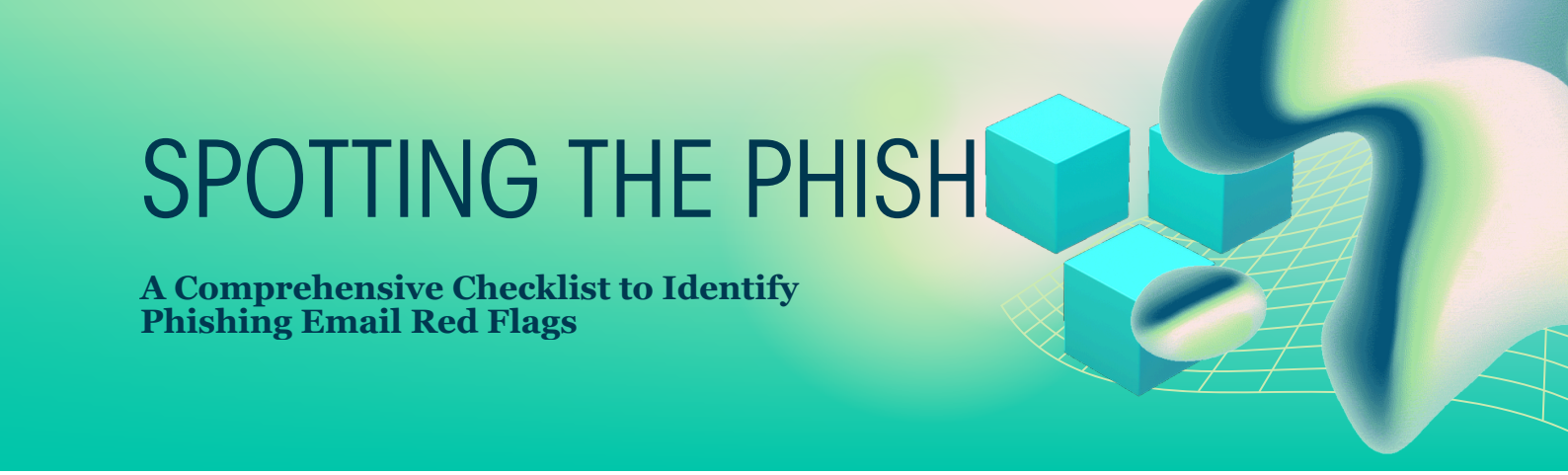

How to Spot a Phishing Email: Checklist for Small Businesses

Stay alert. Stay protected. Avoid costly mistakes before they happen.

Phishing emails are one of the most common ways businesses get breached. Most attacks don't rely on advanced hacking—they rely on simple human mistakes.

Use this checklist to quickly evaluate any suspicious email before clicking, replying, or downloading anything.

Phishing Email Red Flags Checklist

1. Suspicious Sender Address

□ The email looks like it's from a known company but the domain is slightly **off**
□ The sender name is familiar, but the actual email address doesn't **match**
□ The domain includes extra letters, numbers, or misspellings

Why this matters:
Attackers often spoof trusted brands or contacts. A single letter difference can mean the message is fake.

2. Urgent or Threatening Language

□ The message pressures you to act immediately
□ It mentions account suspension, legal action, or financial loss
□ It uses phrases like "Act now," "Final notice," or "Immediate response required"

Why this matters:
Phishing emails rely on urgency to override careful thinking.

3. Unexpected Attachments or Links

□ You weren’t expecting the file or link
□ The attachment type is unusual (ZIP, HTML, EXE, or unknown file)
□ The message asks you to “open” or “review” something quickly

Why this matters:
Malicious files and links are the most common way attackers gain access to your systems.

4. Mismatched or Hidden Links

□ The link text says one thing, but the URL shows something else
□ Hovering over the link reveals a suspicious or unrelated website
□ The link uses a URL shortener or unfamiliar domain

Why this matters:
Fake login pages are designed to steal your credentials.

5. Requests for Sensitive Information

□ The email asks for passwords, login details, or verification codes
□ It requests financial information or payment changes
□ It asks you to confirm account details via email

Why this matters:
Legitimate companies will not request sensitive information through email.

6. Poor Grammar, Formatting, or Branding

□ The email contains spelling or grammar mistakes
□ Logos look distorted or low quality
□ The layout feels inconsistent or unprofessional

Why this matters:
Many phishing emails are created quickly and lack attention to detail.

7. Unusual Requests from Known Contacts

□ A coworker or vendor asks for something out of character
□ The request involves money, passwords, or urgent actions
□ The tone or writing style seems different

Why this matters:
Business Email Compromise (BEC) attacks often impersonate real people.

8. Reply-To Address Doesn’t Match

□ The reply-to email is different from the sender
□ Replies are redirected to a personal or unrelated account

Why this matters:
Attackers use reply-to manipulation to continue conversations outside legitimate systems.

9. QR Codes in Emails (Quishing)

□ The email asks you to scan a QR code instead of clicking a link
□ The purpose of the QR code is unclear

Why this matters:
QR codes can bypass traditional security filters and lead to malicious sites.

10. “Too Good to Be True” Offers

□ Unexpected refunds, prizes, or financial rewards
□ Messages claiming you’ve won something or are owed money

Why this matters:
These are designed to lure you into clicking or sharing information.

What To Do If You Spot a Suspicious Email

Do **not** click links or download attachments
Do **not** reply or provide any information
Verify the sender through a **separate, trusted method**
Report the email to your IT provider or internal contact
Delete the message after reporting

Quick Rule of Thumb

If something feels off, it probably is.

Taking an extra 30 seconds to verify an email can prevent hours of downtime, data loss, or financial damage.

Strengthen Your Email Security

This checklist helps you spot threats but prevention is stronger than reaction.