Phishing Results: User Suspension Notice
October 2022

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *10/17/2022 User Suspension notice*. This scenario included an upgrade notice prompting users to click on the "Activate Now" link to access their Zoom account. Upon clicking the link, a web page opened requesting an email address and password.

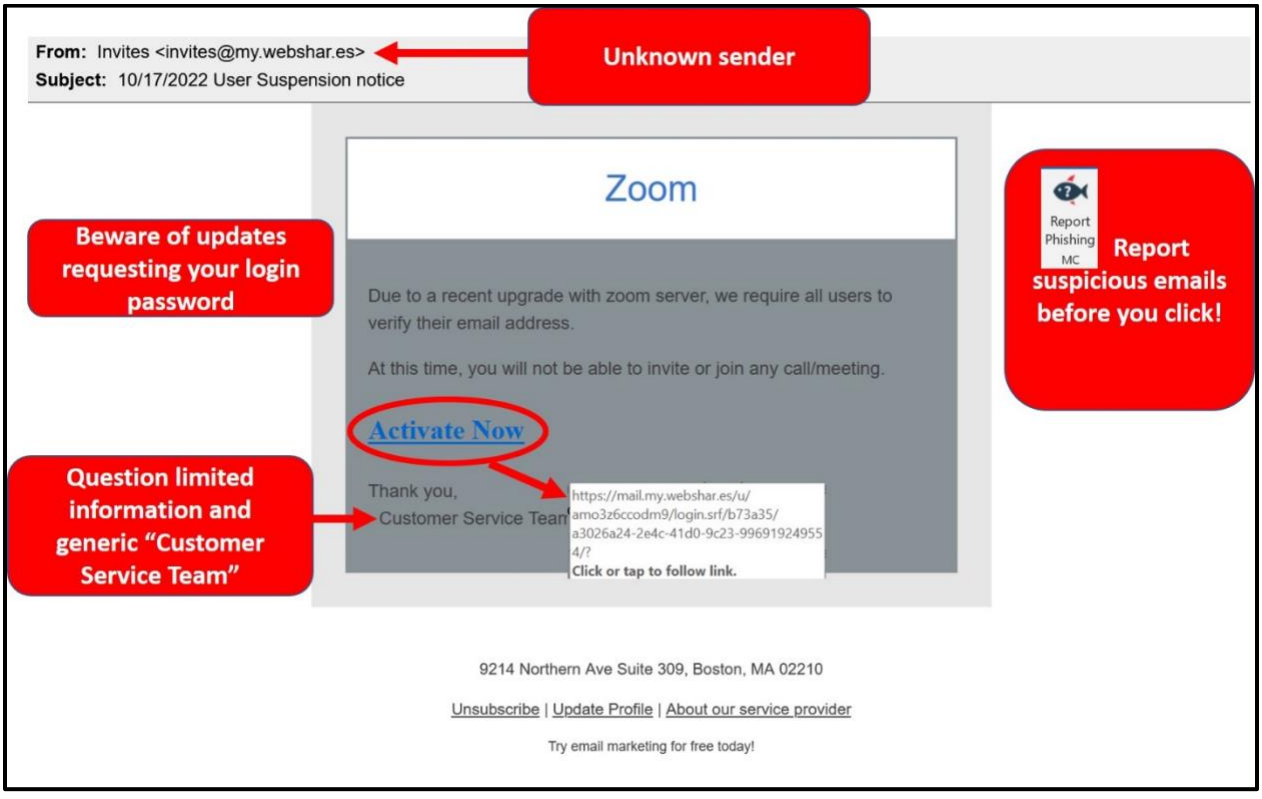
Cybercriminals use these brand impersonation scams to steal your login credentials. The email is carefully designed with an image of the brand logo to fool the recipient into trusting the communication and follow through with the request. To convince you to act in haste, the attacker includes a warning that the application will not function until you complete the request.

**Good news: 923 employees reported** the phishing scenario to the Phishtrap. **Nice work MC!**

**Opportunities for improvement: 56 employees clicked the link within the training email; of these individuals, 29 entered their credentials.**

**Did you click? In a real-world phishing attack clicking the link may have prompted you to give up your login credentials.**

Please review the clues and tips within the email to help you identify this message as suspicious:



### 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 your email client allows you to quickly report suspicious emails to IT Security. Learn how to access the Phishing Reporter button when using Office 365 at home. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Follow these additional tips to avoid phishing scams:

- Question any email request that is asking for your login credentials!
- Bookmark sites you frequently use. Instead of clicking a link, use bookmarks to navigate to your favorite sites.
- Check your emotions. Do not be curious and investigate the link – **REPORT the email**.
- Keep your MC business limited to your MC email address and use your personal email address for personal business.
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.

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