy anything.

Free to print and share

Made by beforeitrugs.com
Checked against official UK sources, October 2026



Why crypto scams work, and how to use this pack

Crypto scams don't need you to be careless. They use the same tricks as every other fraud (trust, hurry and a promise) and add one thing that makes them worse: a crypto payment usually can't be reversed.

SCAM 1

Romance and pig butchering

A new online friend introduces a "platform" that keeps growing.

SCAM 2

Fake investment sites and apps

Slick adverts, fake dashboards and blocked withdrawals.

SCAM 3

Impersonation

Fake banks, fake police, fake support and clone firms.

SCAM 4

Recovery scams

"We can get your money back," for a fee.

SCAM 5

Fake airdrops and drainers

One click or one signature empties a wallet.

PAGE INSIDE

03	Romance and pig butchering
04	Fake investment platforms
05	Impersonation
06	Recovery scams
07	Fake airdrops and wallet drainers
08	The warning signs, all in one place
09	The one-page checklist
10	What to do and where to report
11	For teens: memecoin hype
12	Talking about it, and our sources

THE ONE RULE

Nobody genuine will ever ask for a crypto wallet's seed phrase (the 12 or 24 secret words) or rush you into sending money. Not a bank, not the police, not a regulator, not a friend you met online.

How to use it

- **Parents:** read pages 3 to 7 yourself, then go through page 11 with your teenager.
- **Schools:** pages 8, 9 and 11 work as a lesson starter or a printed handout.
- **Workplaces:** print page 9 for a noticeboard and page 10 for the people who handle money.

Everything here is general information about scams. It isn't financial advice and it doesn't tell anyone to buy, sell or hold anything.

REMEMBER 1

A crypto payment usually can't be pulled back by a bank, so checking first is the only protection that always works.

REMEMBER 2

Pressure, secrecy and fees to get your own money out are the scammer's tools, whatever the story.

REMEMBER 3

Report it, without shame: Report Fraud on 0300 123 2040, or Police Scotland on 101.

Romance and "pig butchering"

A friendship or romance that slowly turns into an investment. Police forces describe pig butchering as a long-term fraud that mixes romance, investment and crypto. The name comes from the idea of "fattening up" a victim before taking everything.

01

How it usually goes

- 1 **A stranger makes contact.** A dating app, a social media message, or a friendly text out of nowhere.
- 2 **Weeks of chat.** Kind, attentive, always available, and keen to move the conversation to WhatsApp or Telegram.
- 3 **Money comes up casually.** They mention they're doing well trading crypto, and offer to show you how.
- 4 **You're sent to a "platform".** A website or app that looks like a real exchange. A small first deposit seems to grow fast, and a small withdrawal works, to build trust.
- 5 **The pressure builds.** A "special opportunity" needs a bigger deposit, sometimes borrowed or from savings.
- 6 **The money won't come out.** Withdrawals need a "tax", "fee" or "verification deposit" first. Then the friend and the platform vanish.

MANY SMALL PAYMENTS

UK Finance found romance scams averaged 9.7 payments per case in 2025, more than any other scam type. Victims are drawn in bit by bit.

THE NUMBERS

£102 million

lost to romance fraud reported to Report Fraud in 2025, across 10,784 reports, up 29% on 2024. Police said many cases are linked to fake investment opportunities, including crypto.

City of London Police, May 2026

WARNING SIGNS

- You've never met, and they always have a reason not to video call
- They ask you to keep it secret
- The talk keeps turning to money
- The platform isn't on the FCA register
- You need to pay to withdraw your own money

IF IT'S HAPPENING TO SOMEONE YOU KNOW

Don't argue about whether the person is real. Look at the platform together, search its name on the FCA Warning List, and suggest one test: a full withdrawal with no fee. Then call their bank together.

Fake investment platforms

Adverts, videos and "account managers" selling crypto trading, AI bots or guaranteed returns. The website looks professional and the dashboard shows profits. The profits are made up.

