7 WAYS TO SPOT A PHISHING EMAIL

Phishing emails are among the most common tools cybercriminals use, with email spoofing posing a significant threat. This tactic involves impersonating legitimate corporate communications to deceive employees into interacting with malicious messages. Common examples include emails mimicking trusted brands like Amazon, Microsoft, or DHL. Spotting phishing attempts can help protect your organisation from costly security breaches.

1 CHECK THE SENDER'S DOMAIN AND EMAIL ADDRESS

Legitimate companies use their official domain, such as "microsoft.com," not suspicious variants like "microsoft.business.com." If a domain looks unusual, verify it on the company's website.

2 INSPECT THE HEADER AND FOOTER FOR INCONSISTENCIES

Headers and footers that look unprofessional, lack information, or differ from previous emails from the brand are red flags for phishing attempts.

3 CHECK THE SUBJECT LINE AND PREHEADER

Odd phrases, emojis, or unusual formatting in the subject line or preheader can indicate a phishing attempt. If it feels "off," it probably is.

FROM: noreply@gmail.com
SUBJECT: OPEN NOW YOU'VE WON!!!

Congratulations customer,

Your email has been selected. Click to claim your prize now!

https://am@z0nQRfkdjhsjdbgHFULsfjhdsniol88Fb62m

Please refer to attached (PDF FILE) for full prize list.

Regards,
J. Smith

4 ANALYSE THE CONTENT AND IMPLIED URGENCY

Messages that pressure you to act immediately, offer deals that seem too good to be true, or threaten service interruptions for unpaid bills are typical phishing tactics.

5 SPOT FORMATTING MISTAKES

Strange formatting, spelling errors, poor grammar, or mismatched colours, logos, or fonts often signal a phishing email.

6 BE WARY OF UNEXPECTED ATTACHMENTS LIKE PDFs OR WORD DOCS

Attachments like PDFs or Word Docs you weren't expecting—or with unusual file names—may contain malware or ransomware, frequently deployed via phishing emails.

7 USE CAUTION AND VERIFY LINKS BEFORE CLICKING

Hover over links to see where they lead. If the URL doesn't match the company's domain, it's likely fraudulent. Avoid clicking links for password resets and log in directly on the company's website.

BETTER SAFE THAN SORRY WHEN IT COMES TO EMAIL MANAGEMENT

Phishing continues to be a leading threat to organisations, targeting employees with deceptive emails designed to exploit vulnerabilities. With our training system, your team can gain the knowledge and skills to identify and prevent these attacks before they cause harm. Our solution provides comprehensive training tailored to your business needs, equipping employees with the confidence to recognise phishing attempts and respond appropriately.

We offer interactive and engaging training modules that simulate real-world phishing scenarios, ensuring employees can practise identifying and handling threats in a safe environment. By fostering awareness and proactive behaviour, your team will be empowered to stay one step ahead of cybercriminals, enhancing your organisation's overall security posture.

Explore our employee training options. Contact us to learn more.

StepFwd IT
1300 131 679
stepfwdit.com.au
hello@stepfwdit.com.au