Five ways to spot a phishing attempt

Someone at the Medical Center receives a phishing email nearly every day. An attacker falsely identifies himself or herself as a trustworthy source and tries to exploit someone with an email that directs them to a fake website; usually under the auspices of being from human resources or as an email update. Despite awareness of such attacks, phishing continues to be used successfully in increasing numbers. Symantec, an industry leader in cybersecurity, reported that phishing rates decreased slightly in September, down to one in 2,644 emails (https://www.symantec.com/security_response/publications/monthlythreatreport.jsp). Email remains the number one attack method in the world of cybercrime. However, pop-up warnings, strange cold calls, and confusing search results are also phishing attempts.

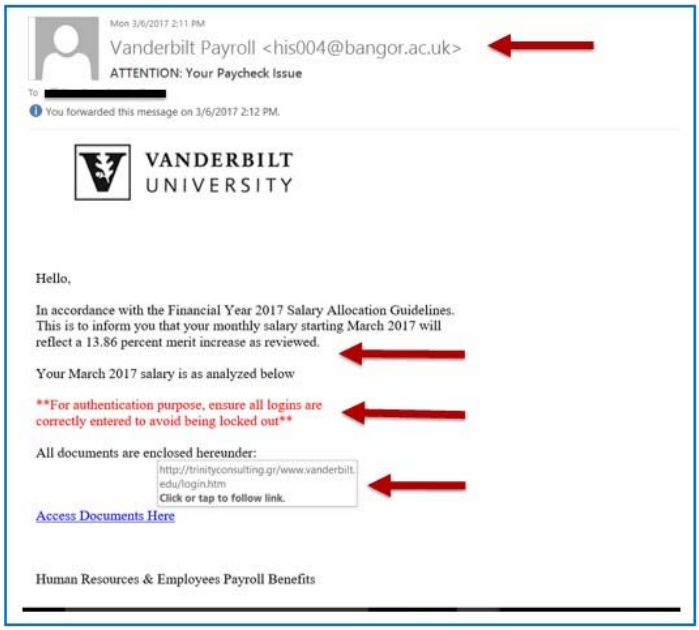
Some facts about phishing:

- 78% of people claim to be aware of the risks of unknown links in emails but click them anyway
- Phishing emails continue to be a primary delivery method for viruses and malware
- Phishing volume has grown by 33% in the five most targeted industries since 2016
- Healthcare is one of the top five most targeted industries

Why do phishing attempts continue to work when we know better?

Attackers have learned to craft their messages to prey on emotions and desires that are common to most everyone:

1. Concern: “IT has detected an issue with your account. Log-in here immediately.”
2. Confusion: “Your order has shipped. Log-in here for tracking information.”
3. Greed: “Click here to receive your free concert tickets!” Attackers make phishing attacks even more difficult to detect by customizing their message specifically for their victims. This practice is referred to as spear phishing.



For example, an attacker might craft an email to appear as if it came from the HR department and use what appears to be official company credentials. These types of messages can be very difficult, even for experienced users to detect.

The example shown here shows a potential attack on a VUMC employee and plays on concern and greed with a promised 13.86% pay raise.

You can protect yourself and VUMC from phishing attempts

The number one method to avoid falling victim to a phishing attack is continuous education and awareness of the threat. Know how attackers are tricking people and the signs to look for.

Five tips for spotting an email phishing attempt:

1. Check embedded links. Hover over the link to see the URL, but don't click it. Never click on any links or open any attachments that you are not expecting to receive.

2. Verify the display name of the sender. Do you recognize them?

3. Check the body of the message.

- Does it contain mistakes or strange language?
- Does it contain threatening or urgent language?
- Check the signature of the message. Most professional emails will have a signature line.
- Never give up personal information. VUMC will never ask for your personal information in an email.

4. If you do receive an email from someone you know that seems off, give them a call to verify they sent it to you before opening it.

5. If you are unsure about an email, call the Help Desk at 343-HELP (3-4357) or send the email to the VUMC IT Security Operations Incident Response team at phishing@vumc.org (mailto:phishing@vumc.org) and ask them to verify it for you.

The entire Medical Center workforce can play a part in identifying and eliminating the effects of phishing emails. By reporting a suspicious email, someone can protect their data, and potentially data in their department, and across VUMC. See the VUMC IT Blog at www.vumc.org/it/main (http://www.vumc.org/it/main) for more information about Cybersecurity Awareness month and how to keep VUMC data secure.