Zoho eProtect

Phishing awareness guide

ZOHO

Phishing awareness guide

Phishing remains one of the most common and effective cyberattacks today, targeting employees through seemingly harmless emails that trick them into engaging with malicious emails. These messages are designed to look genuine. They often imitate trusted brands, colleagues, or even internal teams, making it easy for anyone to fall for them.

This guide will help you understand what phishing is, the different forms it can take, and how to spot and report suspicious emails so you can protect both yourself and your organization.

What is phishing?

Phishing is a technique in which the attacker assumes the identity of someone the victim usually places their trust in to extract sensitive information such as bank account numbers, credit card numbers, or account credentials. This impersonated identity may be a bank the target has an account with, an online platform they shop from, shipping agencies, or other such platforms that they regularly interact with.

Common forms of phishing emails

Threat actors create phishing emails under the pretext of many genuine-seeming scenarios.

Fake account alerts: Emails claiming unusual login activity or password issues, urging you to click a link to "secure" your account.

Invoice or payment requests: Messages posing as vendors or finance teams, requesting urgent payments or updated billing details to steal money or credentials.

Delivery or shipment notices: Fake courier updates with tracking links or attachments that install malware when opened.

Job or prize offers: Promises of employment, rewards, or lotteries to entice users into sharing personal or banking information.

Internal impersonation (CEO fraud): Emails appearing to be from executives or HR, requesting sensitive data or confidential files under urgent pretenses.

Document sharing invitations: Phony links to view shared files (e.g., “View this PDF”) leading to credential-harvesting login pages.

How can you spot phishing emails?

1 **Suspicious sender address:** Email comes from a misspelled or unfamiliar domain that mimics a trusted source but isn’t quite right.

2 **Generic greetings:** Uses vague salutations like “Dear User” instead of your actual name to cast a wide net.

3 **Urgent or threatening language:** Creates panic with warnings of account closure, fines, or security breaches to rush you into clicking.

4 **Unexpected links or attachments:** Includes links or files you weren’t expecting, often hiding malicious downloads or fake login pages.

5 **Spelling and grammar errors:** Poor grammar, awkward phrasing, or inconsistent formatting can signal a scam or an attempt to bypass security filters.

6 **Too-good-to-be-true offers:** Promises rewards, refunds, or prizes that seem unusually generous or unrealistic.

7 **Mismatched URLs:** Hovering over links shows a different, suspicious web address than what's displayed in the email.

8 **Requests for sensitive information:** Legitimate companies rarely ask for passwords, bank details, or personal data via email.

9 **Inconsistent branding:** Logos, colors, or email signatures that look slightly off compared to the real company's style.

10 **Unexpected requests from "known" contacts:** Emails from colleagues or vendors that don't match their usual tone or contain odd instructions.

While there are many more markers to pay attention to while identifying phishing emails, these are some of the evident attributes.

What to do if you spot a phishing email?

If you notice any of the red flags above, follow these steps immediately to stay safe:

- Do not click anything or respond to the email.
- Verify the sender.
- Report it.
- Mark as spam or phishing.
- Change your password immediately if you've engaged with the email.

Conclusion

Phishing attacks succeed because they exploit trust and urgency. By learning to recognize warning signs, avoiding suspicious links, and promptly reporting anything unusual, you become a key line of defense for your organization.

This guide was released by Zoho eProtect as part of Cybersecurity Awareness Month 2025. eProtect is a cloud-based email security and archiving solution that provides advanced threat protection for all on-premise and cloud email accounts. eProtect is the security solution powering Zoho Mail, a platform trusted by millions of users.