Phishing Attack Examples

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.

Examples

Phishing Example: Fake Account Deletion Notice

> This example shows a normal-looking email that tries to trick users into thinking their account will be deleted unless they enter login credentials and complete multi-factor verification. If a user submits those credentials, their account can be compromised — notify Action Target IT ***IMMEDIATELY***.

Picture #1 - The Phishing Email

From: Tony Diaz <reservations@basslake.com>
Sent: Friday, October 17, 2025 9:10 AM
To: [redacted]@actiontarget.com>
Subject: [redacted]@actiontarget.com Deletion Notice

Seems like a normal email address.

Exercise Caution: This email originated from outside our organization. DO NOT click on any images, links, or open any attachments, unless you have verified the sender and determined the content is safe.

The Action Target IT team would not delete your account because of an incomplete verification step.

Doesn't address the person receiving this

Hello,

Just a quick reminder, your email account ([redacted]@actiontarget.com) is scheduled for deletion later today (about 4 hours from now) because the verification step hasn't been completed yet.

If you still use this account, you'll need to verify it now to keep access to your mail, attachment, notes, and everything else linked to it.

You can complete the verification here:

Complete Verification

Hovering over this link would show you a preview in the bottom left of your screen, thus allowing you to see if the link is legitimate.

Once that's done, you're all set — nothing else is needed.

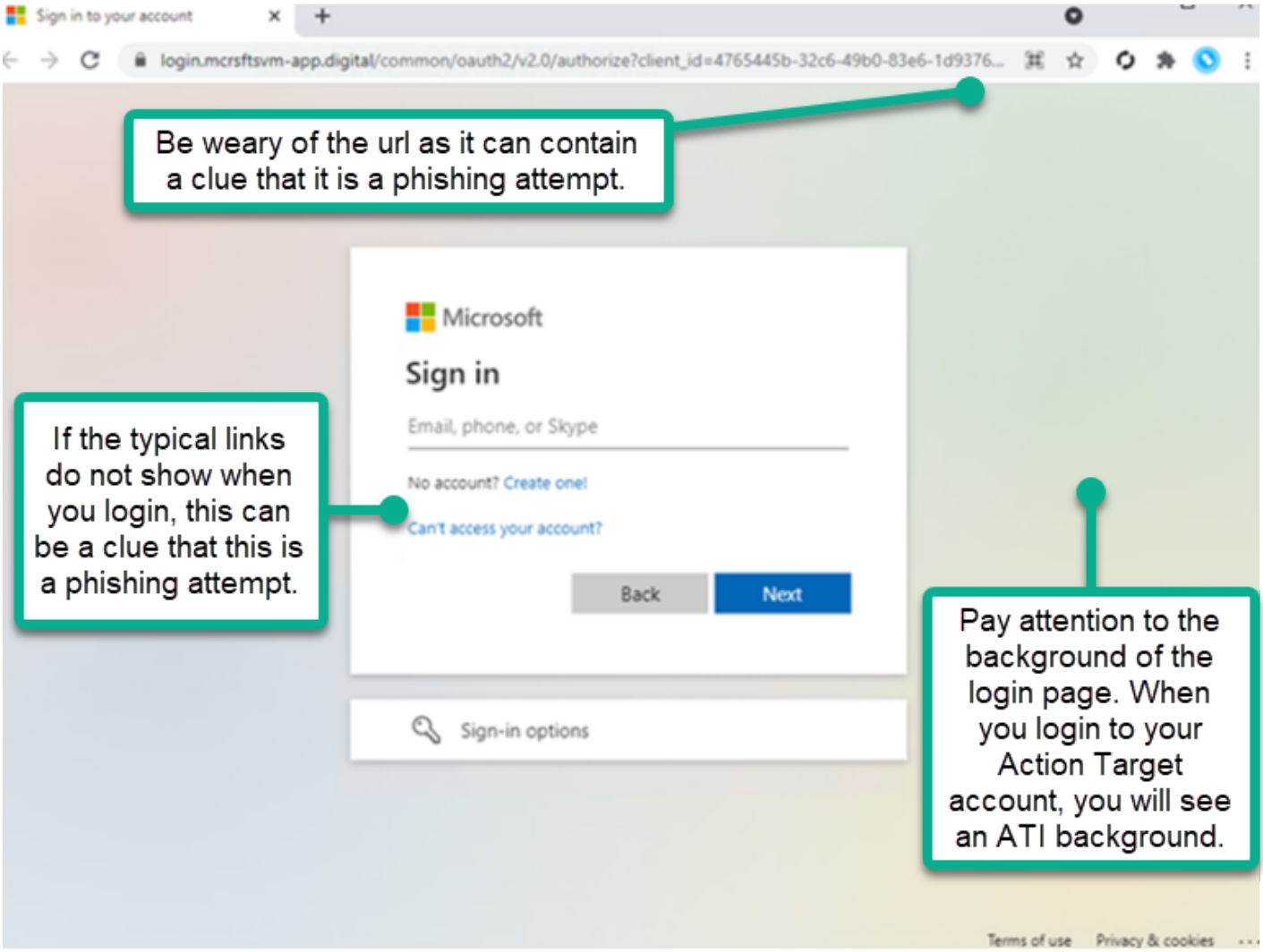
Best,

Tony Diaz
IT/Helpdesk Admin

The only IT team to reach out about any account issues/problems/inquiries is the Action Target IT team.

