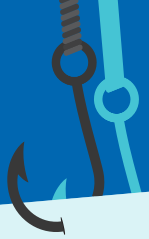


Tips for Spotting **Phishing Emails**

As your partner in all things safety, sharing knowledge across the Reciprocal and beyond is critical in helping us turn the corner on patient safety. When it comes to remaining vigilant about cybersecurity, we believe consistent training is key to mitigating risk.

Below are a few top tips for spotting phishing emails. HIROC Subscribers are encouraged to share this resource with their staff to reinforce internal education programs around cybersecurity risks.

Have questions for HIROC?

Reach out to us at inquiries@hiroc.com

Why are phishing emails a concern?

Phishing emails are one of the most common ways hackers infiltrate organizations since they target the most vulnerable point in an organization: its people.

Phishing emails can result in ransomware and malware attacks, disruption, and downtime. They can also lead to criminals accessing your email accounts, changing passwords, and gaining access to critical applications or personal health information.

Common characteristics of phishing emails

Cyber criminals and fraudsters design their phishing emails to display in various deceptive ways, such as pretending to be a member of your organization's executive team, admin, IT departments, or mask themselves as popular applications and services such as Zoom, Microsoft Teams, Outlook, UPS, Dropbox, Google, Facebook, and more.

These emails frequently contain messages with urgent requests, and may entice you to act on something, like clicking a link, downloading a file, or divulging private and sensitive information.

Tips to help spot phishing emails

- Pay close attention to the "external email" warning banner, which will display when an email is coming from outside of your organization.
  - If you do not have an email warning banner system already set up, it is necessary to do so for proper cyber hygiene.
- If you receive a message from a colleague within your organization or someone you know, but the tone or wording does not sound like them, try calling the sender or getting ahold of them in a different way first to verify with them before taking any action on the email.
- If a colleague is asking you to attend a meeting, click a link, or download a file, it will always come from an email address that is part of your organization.
  - You can check if a sender is part of your organization by looking at their domain name. A domain name is a unique, easy-to-remember address used to access websites, such as *google.com*, *facebook.com*, and *hiroc.com*. Do not click on any links from a sender that is outside of your organization without verifying first. When in doubt, pick up the phone and call your colleague to confirm.
- If there is a sense of urgency from the sender demanding immediate action on an email (this could be from someone external, or even within your organization whose email may have been compromised) – be vigilant. If you receive an attachment or link that you were not expecting, the attacker is likely trying to rush you into making a hasty mistake.
- To check if a link is phony, hover your cursor over any links or buttons to display its URL (Uniform Resource Locator). **Do not click** any unfamiliar URLs, especially from senders emailing from outside your organization.
- When in doubt, always forward suspicious emails to your organization's IT team or helpdesk for verification.

