8503 Hilltop Drive, Ooltewah, TN
423.238.4171

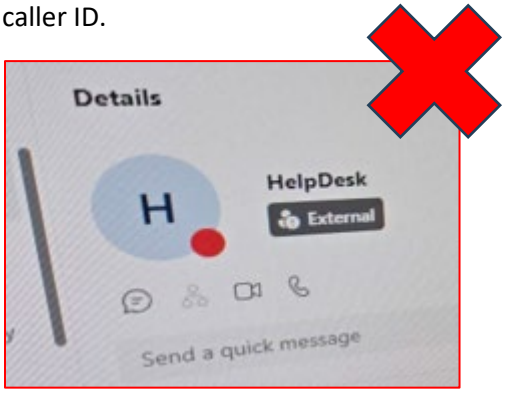
To: All Employees
From: Billy Fox, Director of IT Infrastructure
Re: Active Cyber Threat! Phishing Attempts to Look Out For!
Date: March 10, 2026

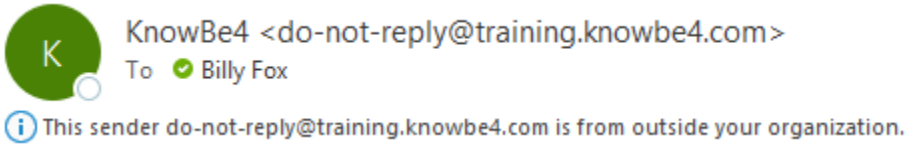
What is Happening

Scammers are attempting to contact Miller employees directly via Microsoft Teams calls, using a caller ID that displays "HelpDesk," as shown in the Teams Example below.

This is not a traditional phone call. The scammer is initiating calls by dialing employee email addresses, which is a capability within Teams.

Please be aware that although Miller IT uses the email address help@millerind.com, we will never call you from an account labeled HelpDesk, IT Support, IT Department, or Administrator. Legitimate calls from IT will always come directly from identifiable IT Department staff—not from a vague or generic caller ID.





Teams Example Email Example

How to Identify External Communications

An important warning sign is the "External" badge visible on these calls and emails.

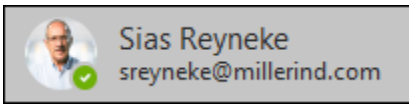
We have configured both email and Teams to clearly flag communications originating outside the organization, using indicators such as "External" or "The sender is from outside your organization," as shown in the examples above.

8503 Hilltop Drive, Ooltewah, TN
423.238.4171

When you see these badges, it means the individual you are communicating with is not affiliated with Miller Industries or its subsidiaries.

You can also help verify a person's identity by comparing their profile photo in Outlook with the one displayed in Teams, as shown in the examples below.

We include employee photos in both systems for this purpose. If the photos do not match, there is a strong possibility that the account is being spoofed. *If a message or call is marked as External and displays an employee photo, it is very likely fraudulent.*



Outlook Example

Teams Example

What to Do If This Happens

If you receive an unexpected call, message, or email—especially one marked **External**—take the following steps:

- **Do not engage.** Do not follow instructions, click links, share information, or install software.
- **End the call or conversation immediately.**
- **Report it to IT right away** by contacting me (Billy Fox), Sias, or a member of our IT staff. Another option is to email help@millerind.com and include screenshots, if possible.
- **If you have already interacted with or followed instructions, report it immediately.** The sooner we are notified, the faster we can respond and minimize impact.

Always treat externally flagged communications—whether email or Teams—cautiously. While we have been able to quickly stop and mitigate these attacks so far, incidents like these highlight the ongoing risk and underscore the importance of staying vigilant in our cybersecurity practices. Your quick action and reporting are critical to protecting Miller Industries.

Thank you for your continued awareness and cooperation.

Billy Fox
Director of IT Infrastructure
Miller Industries
423-238-4171