Examples

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

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.

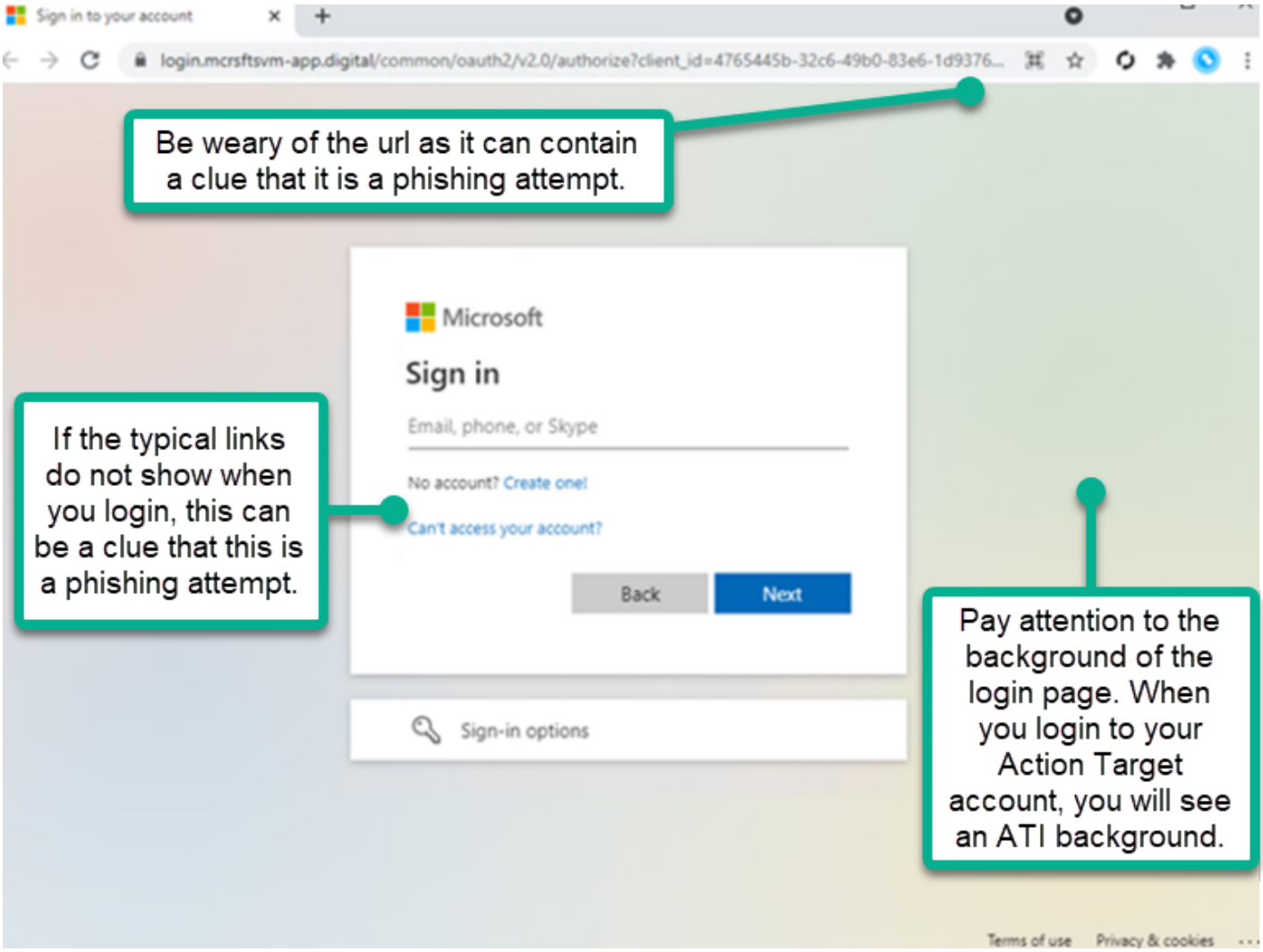
Best,

Tony Diaz
IT/Helpdesk Admin

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

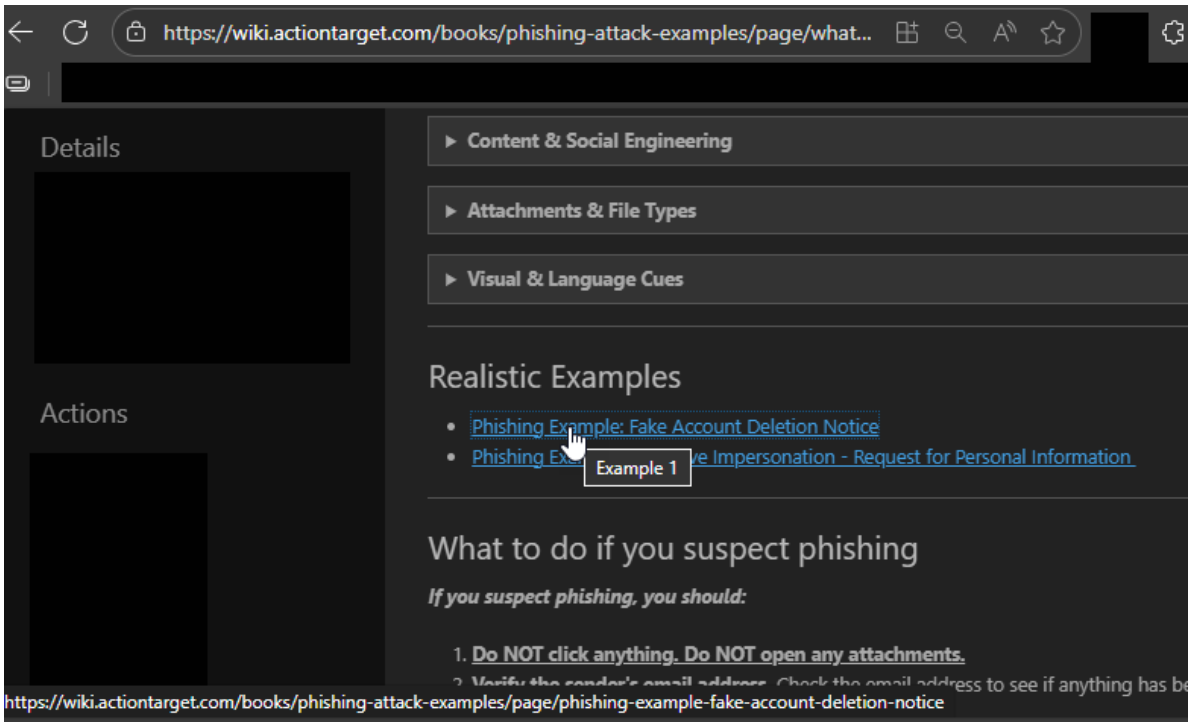
Pines Resort
54432 Road 432 Bass Lake CA 93604
800-350-7463

