Recognising Phishing & Online Scams

[Bridge4Mothers](#) © 2026 by [Bridge4Mothers Erasmus+ VET KA210](#) is licensed under [Creative Commons Attribution 4.0 International](#)

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

WHAT IS PHISHING?

Phishing is a type of online scam where someone pretends to be a trusted person or organisation to trick you into giving away information, clicking a dangerous link, downloading something, or sending money.

Phishing can arrive through:

- 📧 Email
- 💬 Text messages
- 📱 Social media messages
- 🌐 Fake websites
- 📞 Phone calls
- 💻 Pop-up messages

The message may look as if it comes from a bank, delivery company, government organisation, social media platform, or someone you know.

DEMONSTRATION: IS THIS EMAIL SAFE?

Imagine you receive this email:

From: Security Team security-alert@example.com

Subject: URGENT: Your account will be deleted today!

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Dear Customer,

We have detected suspicious activity on your account.

Your account will be permanently deleted in **24 hours** unless you verify your information.

Click here to confirm your account:

[VERIFY YOUR ACCOUNT NOW]

Please provide your password and security code.

Thank you,
Security Team

Would you click the link?

STOP!

Let's investigate the message first.

1. CHECK WHO SENT THE MESSAGE

Look carefully at the sender's email address.

Do not look only at the name.

A scammer can make an email appear to come from: **"Your Bank"**

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

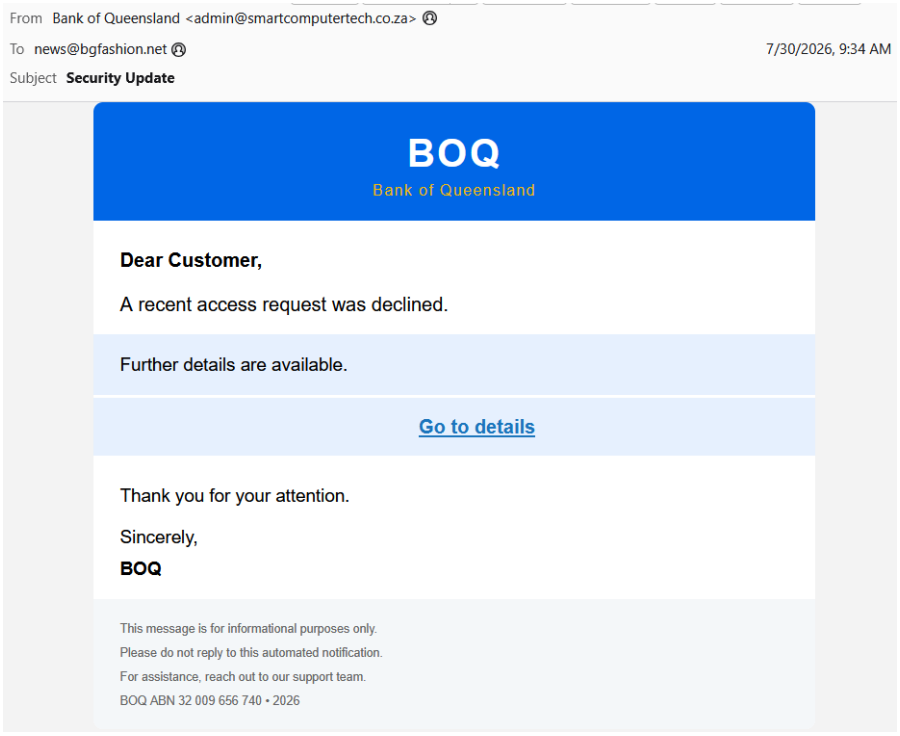
But the actual email address may be something completely different.

Ask: Does the email address match the organisation it claims to represent?

🚩 Warning sign

The sender's address looks unusual, contains random characters, or uses a domain that does not belong to the organisation.

Here is an example phishing email I received:



From Bank of Queensland <admin@smartcomputertech.co.za>
To news@bgfashion.net 7/30/2026, 9:34 AM
Subject **Security Update**

BOQ
Bank of Queensland

Dear Customer,

A recent access request was declined.

Further details are available.

Go to details

Thank you for your attention.

Sincerely,
BOQ

This message is for informational purposes only.
Please do not reply to this automated notification.
For assistance, reach out to our support team.
BOQ ABN 32 009 656 740 • 2026

Bridge4Mothers **© 2026 by** *Bridge4Mothers Erasmus+ VET KA210* **is licensed under** *Creative Commons Attribution 4.0 International*

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

You can see the name Bank of Queensland, but the Sender's email address does not look legitimate - admin@smartcomputertech.co.za

2. BE CAREFUL WITH URGENT MESSAGES

Scammers often want you to act quickly. Look for phrases such as:

- URGENT
- Act now
- Your account will be deleted
- You have only 24 hours
- Last warning
- Immediate action required

The goal is to make you panic before you have time to think.

🚩 Warning sign

The message creates fear, pressure, or urgency.

REMEMBER:

Stop. Take a breath. Check before you act.

3. CHECK WHAT THEY ARE ASKING FOR

Be extremely careful if a message asks for:

- Your password

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Bank details
- Credit/debit card information
- Security codes
- Personal identification information
- Copies of documents
- Money or gift cards

IMPORTANT

A legitimate organisation will not normally ask you to send your password or security code by email or message.

🚩 Warning sign

The message asks you to provide sensitive information.