02

How it usually goes

- 1 **An advert finds you.** Often on social media, often using a celebrity's photo or a fake news article. The FCA says scammers also target people searching for investments online.
- 2 **A friendly "account manager" calls.** They help you open an account, and may ask you to install an app that lets them see or control your screen.
- 3 **The balance climbs.** The FCA warns that scammers manipulate software to fake prices and returns.
- 4 **You're asked for more.** A bonus for topping up, a deadline, or a suggestion to bring in a friend or relative.
- 5 **The account closes.** When you try to withdraw, there's a fee, a delay or silence. The FCA says scammers may act quickly once you've invested, closing the account and taking the money.

The FCA's three questions

- ☐ Were you contacted out of the blue?
- ☐ Are you being pressured to invest quickly?
- ☐ Are the returns being promised unrealistic?

A yes to any of them is a reason to stop and check.

THE NUMBERS

£221.5 million

lost to investment scams paid by bank transfer in the UK in 2025, up 40%, across 14,893 cases. The largest category of these scams.

UK Finance Annual Fraud Report, June 2026

CHECK BEFORE YOU PAY

Look the firm up on the FCA Firm Checker and the FCA Warning List, and contact it only using the details listed there. The FCA issued 2,329 warnings about unauthorised firms and individuals in 2025.

FCA, April 2026

CELEBRITY ADVERTS

Famous faces in crypto adverts are very often used without permission. A real investment doesn't need a TV presenter to vouch for it in a pop-up.

IF YOU'VE ALREADY PAID IN

Stop paying, including any withdrawal fee. Remove any screen-sharing app they asked you to install. Call your bank on 159, then report it to Report Fraud or Police Scotland.

Impersonation: fake banks, police and support

The scammer pretends to be someone you already trust. The story changes, but the ask is the same: move your money somewhere "safe", or hand over the details that unlock it.

03

WHO THEY PRETEND TO BE	WHAT THEY SAY	THE TELL
Your bank	"Your account is under attack. Move your money to a safe account while we fix it."	No bank asks you to move money to keep it safe. Hang up and call 159.
The police	"We've arrested someone with your details. Your crypto is at risk."	Police will never ask for your seed phrase. Hang up and call 101 to check.
Crypto exchange or wallet support	A helpful reply or DM: "I can fix that, just verify your wallet here."	Real support never DMs first and never needs your seed phrase.
The FCA or government	A letter or email about compensation, a fine or a "frozen" account.	The FCA says it would never ask you to pay to get money back.
A real firm (a clone)	The right name, logo and reference number, but a different phone number or website.	Use only the contact details on the FCA register.
A celebrity	A video or post backing a crypto scheme or giveaway.	Faces and voices can be faked. Giveaways that need a deposit are scams.

HAPPENING NOW

In 2026 the Eastern Region Special Operations Unit warned UK crypto holders about calls from bogus police officers, followed by a second call from someone posing as a crypto company, trying to get victims' seed phrases.

ERSOU, March 2026

WHAT 159 DOES

If you get a call about your money, hang up and dial 159 from a phone. It connects you to your own bank's fraud line if your bank is part of the scheme, run by Stop Scams UK. Scammers can't easily fake a three-digit number.

Stop Scams UK

Recovery scams: the second scam

Someone who has just lost money is contacted by a "recovery firm", lawyer, investigator or even someone posing as police, offering to get it back for a fee. The FCA calls these recovery room scams, and warns the fees can add up to more than the first loss.

04

How it usually goes

- 1 **They find the victim.** Through a post about the loss, an advert for "crypto recovery", or a list of victims. The FCA says the original scammers may run the recovery room themselves.
- 2 **They sound official.** Case numbers, a UK address, a law firm letterhead, or a claim to work with the police or the government.
- 3 **They ask for a fee.** Described as a tax, a solicitor's fee or an admin charge. The FCA says the scam tends to involve cold calling and high pressure.
- 4 **Then another fee.** Each payment "unlocks" the next step, until the victim runs out or stops.

The tells

- They contacted you first, out of the blue
- Money up front, or a guarantee of success
- An offer to "hack" the scammer or "reverse" a transaction
- A request for your seed phrase, ID or remote access
- A Gmail, Yahoo or Hotmail address, which the FCA says recovery rooms often use

THE FCA'S POSITION

The FCA says it would never suggest you make payments to recover lost funds. If you're asked for a fee or bank details, end all contact and don't pay anything.

FCA, recovery room scams

THE HONEST TRUTH

A crypto payment on a blockchain can't be pulled back by anyone you pay. Money that does come back usually comes through your own bank, for a bank transfer you made to a scammer, or through a police investigation. Neither charges a fee.

IF YOU'VE BEEN HIT

Report it to Report Fraud, or Police Scotland on 101. Expect the "recovery" offers to follow, and ignore every one.

BEFORE REPLYING TO ANY OFFER OF HELP

Look the firm up on the FCA Firm Checker and call it only on the number listed there. If you can't find it, or it asks for anything up front, that's your answer.

Fake airdrops and wallet drainers

Aimed at people who already hold crypto in their own wallet app. A "free tokens" offer or a copy of a real website leads to one click or one signature that hands everything over.

05

How it usually goes

- 1 **Something free appears.** Tokens or NFTs land in the wallet unasked, or a post says "claim your airdrop before it ends".
- 2 **A link to a lookalike site.** It copies a real project, sometimes as the top paid result in a search.
- 3 **"Connect your wallet."** Connecting only lets the site see the wallet. The danger is the next step.
- 4 **"Sign to claim."** The transaction actually sends the wallet's tokens away, or hands over control of them. On Solana, as on most blockchains, a signed transaction can't be undone.

Other disguises

- Fake "revoke" or "wallet checker" sites, sent in a reply to someone asking for help
- Fake wallet apps with the right logo and the wrong publisher
- Trading bots that ask for a private key "to trade faster"

THE NUMBERS

\$84 million

stolen by wallet drainers in 2025 from about 106,000 victims, counting Ethereum-style networks only. That was down from about \$494 million in 2024. The tools keep changing.

Scam Sniffer 2025 report

HABITS THAT STOP IT

- Ignore tokens you didn't ask for. Don't visit their links.
- Reach crypto sites from a bookmark, never an advert or a DM.
- Read every wallet preview. Reject anything that moves tokens you didn't mean to.
- Keep most crypto in a wallet that never connects to sites.

IF A WALLET HAS BEEN DRAINED

Stop signing anything. Make a brand new wallet with a new seed phrase on a device you trust, and move whatever is left into it. Don't send anything back to the old wallet, then report it.

The warning signs, all in one place

Most crypto scams show at least two of these. One is enough to stop and check with someone you trust.

1	They contacted you first	A message, call, advert or text you didn't go looking for.	All five
2	There's a rush	A deadline, a "last chance", a threat that your money will be lost if you wait.	Investment, impersonation, airdrops
3	Returns that sound too good	Guaranteed profits, a fixed percentage a day, "can't lose".	Romance, investment
4	You have to pay to get paid	A fee, tax or deposit before a withdrawal, a prize or a recovery.	Romance, investment, recovery
5	They want your seed phrase	Or a private key, a one-time code, or remote access to your screen.	Impersonation, recovery, drainers
6	Keep it secret	Don't tell your bank, your family or your friends. Scammers isolate people.	Romance, impersonation
7	Move it somewhere "safe"	A "safe account", a "secure wallet", a "protected" address someone gives you.	Impersonation
8	You can't check who they are	Not on the FCA register, details that don't match it, only a chat app or webmail.	Investment, recovery
9	Something free needs a click	Unexpected tokens, a "claim" link, a giveaway that needs a deposit first.	Airdrops, impersonation
10	They offer to undo a loss	Hacking a scammer, reversing a transaction, guaranteed recovery.	Recovery

WHY CRYPTO MAKES IT WORSE

The FCA says crypto is generally not regulated by it, so you don't get the protections of the UK's financial regulation, such as the Financial Ombudsman Service or the Financial Services Compensation Scheme. And a blockchain payment can't be cancelled by a bank. Checking before you send is the only protection that always works.