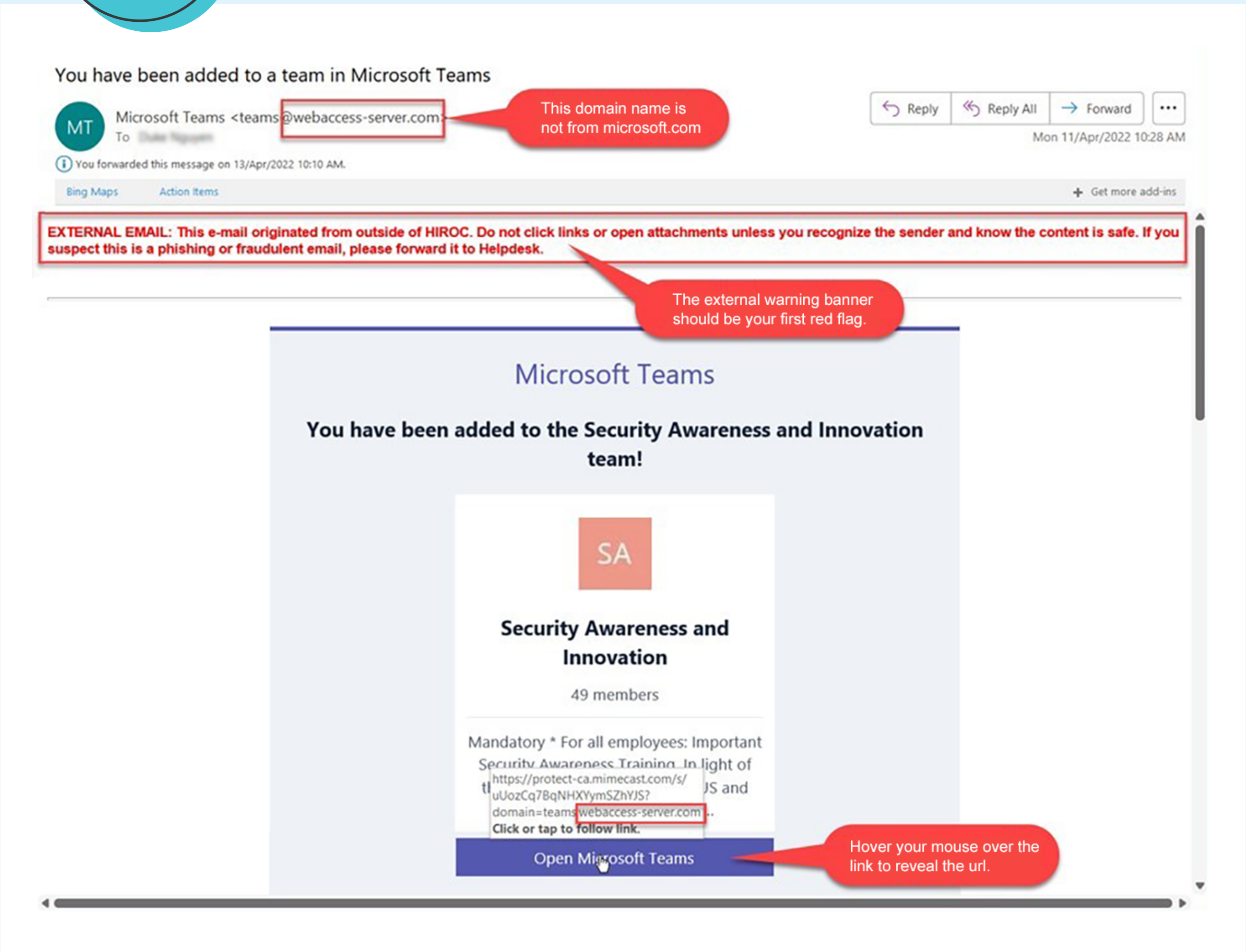
Preparing your team with a phishing test program

HIROC has a robust cybersecurity training program for its employees. HIROC employees are regularly tested with faux phishing emails created by their IT department to keep everyone vigilant and informed.

Employees are also encouraged to actively forward any suspicious emails to the IT team to verify the sender and determine whether they're safe to open.

Here are some test phishing email examples from our cybersecurity program:

example 1



You have been added to a team in Microsoft Teams

Microsoft Teams <teams@webaccess-server.com>
To [redacted]

You forwarded this message on 13/Apr/2022 10:10 AM.

Mon 11/Apr/2022 10:28 AM

This domain name is not from microsoft.com

EXTERNAL EMAIL: This e-mail originated from outside of HIROC. Do not click links or open attachments unless you recognize the sender and know the content is safe. If you suspect this is a phishing or fraudulent email, please forward it to Helpdesk.

The external warning banner should be your first red flag.

Microsoft Teams

You have been added to the Security Awareness and Innovation team!

