

8 Tips To Detect Phishing Scams

01

Double Check Sender's Email



Make sure the email in your inbox is coming from a trusted source. Scammers tick trusted domains with variations.

Keep an Eye on Typos



Attackers don't usually focus on grammatically correct sentences. Check if the email has any typos or spelling errors.

02

03

Just Hover Before You Click



Don't click the link in the email randomly. Check the preview, and see where it takes, as ignoring can be an entry point to hacking.

Emails that Create Urgency



Spammers send an email saying, "Action Required," and tick the common user. Avoid sharing personal details, such as phone, contact etc, under pressure.

04

05

Don't Trust Attachments



Stay calm. Attachments contain malicious content that can be harmful. So, only open attachments from trusted sources.

Stay up to Date



Never stay behind. Keep all the software up to date. Also, apply a spam filter in advance to beware of phishing scams.

06

07

Rewards can be Tricky



You may get an email with the subject line, "You've won \$10,000!" Don't take any action. You cannot win a lottery without participating.

Call Out, Immediately



If you ever notice that your device's security has been compromised, reach out to the IT security team immediately.

08