

HPN Phishing Awareness Training



Phishing Awareness Training



- How to Recognize and Avoid Phishing Attacks
- This self-paced training will help you protect yourself and the organization.
- By the end of this training, you will understand how to identify, avoid, and report phishing attempts that could compromise sensitive information or systems.



How to Use This Training



- Read each slide carefully. No presenter is required.
- Think about how these examples apply to your daily work.
- You will answer a short knowledge check at the end.



-



Why Phishing Matters to You



- A single mistake can:
 - Expose patient or employee data
 - Disrupt clinical and business operations
 - Lead to ransomware or system downtime
- Your awareness helps keep everyone safe.



How Phishing Usually Works



- Most phishing follows a simple pattern:
 1. You receive an unexpected message
 2. The message creates urgency or fear
 3. You are asked to click, open, or respond
 4. The attacker gains access or information



Common Phishing Warning Signs



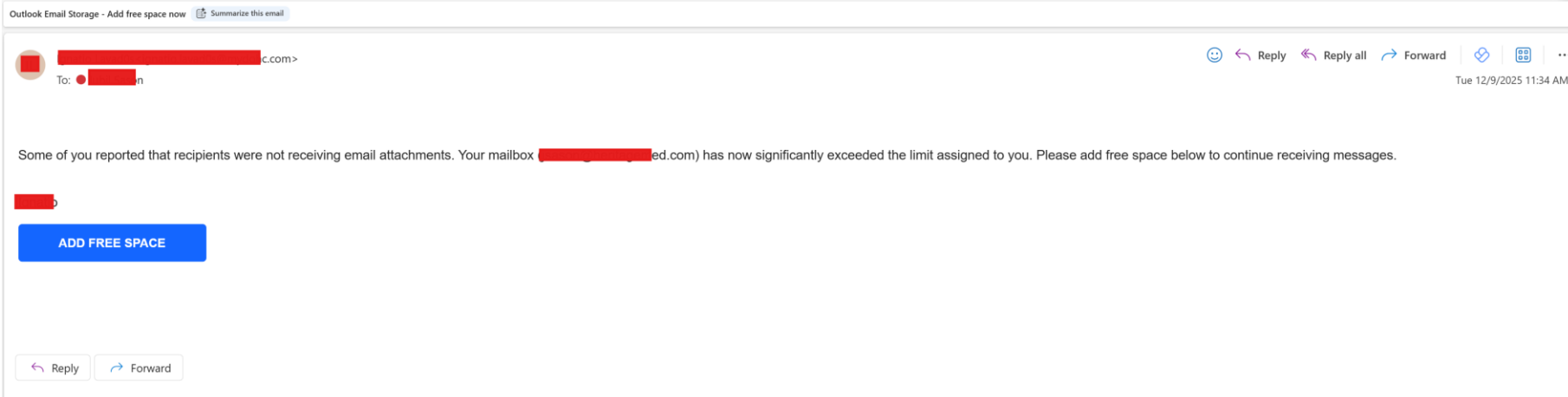
- Be cautious if a message:
 - Feels urgent or threatening
 - Asks for passwords or money
 - Includes unexpected attachments or links
 - Comes from a sender that looks slightly unusual



Real-Life Example: Urgent IT Message



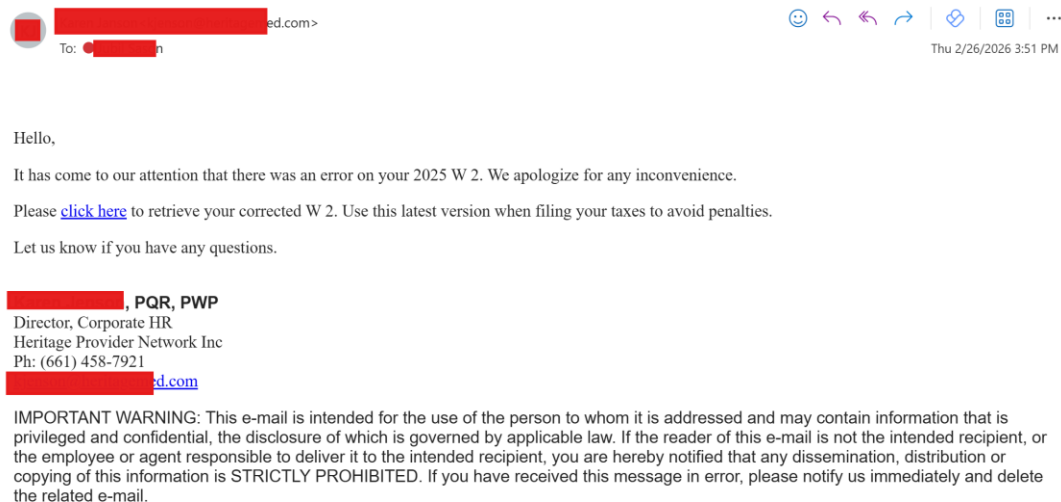
- A message claims to be from Information Technology Team.
- It asks you to click a link to do an update your Outlook Storage.
- Red flags:
 - Unusual request
 - Urgent or confidential language



Real-Life Example: Urgent Message from Finance Team



- A senior Finance Team member you regularly work with sends you a message requesting action.
- Red flags:
 - The email is sent at an unusual time
 - The message uses urgent or confidential language
 - The message prompts you to click a link to access a document that is typically available through trusted sources such as ADP.



Real-Life Example: Patient Record Request



- You receive an email that appears to be from a clinic, provider, or billing department asking you to urgently review or send patient information.
- Red flags:
 - The request includes urgent or threatening language
 - The sender's email address looks slightly unusual
 - The message asks for patient data, login credentials, or an unexpected attachment
 - The request does not follow normal HIPAA or company procedures
- Reminder: Always verify patient-related requests through approved channels before sharing information.

Real-Life Example: Fake Invoice



- You receive an email that appears to be from a vendor.
- It asks you to review or pay an invoice immediately.
- Red flags:
 - You were not expecting the invoice
 - The message pressures you to act quickly



Real-Life Example: Password Reset Scam



- You receive an urgent email saying your account will be locked unless you reset your password immediately.
- The message includes a link to a login page that looks legitimate.
- Red flags:
 - You did not request a password reset
 - The message creates urgency or fear
 - The sender's address looks unusual or slightly misspelled
 - The link directs you to a login page asking for credentials

Remember: Attackers use fake password reset emails to steal credentials and gain access to company systems and patient information.

Real-Life Example: Executive Message



- A message claims to be from leadership.
- It asks for gift cards, wire transfers, or sensitive information.
- Red flags:
 - Unusual request
 - Urgent or confidential language

What You Should Do



- If something feels suspicious:
 - Do not click links or open attachments
 - Do not reply or provide information
 - Verify the request using a known contact method

Reporting Phishing Is Important



- Reporting helps:
 - Protect coworkers from the same attack
 - Allow Security to block threats
 - Reduce risk to patients and systems
- Report even if you are unsure.



If You Clicked Something



- Mistakes can happen.
- If you clicked a link or attachment:
 - Report it immediately to IT Support and Cybersecurity Team
 - Please follow all instructions from the IT or Security Team, such as disconnecting from the network, Wi-Fi, or VPN, and turning off your computer as directed
 - You will not be punished for reporting

Key Takeaways



- Pause before you click.
- Urgency is a common phishing tactic.
- When in doubt, do not interact with the message.
- Reporting quickly makes a difference.

Quick Decision Checklist



- Was I expecting this message?
- Is the sender legitimate and correctly spelled?
- Is the message creating urgency or pressure?
- Should I verify this through another trusted method?