4. DON'T CLICK THE LINK IMMEDIATELY

A link may take you to a fake website designed to steal your information. Before clicking, check where the link is going.

On a computer, you can often **hover over the link without clicking it** to see the destination.

Ask: Does this address belong to the organisation?

🚩 Warning sign

The link:

- Looks strange

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Contains spelling mistakes
- Uses an unfamiliar domain
- Redirects to a different website
- Does not match the organisation mentioned in the message

SAFER OPTION

Instead of clicking the link in the message, open the organisation's official website yourself using a saved bookmark or by typing the known web address.

5. LOOK FOR SPELLING AND GRAMMAR PROBLEMS

Some scam messages contain:

- Spelling mistakes
- Strange grammar
- Unusual wording
- Poor formatting
- Unprofessional language

However, remember:

GOOD SPELLING DOES NOT MEAN A MESSAGE IS SAFE.

Scammers can create very professional-looking messages. Treat spelling and grammar as **one clue**, not proof.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

6. CHECK THE STORY

Ask yourself: "Does this message make sense?"

For example:

"Your package could not be delivered."

But you haven't ordered anything.

Or:

"Your bank account has been locked."

But the message comes from an unfamiliar email address.

Or:

"You have won a prize!"

But you never entered a competition.

🚩 **Warning sign**

The message is unexpected or doesn't match anything you have done.

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

7. DON'T TRUST LOGOS AND DESIGN

A scam email may contain:

- Company logos
- Official-looking colours
- Professional formatting
- Photos
- Legal-looking text

These things can be copied.

REMEMBER:

A message can look real and still be fake. Always check the sender, request, link, and context.

THE 6-POINT PHISHING CHECK

Before clicking a link or responding to an unexpected message, ask:

1. WHO?

Who sent it?

2. WHY?

Why are they contacting me?

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

3. URGENT?

Are they trying to rush me?

4. WHAT?

What are they asking me to do?

5. LINK?

Where does the link really go?

6. SAFE?

Can I verify this another way?

ACTIVITY: SPOT THE RED FLAGS

Read this message:

Congratulations! 🎉

You have been selected to receive a €500 shopping voucher!

You must claim your prize within 2 hours. Click the link below and enter your full name, bank card details and password.

CLAIM YOUR PRIZE NOW!

Bridge4Mothers ***© 2026 by*** *Bridge4Mothers Erasmus+ VET KA210* ***is licensed under*** *Creative Commons Attribution 4.0 International*

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

WHICH WARNING SIGNS CAN YOU FIND?

☐ You did not enter a competition.

☐ The message creates urgency.

☐ It asks for financial information.

☐ It asks for a password.

☐ It asks you to click a link.

☐ It promises a valuable prize.

☐ The sender has not been verified.

WOULD YOU CLICK THE LINK?

No.

The safest response is to **not click, not reply, and not provide any information.**

WHAT SHOULD YOU DO IF YOU RECEIVE A PHISHING MESSAGE?

STOP

Don't click anything.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

CHECK

Look at the sender, message, link, and request.

VERIFY

Contact the organisation using an official website, app, or phone number you already know.

DELETE

If the message is clearly a scam, delete it.

REPORT

Use your email provider, messaging app, bank, or relevant platform's reporting tools when appropriate.

WHAT IF YOU ALREADY CLICKED?

Don't panic. Take action quickly.

IF YOU ENTERED YOUR PASSWORD:

- Change the password immediately.
- Change it anywhere else you reused it.
- Turn on two-factor authentication.
- Check for suspicious account activity.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

IF YOU PROVIDED BANK OR CARD INFORMATION:

- Contact your bank using its official contact details.
- Explain what happened.
- Follow the bank's instructions.

IF YOU DOWNLOADED A SUSPICIOUS FILE:

- Do not open it again.
- Run your device's security/antivirus checks.
- Seek technical help if necessary.

IF YOU SENT MONEY:

- Contact your bank or payment provider as soon as possible.
- Keep records of the transaction and messages.

MINI CHALLENGE

Imagine you receive this text message:

Your delivery could not be completed. Pay €1.99 to reschedule your delivery: [link]

BEFORE DOING ANYTHING, ASK:

Who sent it?

Was I expecting a delivery?

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

Does the link belong to the delivery company?

Why am I being asked to pay through this link?

How could I verify the message safely?

YOUR DECISION:

☐ Click the link

☐ Reply to the message

☐ Ignore it and verify through the company's official website/app

☐ Give the sender my personal details

YOUR ANTI-PHISHING CHECKLIST

Before interacting with an unexpected message:

☐ I checked the sender.

☐ I checked the actual email address or phone number.

☐ I looked for urgent or threatening language.

☐ I checked what information the sender wants.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: *Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

☐ I did not click the link immediately.

☐ I checked where the link leads.

☐ I considered whether I was expecting the message.

☐ I know how to verify the message through an official channel.

☐ I know what to do if I accidentally provide information.

REMEMBER

STOP → CHECK → VERIFY

STOP before clicking.

CHECK the sender, message, link, and request.

VERIFY using an official source.

THINK BEFORE YOU CLICK.

NEVER SHARE PASSWORDS OR SECURITY CODES.

IF SOMETHING FEELS WRONG, STOP AND CHECK.

Bridge4Mothers © 2026 by Bridge4Mothers Erasmus+ VET KA210 is licensed under Creative Commons Attribution 4.0 International

Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.