Security Awareness and Innovation

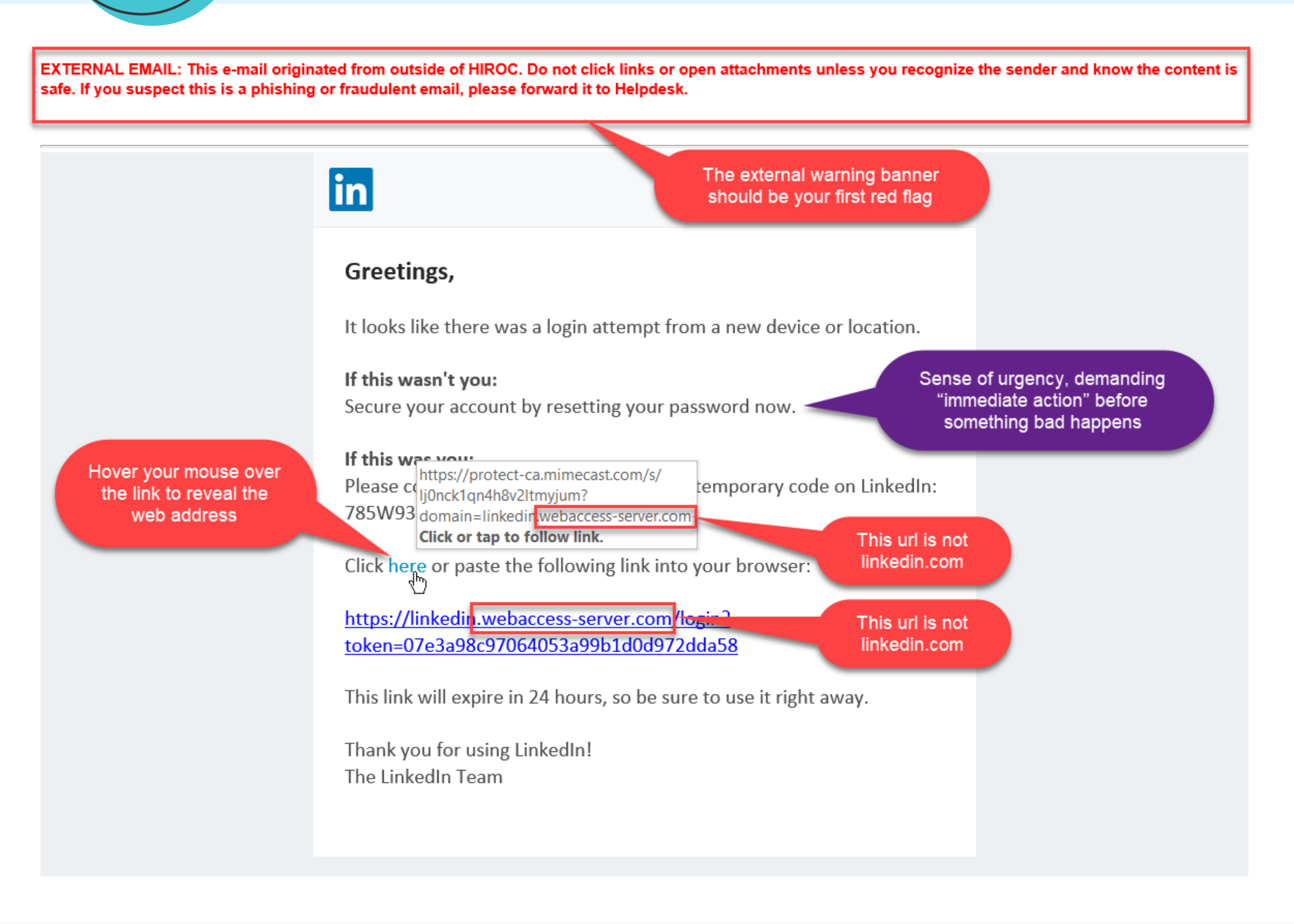
49 members

Mandatory * For all employees: Important Security Awareness Training. In light of tl JS and

https://protect-ca.mimecast.com/s/uUozCq7BqNHXYymSZhYJS?domain=teams.webaccess-server.com...
Click or tap to follow link.

Hover your mouse over the link to reveal the url.

example
2



EXTERNAL EMAIL: This e-mail originated from outside of HIROC. Do not click links or open attachments unless you recognize the sender and know the content is safe. If you suspect this is a phishing or fraudulent email, please forward it to Helpdesk.

The external warning banner should be your first red flag

Greetings,

It looks like there was a login attempt from a new device or location.

If this wasn't you:
Secure your account by resetting your password now.

Sense of urgency, demanding "immediate action" before something bad happens

If this was you:
Please c temporary code on LinkedIn:
785W93

https://protect-ca.mimecast.com/s/
lj0nck1qn4h8v2ltmyjum?
domain=linkedin.webaccess-server.com
Click or tap to follow link.

Hover your mouse over the link to reveal the web address

This url is not linkedin.com

Click here or paste the following link into your browser:

https://linkedin.webaccess-server.com/login?
token=07e3a98c97064053a99b1d0d972dda58

This url is not linkedin.com

This link will expire in 24 hours, so be sure to use it right away.

Thank you for using LinkedIn!
The LinkedIn Team

Other HIROC Cybersecurity Resources

Guide: Hosting a Successful Cyber Breach Tabletop Exercise

Planning for Cyber Security Incidents: A Crisis Communications Guide

Mitigating Your Cyber Risk: HIROC & CyberClan Share Best Practices

Cyber Risk Management: A Guide for Healthcare Providers and Administrators

Key Measures for Preventing and Mitigating Cyber Attacks and Ransomware

This is a resource for quality assurance and risk management purposes only, and is not intended to provide or replace legal or medical advice or reflect standards of care and/or standards of practice of a regulatory body. The information contained in this resource was deemed accurate at the time of publication, however, practices may change without notice.