PROXIMUS CYBERSECURITY AWARENESS

JANUARY 2025

PHISHING TRAINING

WHAT IS PHISHING?

Phishing is one of the most common cybersecurity threats in workplaces. It involves fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity. Employees must be aware of these threats to safeguard company data and personal information.

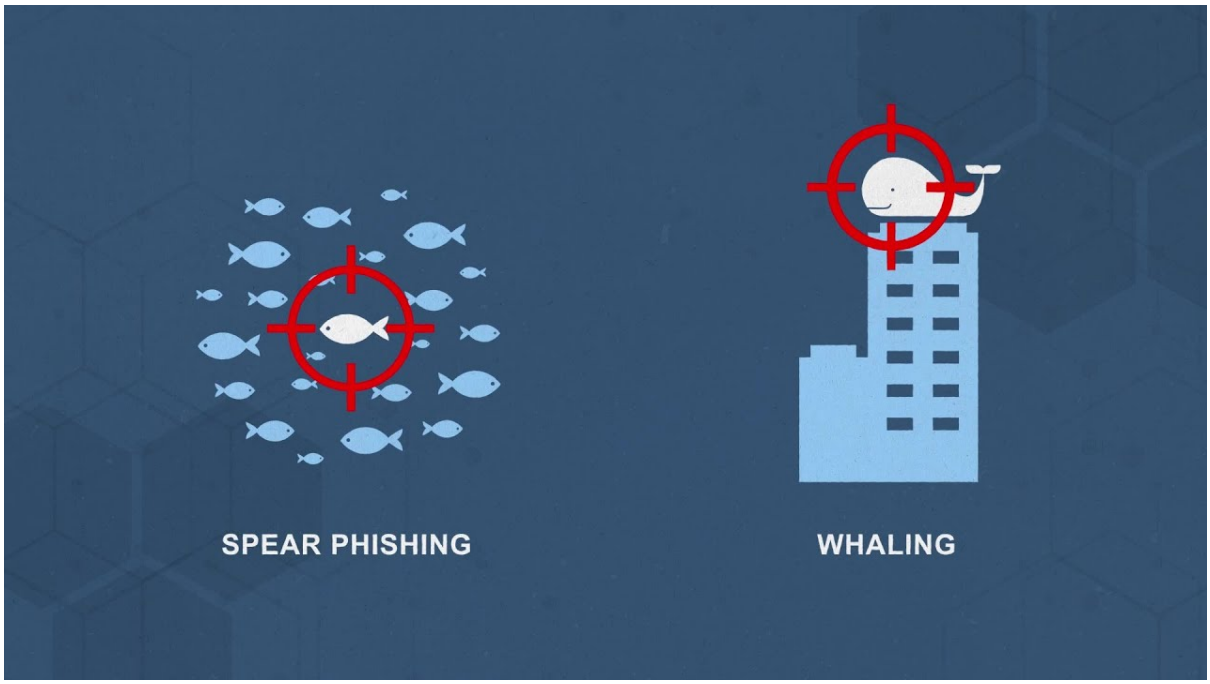
Definition: It is a form of cyber attack where attackers use deceptive emails, messages, or websites to steal personal and corporate information, such as passwords, financial data, or confidential business details.

Watch the following video to better understand:

COMMON TYPES OF PHISHING ATTACKS

1. **Email Phishing:** Fraudulent emails that mimic legitimate sources, often urging employees to click on malicious links or download harmful attachments.
2. **Spear Phishing:** Highly targeted attacks aimed at specific individuals or departments using personalised information.
3. **Whaling:** Targeting high-profile employees, such as executives, to gain access to sensitive business data.
4. **Smishing (SMS Phishing):** Malicious messages sent via SMS or messaging apps.
5. **Vishing (Voice Phishing):** Phone calls from attackers impersonating IT support or executives to extract sensitive information.

Watch the following video to better understand:



HOW TO DETECT PHISHING EMAILS

Look for these warning signs:

- **Suspicious Sender Email:** Hover over the sender's email address. Does it match the organisation's official domain?
- **Urgent or Threatening Language:** Phrases like "Immediate Action Required" or "Your Account Will Be Locked" create panic.
- **Unexpected Attachments or Links:** Do not open attachments or click links from unknown senders. Hover over links to verify authenticity.
- **Poor Grammar and Spelling Mistakes:** Legitimate businesses maintain professional communication.
- **Unusual Requests:** If an email asks for sensitive data or urgent money transfers, verify with the sender through another channel.

