7 WAYS TO SPOT A PHISHING EMAIL

One of today's biggest phishing risks is email spoofing. This form of phishing involves cybercriminals mimicking official corporate communications to lure unsuspecting employees into interacting with them. In this scheme, emails purporting to be from large firms, such as Amazon, Microsoft or DHL, are malicious. Discerning what is real versus what is fake can help your organization prevent costly cybersecurity breaches.

1 CHECK THE SENDER'S DOMAIN AND EMAIL ADDRESS

Legitimate companies send emails from their official domain, like "microsoft.com," and not variants like "microsoft.business.com." If a domain looks odd, check the address on the company's website.

2 PAY ATTENTION TO THE HEADER AND FOOTER FOR CLUES

If the header or footer is inconsistent with other messages from that brand or has missing information or is just slapdash, it's likely the message is a phishing attempt.

3 LOOK AT THE SUBJECT LINE AND PREHEADER

Does the subject line or preheader of a message seem a little "off" to you? Are there odd phrases, emojis or unusual things in the subject line and/or preheader? If yes, it indicates phishing.

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 ANALYZE THE CONTENT AND IMPLIED URGENCY

Claiming an action is urgent, offering a special that's too good to be true or insisting a company must make a payment before services are cut off are all hallmarks of phishing.

5 BEWARE OF FORMATTING RED FLAGS

This is where many of us catch phishing attempts. If the message has strange formatting, spelling mistakes or bad grammar, or the colors, logos and fonts are "off," it's probably phishing.

6 BE WARY OF UNEXPECTED ATTACHMENTS LIKE PDFs OR WORD DOCS

If you aren't expecting an attachment or an attachment looks suspicious because it has a strange name, it might be malware or ransomware, which are frequently deployed through phishing.

7 USE CAUTION IF A MESSAGE ASKS YOU TO LOG IN THROUGH A NEW LINK

Consider the links that a message asks you to click to see if they go to the company's actual domain or log in on their site directly. Fraudulent password reset requests are a staple of phishing.

BETTER SAFE THAN SORRY WHEN IT COMES TO EMAIL MANAGEMENT

Phishing is one of the most common attack vectors employees encounter. The good news, however, is that regular security awareness training empowers employees to spot and stop bogus messages, such as fake branded emails, and reduces your company's chance of experiencing a damaging cyberattack.

Choose a training platform/learning management system that allows you to design training courses and then upload/deploy them to team members. The solution must host a wide range of training courses including employee safety, conduct (anti-harassment), orientation/employee onboarding, cybersecurity, policy changes and more.

We have the right training solution for your business. Contact us to learn more.
Contact sales@mindburnsolutions.com or call us @ 717.303.3309