

WHAT TO DO IF SOMEONE TRIES TO TRICK YOU OUT OF MONEY OR DATA

OFFICIAL UPDATES LU-Alert · RTL, 100.7 · 112

DO THIS NOW

- 1** Do not pay, click links or share codes, card details or a copy of your ID. Hang up or stop replying, even if the caller insists it is urgent.
- 2** Check through a channel you choose: call the number printed on your card or on the official website, never the one the message or caller gave you.
- 3** If you already paid or gave card details or bank codes, call your bank straight away, and the card operator named on your card (in Luxembourg usually Worldline), to block the cards.
- 4** Officials never ask for money. Donations go only through channels announced by the authorities, and you never hand your identity papers to anyone offering help.
- 5** If someone in a uniform or with a badge is at your door and something feels wrong, keep the door shut and call the police on **113**. Impostors copy uniforms and insignia.
- 6** Report it to the national cyber-fraud help service (cyberfraud.lu), and make a police report if money or documents were taken. Keep the messages and screenshots as evidence.
- 7** Warn your family and neighbours, especially older relatives: the same scam usually goes to many people at once.

BEFORE

LEARN THE SIGNS OF A SCAM

- Urgency, threats, a prize, or a request to click, pay or send a copy of your ID are red flags. So are spelling mistakes, odd sender addresses and web addresses that almost match the real one.
- Never click a link in an unexpected message. Type the address yourself, or

call back on a number you looked up.

- Official warnings reach you through LU-Alert, the radio and official websites, never through a message asking you to pay. See **Alerts and sirens**.
- Share less about yourself online. Addresses, holiday dates and photos of

documents help scammers sound convincing.

AGREE A FAMILY RULE

- Agree not to send money or share codes or cards by phone or message. If a caller says they are from your bank or the police, hang up and call the number printed on your card.

AFTER

- Watch your bank statements for several weeks, and report any charge you do not recognise at once.
- If you gave a password, change it from a device you trust and switch on two-step login. If a device or account was taken over, see **Cyberattack**.
- If you feel angry or anxious after a scam, talk to someone you trust. Tell them what happened so they can watch out for it too.

IF YOU ARE...

OLDER, OR LIVING ALONE

- Keep a card next to the telephone with the family rule: no money, codes or cards by phone or message, and call back on the number printed on your card.

LOOKING AFTER CHILDREN

- Agree that children never pay online and never send photos of themselves or of documents without asking you first. BEE SECURE, the national service for safer internet use, has material for families.

DURING A WIDER CRISIS

- Scams peak in a crisis: fake collections, fake officials, fake offers of help. Check who is collecting, and give only through channels announced by the authorities.

EASY-READ SUMMARY

 Do not pay or click when someone rushes you.

 Call your bank on the number on your card.

 Officials never ask you for money.

 Tell your family about the scam.

 Real alerts come from LU-Alert and the radio.

Last reviewed: 28/10/2026 Sources for this page