Before you send money or crypto, or sign anything

Run through this every time. If you can't tick a line, stop and talk to someone you trust first.

- ☐ **I went looking for this.** Nobody contacted me out of the blue about it.
Unexpected calls, DMs, adverts and texts are where many scams start.

- ☐ **Nobody is rushing me.** I'd be happy to wait a day and decide tomorrow.
Real opportunities and real banks can wait. Scams can't.

- ☐ **I've checked the firm myself** on the FCA Firm Checker and the Warning List.
And I'm using the phone number and website from the register, not the ones I was sent.

- ☐ **Nobody has asked for my seed phrase,** private key, one-time code or remote access.
If they have, it's a scam. Every time.

- ☐ **I don't have to pay a fee to get money out.**
Fees to withdraw, unlock or recover money are a scam's way of taking more.

- ☐ **The returns are believable.** Nobody has guaranteed a profit.
Guaranteed, fixed or "can't lose" returns are a warning sign.

- ☐ **I can tell my family or bank about this** without being told to keep it secret.

- ☐ **I opened the website myself,** from a bookmark or by typing it, not from a link, advert or DM.

- ☐ **I've read what I'm signing** and nothing is leaving my wallet that I didn't intend.

- ☐ **I can afford to lose this amount completely.**
Crypto is high risk. Most memecoins go to zero.

GOT A CALL ABOUT YOUR MONEY?

Hang up. Call 159 to reach your bank, or the number on the back of your card.

THINK IT'S A SCAM?

Report Fraud: reportfraud.police.uk or 0300 123 2040. Scotland: Police Scotland on 101.

What to do and where to report

Act quickly, without blaming yourself or anyone else. Scams are built by organised criminals to fool careful people.

Where to report

England, Wales and Northern Ireland Report Fraud, which replaced Action Fraud in December 2025	Online: reportfraud.police.uk Phone: 0300 123 2040
In Scotland Police Scotland	Phone: 101 Emergency: 999
A firm was involved Financial Conduct Authority	Online: fca.org.uk/consumers/report-scam Phone: 0800 111 6768
Your bank's fraud line The Stop Scams UK service	Phone: 159
Free advice in England and Wales Citizens Advice consumer helpline	Phone: 0808 223 1133 In Welsh: 0808 223 1144
Advice in Scotland Advice Direct Scotland	Online: consumeradvice.scot Phone: 0808 164 6000
Advice in Northern Ireland Consumerline, on nidirect	Phone: 0300 123 6262

The first hour

- 1 Stop paying.** No more deposits, fees or "taxes", whatever they say.
- 2 Call your bank** if you paid by bank transfer or card. Use 159 or the number on your card.
- 3 Secure the wallet** if a seed phrase was shared or something odd was signed: make a new wallet with a new phrase and move what's left.
- 4 Save everything:** messages, numbers, websites, wallet addresses and transaction IDs.
- 5 Report it** to the right place on this page.
- 6 Ignore recovery offers.** They're the second scam (page 6).

LOOKING AFTER PEOPLE

Losing money to a scam can bring shame, anger and sleepless nights. Samaritans are free to call any time on 116 123. If trading feels like gambling that can't stop, the National Gambling Helpline (GamCare) is free, 24 hours a day, on 0808 8020 133.

THE TAX SIDE

A crypto loss can sometimes be claimed against Capital Gains Tax, and stolen crypto is treated differently from coins that became worthless. HMRC's guidance is on gov.uk. Check with HMRC or an accountant.

Memecoin hype: who's actually making the money?