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?

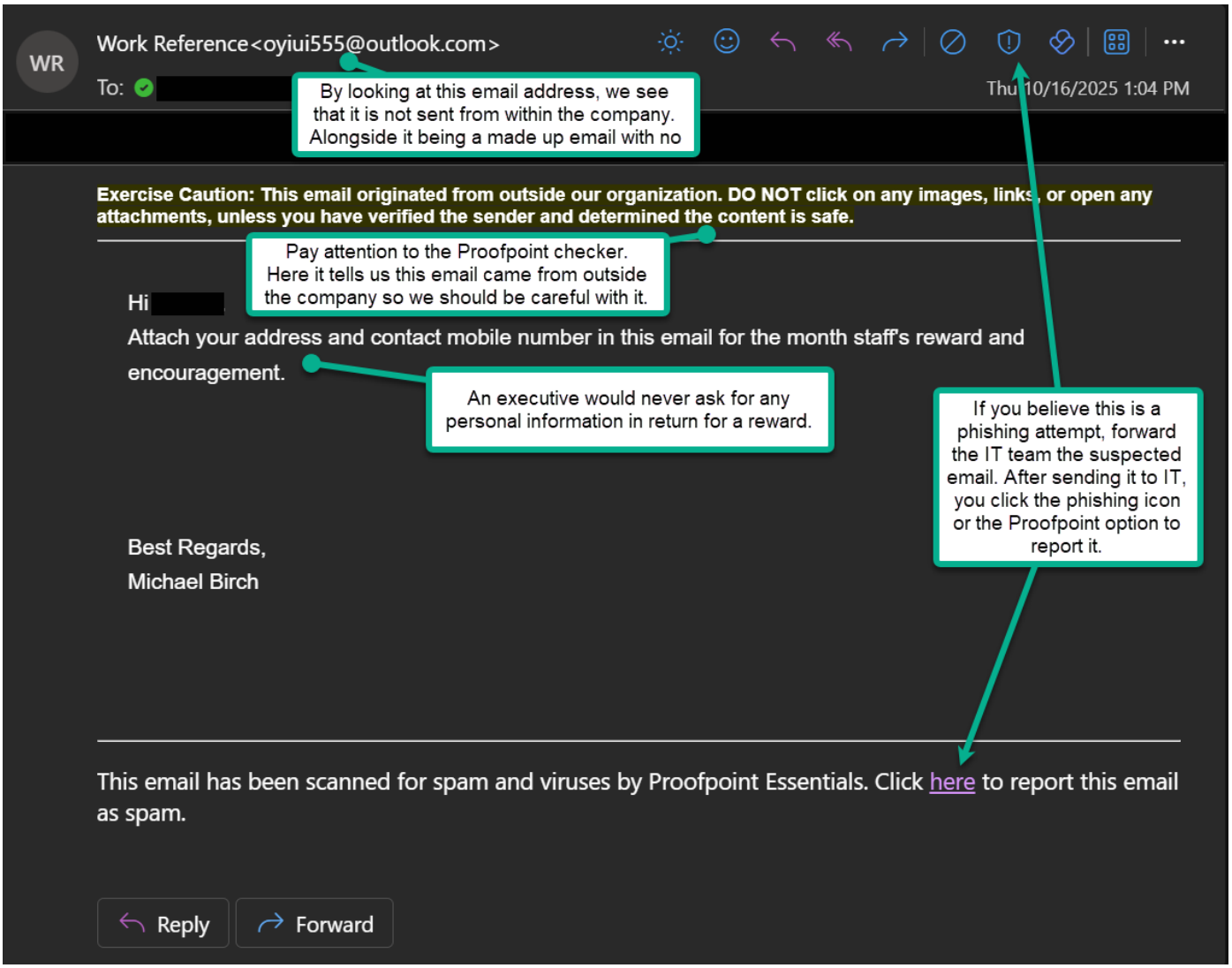
> This email is trying to trick you into giving up your Action Target login and multi-factor authentication by creating a false emergency — for example, claiming your account will be deleted unless you “verify” right away. If you enter your credentials or MFA code, attackers can take over your account 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***.