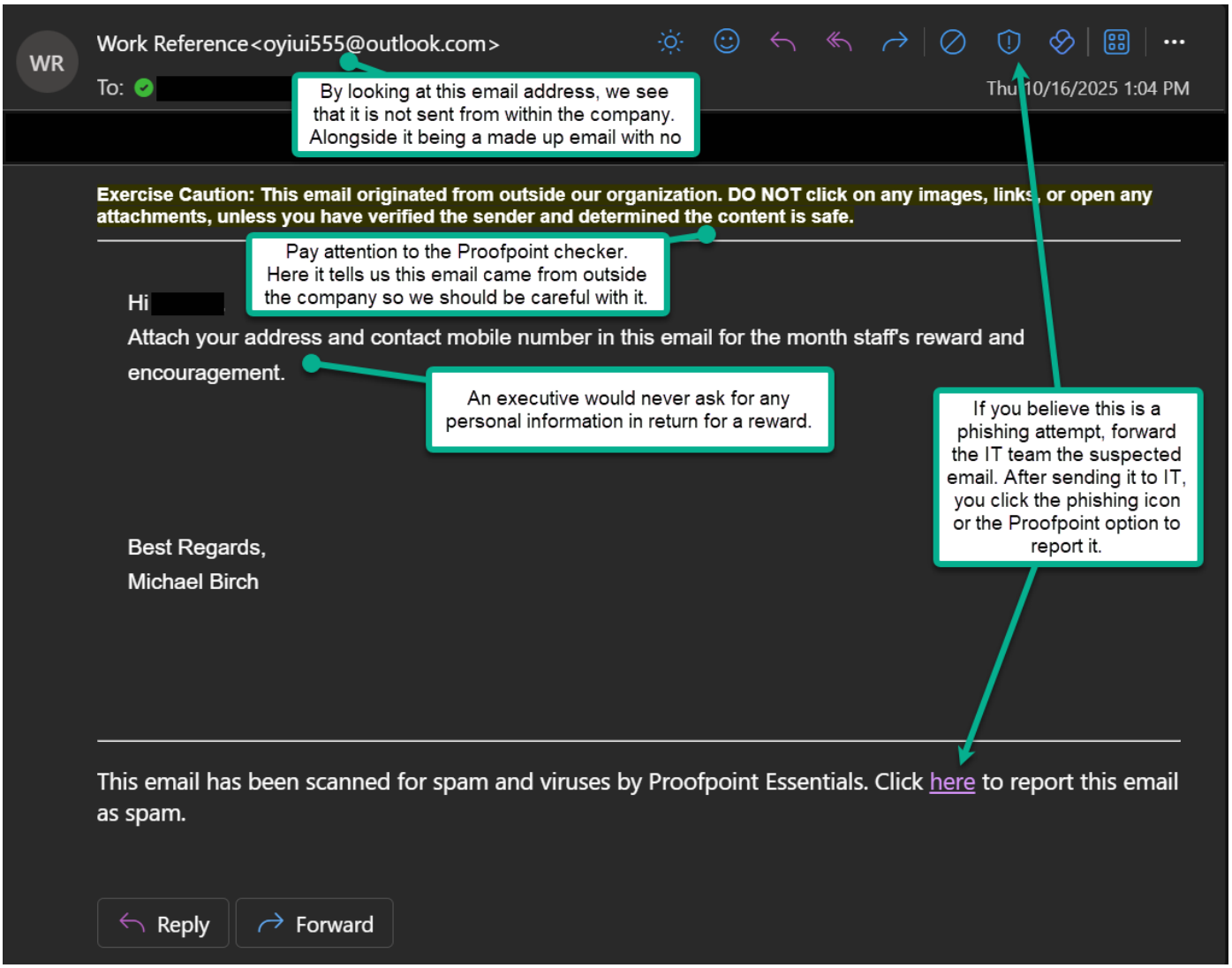
Phishing Example: Executive Impersonation - Request for Personal Information

> 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***.

Revision #6
Created 21 October 2025 16:47:20 by Tanner Bench
Updated 21 October 2025 17:48:01 by Tanner Bench