What to Look Out for in Phishing Emails

> Phishing emails try to trick recipients into revealing credentials, installing malware, or transferring money. Attackers use urgency, impersonation, and fake links. Train yourself to pause, inspect, and verify before clicking or replying.

Red Flags to Look for in Phishing Emails

Sender & Identity

Display Name VS. Real Address: An email might be from IT-ServiceDesk <servicedesk@actiontarget.com> -- ensure to hover or view the full address to ensure it is a legitimate email.

Spoofed Domains: If you are skeptical of an email, ensure to check the email address and make sure it is the correct email address.

> Ex) account-security@amaz0n.com VS. account-security@amazon.com
> The first email address has a '0' instead of an 'o'. This is a solid way of determining if you are experiencing a phishing attack. If you are still uncertain, reach out to the IT department for help.

Reply-to is Different: The sender could be bob@actiontarget.com but the reply-to is timmy@gmail.com.

Links & URLs

Hover before clicking: Hover over a link to preview the destination. If the visible text says company.com/login but hovering shows http://bad-site.com/XYZ, it is phishing.

>

> When hovering over the link, you will see the destination in the bottom left-hand corner of the screen.

Shortened or obfuscated links: Bit.ly links or long, token-filled URLs -- Treat these with caution!

> A token filled URL will have a long, random string of characters that are often after a ? or #. Ex of a ? token) https://microsoft.com.verify-login.info/?id=U29tZVRva2VuVmFsdWU9MTIzNDU= Ex of a # token) https://paypal.com.security-check.io/#token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

Mismatch Example: Link text will say "*Secure your account*" **--->** Hovering shows http://212.16.152.5/verify

Content & Social Engineering

Urgency & Threats: "Your account will be deleted in 24 hours unless you verify"

Too good to be true: "You won $5,000 - Click to claim"

Unrequested Attachments: Attachments asking you to enable macros; opening can run malware on your device.

Spear-phish signs: Uses your co-worker's, manager's, or an executive's name or specific project details to get information

Attachments & File Types

High-risk file types: .exe, .scr, .bat, .com, .js, .vbs, .jar

Malicious Office files: .docx or .xlsx that prompt users to "Enable Editing" or macros

Compressed files: .zip or .7z with executables (.exe) inside

Visual & Language Cues

Poor grammar/spelling: Keep an eye out for improper spelling and incorrect grammar. These can be signs of a phishing email.

Off-brand fonts, odd spacing, or low-quality logos: This is another sign of a phishing email.

Incorrect salutations or signature block: There could be no phone number or a different formatting than usual.

Realistic Examples

- Phishing Example: Fake Account Deletion Notice
- Phishing Example: Executive Impersonation - Request for Personal Information

What to do if you suspect phishing

If you suspect phishing, you should:

1. **Do NOT click anything. Do NOT open any attachments.**
2. **Verify the sender's email address.** Check the email address to see if anything has been spoofed or if something seems off.
3. **Report internally** ---> create a ticket and forward the suspected phishing email to the IT team at servicedesk@actiontarget.com.
4. **If you clicked or opened:** notify the IT team ***IMMEDIATELY***. Time is of the essence. Disconnect from the network (if malware is suspected).
5. **Preserve the email.** Do not delete it until the IT team has a copy of it, so that they may investigate it.

Revision #16
Created 17 October 2025 18:37:58 by Tanner Bench
Updated 21 October 2025 17:17:53 by Tanner Bench