How to recognise online scams

EUROPEAN CYBER SECURITY MONTH

You receive an SMS from Cyberscam Sam, posing as your bank. You click on the link.

You are directed to what looks like your bank's website. You insert your online banking credentials.

Cyberscam Sam has now access to your financial details, and logs in to your online banking.

He calls you impersonating a bank operator and cites your customer information.

Cyberscam Sam persuades you to transfer money to another account under his control.

Protect yourself against online scams!

1. Beware of unsolicited text messages or emails claiming to be from your bank.
2. If they contain links and attachments, avoid clicking on them.
3. If you receive a suspicious call from your bank, hang up. You can verify it by calling your bank's customer services.
4. Never share your banking credentials or authorisation codes.
5. If you think you have been scammed, contact your bank immediately and report it the police.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY