

Phishing Awareness Training

Security Insights for Teams

What is Phishing



Social Engineering to steal credentials

- Phishing leverages manipulation tactics to trick individuals into revealing usernames, passwords, and other confidential data.

Often appears legitimate

- Messages often impersonate trusted entities like IT departments, banks, or company executives to gain user trust.

Common in emails, SMS and even phone calls

- Attackers use various channels – emails, text, and voice – to distribute phishing content and . maximum success

Phishing Red Flags

15

MINS

10 MOST COMMON SIGNS OF A PHISHING EMAIL

Phishing continues to be the #1 attack vector for threat actors – these are the tell-tale signs you need to know.

1



AN UNFAMILIAR TONE OR GREETING

Look for language that isn't quite right – for example, a colleague or family member is a little more formal or casual than normal.

2



GRAMMAR AND SPELLING ERRORS

One of the more common signs of a phishing email is bad spelling and the incorrect use of grammar.

3



INCONSISTENCIES IN EMAIL ADDRESSES, LINKS & DOMAIN NAMES

Look for discrepancies in email addresses, links and domain names. If a link is embedded in the email, hover over the link to verify that what 'pops up' is a legitimate URL.

4



THREATS OR A SENSE OF URGENCY

Emails that threaten negative consequences or use a sense of urgency to encourage, or even demand, immediate action should always be treated with suspicion.

5



SUSPICIOUS ATTACHMENTS

If an email with an attached file is received from an unknown sender or if the recipient did not request or expect to receive the file, the email and attachment should be virus-scanned before opening.

6



UNUSUAL REQUEST

If an email is received asking for something to be done that is not the norm, it is a red flag for a potentially malicious email.

7



SHORT AND SWEET

While many phishing emails will be stuffed with details designed to offer a false sense of security, some phishing messages will have sparse information hoping to trade on their ambiguity.

8



RECIPIENT DID NOT INITIATE THE CONVERSATION

Because phishing emails are unsolicited, an often-used hook is to inform the recipient they won a prize, will qualify for a prize if they reply to the email, or will benefit from a discount by clicking on a link or opening an attachment.

9



REQUEST FOR CREDENTIALS, PAYMENT INFO OR OTHER PERSONAL DETAILS

One of the most sophisticated types of phishing emails contains a link to a fake landing page the attacker created that recipients are directed to in an official-looking email. Recipients should visit the website by typing in the URL, rather than clicking on a link.

10



SEE SOMETHING, SAY SOMETHING

Identification is the first step in the battle against phishing. Organizations need to promote security awareness and condition employees to report potentially malicious emails.

How to Respond

- **Tips:**



- **Don't click unknown links**
- **Report to IT/SOC**
- **Check sender carefully**
- **Use official login portals only**

Insight From Our Phishing Awareness Drill

- **25% Clicked Suspicious Link:** A quarter of participants interacted with a phishing simulation mail, highlighting real vulnerabilities.
- **15% Reported the Threat:** Only a small fraction used proper reporting channels to alert IT/SOC, indicating a need for reinforcement.
- **60% Ignored the Message:** Majority took no action—neither engaging nor reporting—underscoring awareness gaps.
- **Next Steps: Continuous Training:** Plan for quarterly phishing simulations and microlearning to boost resilience.



Any questions? Ask away!

Give your audience space to resolve immediate questions or concerns.