Read the following article and watch the video to better understand:

https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

HOW TO PROTECT YOURSELF FROM PHISHING EMAILS

🔷 **Verify Before Clicking:** Always check links before clicking—hover over them to see where they lead.

🔷 **Use Multi-Factor Authentication (MFA):** Even if your password is stolen, MFA provides an extra layer of security.

🔷 **Be Wary of Unexpected Emails:** If you weren't expecting an email, call the sender to confirm authenticity.

🔷 **Report Suspicious Emails:** Forward phishing attempts to your IT/security team immediately.

🔷 **Keep Software Updated:** Cybercriminals exploit vulnerabilities in outdated software.

Read the following article and watch the video to better understand:

https://www.thetimes.com/money-mentor/fraud-and-scams/the-email-phishing-scams-to-look-out-for-in-2025

WHAT TO DO IF YOU FALL FOR A PHISHING ATTACK?

🚨 **Immediate Actions:**

✔ **Do Not Panic.**

✔ **Disconnect from the Internet** to prevent malware from spreading.

✔ **Change Your Passwords** immediately if you entered credentials.

✔ **Notify IT Support** so they can take preventive measures.

✔ **Monitor Accounts** for any unauthorised transactions.

Watch the following video to better understand what happens after being attacked:

ARE YOU READY FOR A QUICK TEST?

1. What is the most common goal of a phishing attack?

a) To sell you a new product
b) To trick you into revealing sensitive information
c) To test your email security settings
d) To send newsletters

2. You receive an email from "support@proximus-secure.com" asking you to reset your password. What should you do?

a) Click the link and reset your password immediately
b) Reply to the email and ask for confirmation
c) Verify the sender and URL by hovering over the link before taking action
d) Forward the email to all colleagues for awareness

3. Which of the following is a red flag in a phishing email?

a) Unexpected urgency, like "Your account will be suspended today!"
b) Misspellings or grammatical errors
c) Links leading to a slightly misspelled website (e.g., www.pr0ximus.be instead of www.proximus.be)
d) All of the above

4. What should you do if you accidentally click on a phishing link?

a) Close your computer and hope nothing happens
b) Enter your credentials to see if the website works
c) Immediately report it to the IT security team and change your password
d) Ignore it if nothing appears to be wrong

5. An email from "HR@proximus.jobs" asks you to verify your salary details through a link. What is the best action?

a) Open the email and click the link to check

b) b) Call the HR department directly to confirm before clicking anything

c) c) Reply to the email to ask for details

d) d) Forward the email to IT and delete it

6. A Proximus executive sends you an urgent request to transfer money. The email looks real, but you are unsure. What do you do?

a) Immediately transfer the funds since it's from an executive
b) Verify the request through a phone call or internal communication channel
c) Ignore it and do nothing
d) Forward the email to IT and then reply to confirm the request

7. You receive an SMS from "Proximus Support" saying your mobile account has been compromised and asking you to click a link to secure it. What should you do?

a) Click the link to secure your account
b) Reply to the SMS asking for more details
c) Report the message as smishing (SMS phishing) and delete it
d) Forward the SMS to all colleagues to warn them

8. Which is the safest way to access your Proximus employee account?

a) Clicking a link in an email that says "Login Now to Verify Your Account"
b) Typing the official website address (e.g., www.proximus.be) directly into your browser
c) Searching for "Proximus login" on Google and clicking the first result
d) Using a shared link from a colleague via email

9. How can you enhance your security against phishing attacks?

a) Enable multi-factor authentication (MFA) for your accounts
b) Use the same password across all platforms
c) Click on links only if they look official
d) Avoid reporting phishing emails to IT

10. If you suspect a phishing email, what is the best way to report it at Proximus?

a) Delete it and move on
b) Click any links in the email to check if it's real
c) Forward it to the official Proximus security team or IT department
d) Reply to the sender and ask them if it's legitimate

Answer Key

Question	Correct Answer
1	b) To trick you into revealing sensitive information
2	c) Verify the sender and URL by hovering over the link before taking action
3	d) All of the above
4	c) Immediately report it to the IT security team and change your password
5	b) Call the HR department directly to confirm before clicking anything
6	b) Verify the request through a phone call or internal communication channel
7	c) Report the message as smishing (SMS phishing) and delete it
8	b) Typing the official website address (e.g., www.proximus.be) directly into your browser
9	a) Enable multi-factor authentication (MFA) for your accounts
10	c) Forward it to the official Proximus security team or IT department