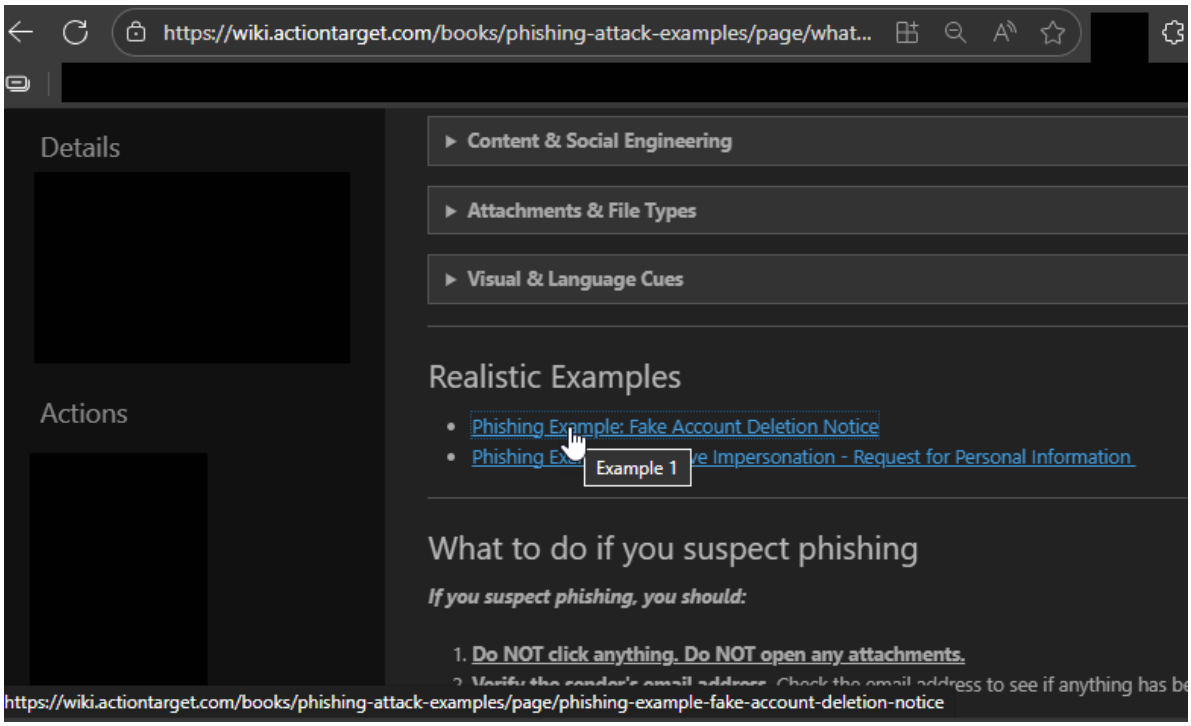
Pines Resort
54432 Road 432 Bass Lake CA 93604
800-350-7463

Picture #2 - Example of What You Could See by Clicking the Link



How to Verify Safely

1. Hover over the link and it will show in the bottom left hand corner of the screen.



2. Compare the domain against the official login domain (@actiontarget.com or company SSO URL)
3. If you are unsure, open a browser and navigate manually to the company portal (do NOT click the suspicious link)
4. Contact the IT team via an independent channel (phone, email, teams, ticket, in-person)

If You Clicked or Entered Credentials (URGENT)

1. ***IMMEDIATELY*** notify the Action Target IT team and forward them the email at servicedesk@actiontarget.com.
2. Provide any details about the incident to the IT team (approx. time, what you entered, screenshots ***if available***)
3. Follow the instructions the IT team provides you - this may require additional containment (password resets, account hold, forensic review).

What's the Goal?