Memecoins are crypto coins built around a joke, a meme or a trend. Anyone can make one in minutes. You'll see them in clips of people turning £50 into thousands. Here's what those clips leave out.

0.6%

Of 17,208 new Solana memecoins we followed for at least a day, 100 were still "standing": still trading properly and not down 90% from their high.

Before It Rugs records, as of 24 October 2026

93%

Of 753 coins we first checked after they'd left the launch site, 93% collapsed or ended their first day at least half below their high.

Before It Rugs records, as of 24 October 2026

How the hype is made

- **Early wallets buy first.** Often the people who made the coin, sometimes spread across lots of wallets so it doesn't show.
- **Then the noise.** Posts, clips, Telegram "calls" and paid promotion. Not all of it says it's paid.
- **The countdown.** "It's about to go to the moon, get in now." Hurry is the point.
- **Then the exit.** The early wallets sell to the people who arrived because of the noise. That's called a rug pull.

The FCA has taken criminal cases against social media influencers for illegal financial promotions. A big following doesn't make a post true.

Ask three questions

- 1 **Who bought before me,** and what happens when they sell?
- 2 **Who's paying for this post,** or getting something if I join in?
- 3 **What happens if it goes to zero?** Could I shrug that off?

IF SOMEONE ASKS YOU

To "hold" crypto for them, pass money through your bank account, or share a wallet's secret words: say no and tell an adult you trust. Moving money for strangers can get you into serious trouble.

OUR READ

Memecoins work more like a game of musical chairs than an investment. Most people who join late lose, and the people shouting loudest usually got in first.

Talking about it, and our sources

People who've been scammed often say nothing because they feel embarrassed. How the first conversation goes decides whether they come to you next time.

Openers that work

CURIOUS, NOT CROSS

"I keep seeing crypto adverts. Have you come across any? What do you make of them?"

MAKE IT SAFE TO TELL YOU

"If anyone ever pressures you over money, you can tell me. You won't be in trouble."

USE A REAL EXAMPLE

Pick one scam from pages 3 to 7 and ask how they'd spot it.

If someone tells you

- Thank them for telling you. That took courage.
- Don't blame. Scams are designed by professionals.
- Help them stop paying and call their bank.
- Help them report it (page 10).
- Warn them about recovery offers (page 6).
- Check on them in a few days, not just today.

Our sources

City of London Police, romance fraud figures for 2025, published May 2026 (via Report Fraud data)

UK Finance, Annual Fraud Report 2026 and press release, 15 June 2026, ukfinance.org.uk

FCA, Crypto investment scams, updated February 2026, fca.org.uk/consumers/crypto-investment-scams

FCA, Recovery room scams, fca.org.uk/consumers/recovery-room-scams

FCA, Clone firms and individuals, and the FCA Warning List, fca.org.uk

FCA, press release on illegal finfluencers, 24 April 2026

ERSOU, warning to cryptocurrency holders about bogus police calls, March 2026, rocu.police.uk

Stop Scams UK, 159, stopscamsuk.org.uk/159

Scam Sniffer, 2025 crypto phishing report, January 2026

Derbyshire Police, warning on pig butchering scams

Citizens Advice, Advice Direct Scotland and Consumerline (nidirect) contact pages

HMRC, Cryptoassets Manual CRYPTO22450 and CRYPTO22500, gov.uk

Before It Rugs, our own records of new Solana memecoins, as of 24 October 2026, beforeitrugs.com/methodology

About this pack. Made by Before It Rugs, a free UK website that checks new Solana memecoins for the warning signs of a rug pull. Facts checked against official sources in October 2026; numbers and phone numbers can change, so check the current versions. This pack is general information, not financial, legal or tax advice, and it doesn't tell anyone to buy, sell or hold anything. Crypto is high risk and memecoins are extremely high risk: most go to zero. Free to print and share for non-commercial use in homes, schools and workplaces. Please don't sell it or remove our name. Edition 1. © 2026 Before It Rugs.