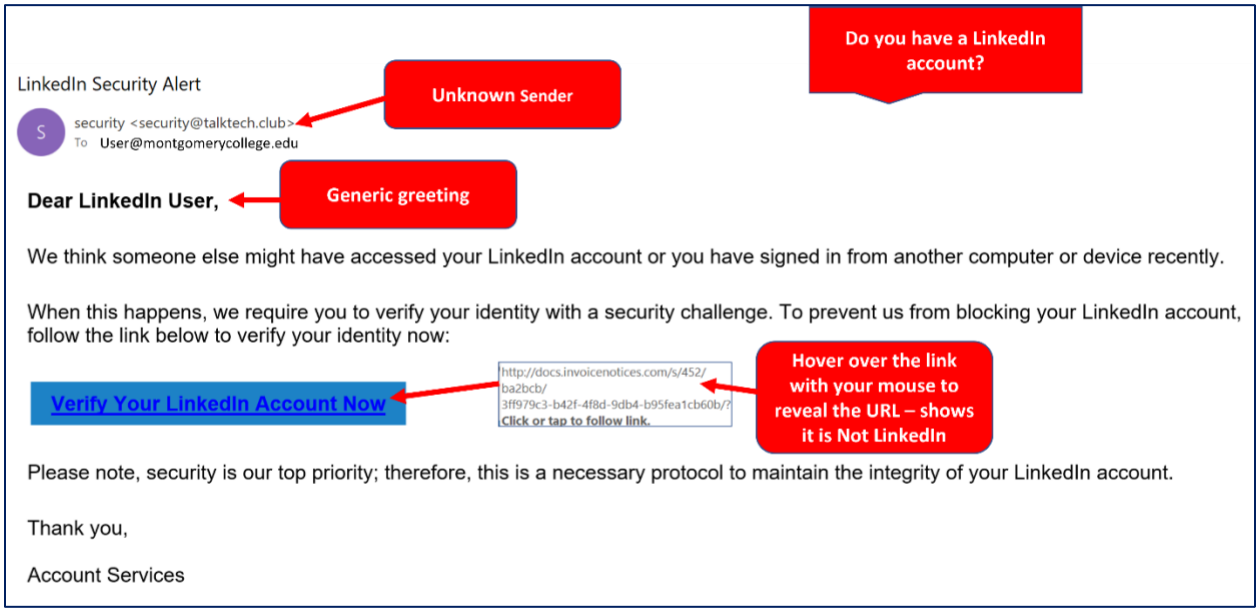
June 2021 Phishing Results: LinkedIn Security Alert

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *LinkedIn Security Alert*, which prompted you to click on a link to “verify” your LinkedIn account. Fake LinkedIn invitations are a common phishing technique. Cyber criminals frequently impersonate social networks, such as LinkedIn, by using logos, signatures, and brand colors to make phishing emails look legitimate.

868 employees reported the phishing scenario to the Phishtrap! Reporting is the preferred action as it provides IT Security the threat intel it needs to respond.

126 employees clicked the link within the training email. There were several clues within the email to help you identify this message as suspicious. Please review the email again and pay close attention to the red
flags:



LinkedIn Security Alert

security <security@talktech.club>
To User@montgomerycollege.edu

Dear LinkedIn User,

We think someone else might have accessed your LinkedIn account or you have signed in from another computer or device recently.

When this happens, we require you to verify your identity with a security challenge. To prevent us from blocking your LinkedIn account, follow the link below to verify your identity now:

Verify Your LinkedIn Account Now

http://docs.invoicenotices.com/s/452/ba2bcb/3ff979c3-b42f-4f8d-9db4-b95fea1cb60b/?
Click or tap to follow link.

Please note, security is our top priority; therefore, this is a necessary protocol to maintain the integrity of your LinkedIn account.

Thank you,

Account Services

Do you have a LinkedIn account?
Unknown Sender
Generic greeting
Hover over the link with your mouse to reveal the URL – shows it is Not LinkedIn

- Avoid clicking links in the notification email, check your LinkedIn requests and activity within LinkedIn
- Update your privacy settings within LinkedIn – review your settings to see what information is publicly available and whether connections can see your email address.
- Follow these recommended guidelines from LinkedIn to protect your account.

What should you do if you suspect an email may be a phishing attempt?

Let IT Security analyze the email for you - **REPORT** the email! The Report Phishing button within Outlook allows you to quickly report suspicious emails to IT Security.

If using Office 365 on the web, follow these steps to pin the Reporter button to your email message surface. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Complete (or revisit) DataSecurity@MC: Annual Review!

DataSecurity@MC: Annual Review training provided by SANS will teach you how to better identify common methods used by cyber attackers who try to gain access to account credentials and information systems. The range of training topics takes about 35 minutes to complete and can be accessed in MC Learns through Workday under the **MC Required Training** category.

Below are some common clues to look for in identifying a suspicious email:

- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- Check your emotions. Do not be curious and investigate the link – **REPORT** the email.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, shipping notices, and stimulus check scams.
- Trust your instincts. If the email content, sender, and link or email attachment seems suspicious, do not open it. Play it safe and REPORT it.

If you have any questions or concerns regarding this process, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology