Scam messages, calls and online shopping

A sudden request for a transfer, a BLIK code or an extra payment is a reason to verify the message through another channel.

Pause

Avoid links in suspicious messages. Open your bank, shop or delivery app yourself and check whether it shows a payment request.

Call a number you already know

If the caller sounds like a relative and asks for money, hang up and call the number already saved in your contacts. AI can imitate a familiar voice.

Check the shop and payment

Look up the seller’s details and return terms. Check the recipient and amount in the banking app before confirming a transaction.

Act after a scam

If you paid or exposed banking information, contact your bank through an official channel. Keep the messages and report the suspicious site or message to CERT Polska.

Practice

A message says: ‘Your parcel is waiting. Pay PLN 1.49.’ Explain how you would check the parcel status without using the link.

Official websites

CERT Polska

Co-funded by the Polish state budget through the Mazovian Voivode.
Active Seniors (ASY) programme · Priority II. Education for older people · 2026 edition