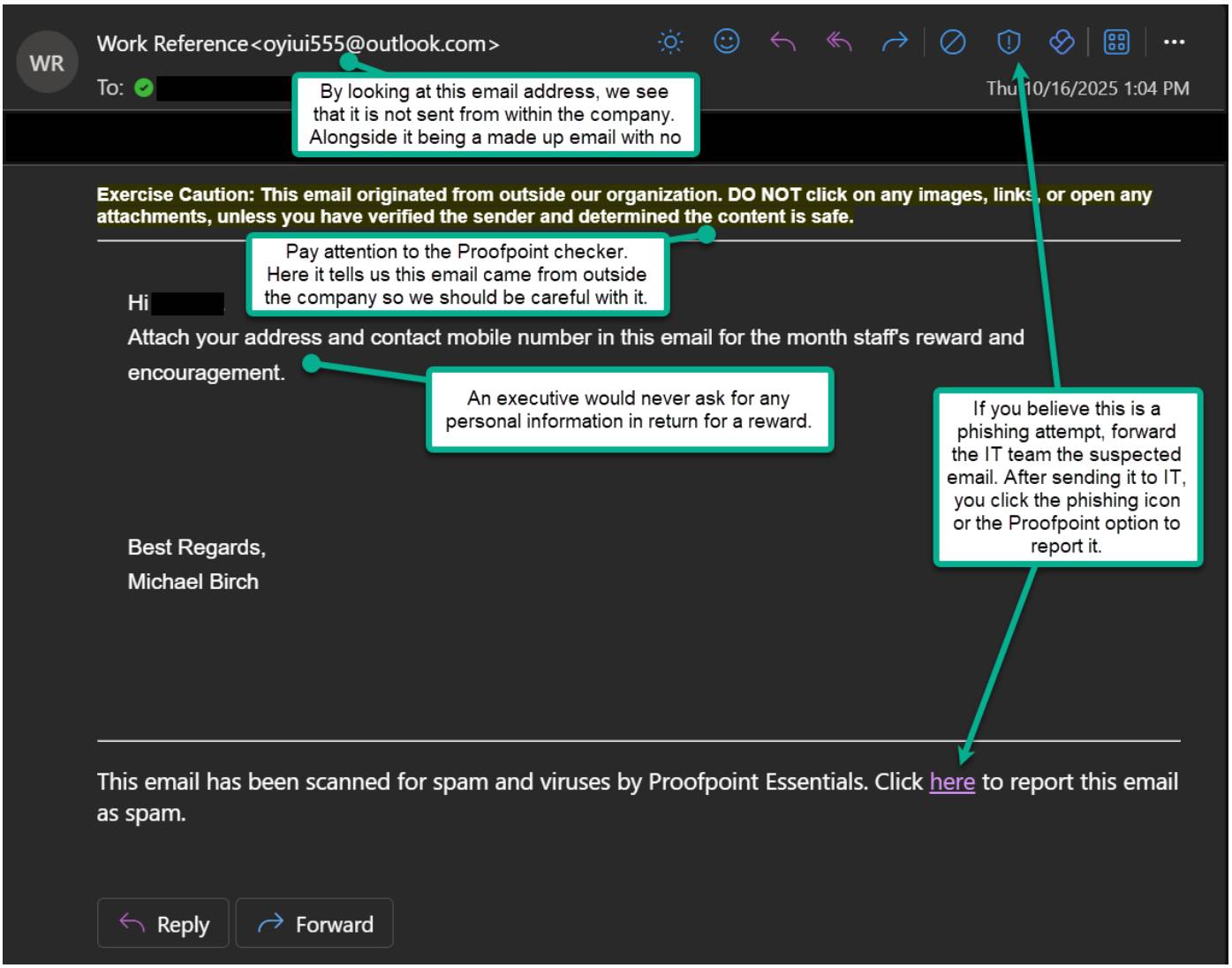
> This email is trying to trick you into giving up your Action Target login and multi-factor authentication by creating a false emergency — for example, claiming your account will be deleted unless you “verify” right away. If you enter your credentials or MFA code, attackers can take over your account and use it to read sensitive messages, send more phishing emails from a trusted address, request fraudulent payments, or create automatic forwarding rules to keep access.
>
> Attackers rely on pressure and perceived authority (pretending to be IT or a trusted service) so you’ll act without checking. Always pause, verify the request through a different channel (phone or the official IT helpdesk), and report the email to IT if anything seems off.

> ***Takeaway:*** Attackers rely on urgency and familiar-looking interfaces. Pause and verify every request for credentials or multi-factor authentication via an independent channel. If you suspect compromise, report to the IT team ***immediately*** -- fast containment reduces the damage.

Phishing Example: Executive Impersonation - Request for Personal Information

> This phishing email impersonates the company’s CEO, asking staff to provide personal information for a supposed “staff reward.” The vague wording, lack of personalization, and request for personal data via email are classic signs of a Business Email Compromise (BEC) attempt.

Picture #1 - The Phishing Email



What to Do Instead

1. If you are not sure whether it is fake or real, verify the request through another channel (e.g., call or message HR to see if they are doing staff reward).
2. Never send personal or company data in response to an unexpected email.
3. Report the email to the IT team and forward it to them. Then you can report it phishing with the Outlook button.

How to Verify an Executive's Email

1. Hover over the sender's name to see the real email address.
2. Compare it to the executive's actual email domain (@actiontarget.com)
3. Look for differences such as extra letter, wrong domain endings, etc.

What's the Goal?

Attackers send CEO, or other executive, impersonation emails to trick employees into sharing personal or company information, sending gift cards, or transferring money. They exploit authority and trust -- if a request appears to come from a high-ranking executive, recipients are less likely to question it.

> ***Remember:*** Even if an email looks like it's from leadership, pause before responding. Verify through official channels and report any suspicious messages ***immediately***.