asporea

Staff Guide: How to Spot and Stop Spoof Emails

Practical training for small business teams

This guide helps your team recognise fake emails that try to steal passwords or hosting access. It gives a simple habit to follow, quick exercises you can run in a team meeting, and steps to take if someone clicks.

What these scams try to do

Criminals send messages that look like account or service alerts. Common themes include mailbox full, password expiring today, or domain suspension. The goal is to create urgency so people click a link and enter their password on a look-alike site. Some messages try to start a payment diversion by asking finance to change bank details.

The 30 second check

1) Check the real link. Hover on a computer or long press on a phone and read the address. If it does not end with the genuine domain you already use, close it.

2) Check the sender. Ignore the display name and read the full email address.

3) Ignore the countdown. Warnings like 24 hour deactivation are designed to rush you.

4) Go in the front door yourself. Open the app or website in the usual way and sign in. If there is a real issue it will be shown there.

The habit to teach: Stop, Check, Choose

Stop before you click. Check the sender and the real link. Choose a safer route by opening the service directly. Repeat this in team reminders every quarter. Short and frequent beats long and rare.

Red flag patterns

Unfamiliar sender domains pretending to be your provider.

Links that look close to the real brand but are not exact.

Poor spelling or odd phrasing.

Buttons that say keep the same password or verify to avoid suspension.

Attachments asking you to enable content or macros.

Requests to change invoice bank details by email.

Quick exercises for a 20 minute team session

Warm up: ask the room what a real notice from your email or hosting provider looks like.

Show and tell: display two screenshots, one genuine and one fake, and ask people to vote.

Link reading drill: practise hovering on links to read the true address.

Portal drill: ask everyone to open the real portal by typing the address instead of clicking links.

Template you can send to staff

Subject: Two minute reminder on suspicious emails

Please remember the simple habit: Stop, Check, Choose. Stop before clicking. Check the sender and the real link by hovering. Choose a safer route by opening the service in the usual way. If you are unsure, forward the message to the internal contact for review and do not click.

If someone clicked by mistake

Change the password for that account at once and for any other account that reused it.

Turn on multi factor authentication if it was off.

Run a malware scan and remove any remote access tools that you did not install.

Check mailbox rules and forwarding in case the attacker added silent forwarding.

Warn finance and your bank to watch for payment diversion attempts.

Report the incident to your email provider and your national cyber authority.

Owner and IT checklist

Set SPF, DKIM and DMARC on your domain and monitor for failures.

Enable multi factor authentication for email, hosting and registrar accounts.

Turn on domain auto renew and registrar lock.

Separate customer service mailboxes from admin recovery addresses.

Enable the Report phishing button in your email platform and route reports to the right person.

Schedule a two minute reminder to staff every quarter.

One page reminder to print

Stop, Check, Choose.
Stop before clicking.
Check the sender and the real link.
Choose a safer route by opening the service directly.
If in doubt ask before you click.