From: Gilinson, Randi D <rgilinson@uabmc.edu>
Sent: Thursday, January 28, 2021 9:02 AM
To: DOPM All Users <DOPMAllUsers@uabmc.edu>
Subject: Computer Tip of the Week -- Tips for spotting Phishing attempts

Tips for spotting Phishing attempts

Brought to you by
Byron Chancellor
- Manager of HelpDesk/IT for DOPM
(in MT-403)

QUESTION:

What are some tips for spotting Phishing attempts?

BACKGROUND:

A Phishing attempt (pronounced "Fishing") is when the bad guys "go fishing" for information from you. It has the potential of very bad results, causing huge amounts of damage to the organization you're in. It's the more evil cousin of "Spam" email.

The bad guys know all sorts of tricks, so we all have to outsmart them.

ANSWER:

1. Don't trust the display name of the email sender.
Make sure to check the email address. Just because it says it's from a name or institution you recognize doesn't mean it actually is. If the sender says he's the UAB President but the email address is uabprez123@gmail.com, then it is a phishing attempt.

2. Look but do not click.
Did you know you can hover your mouse cursor over parts of an email? Doing so may reveal additional information or information different from what the visible text says.

3. Check for spelling and grammatical errors.
Grammar or spelling mistakes can indicate that English is not the first language of the sender and are strong indicators that the email is fraudulent.

4. Consider the salutation.
Is the greeting extremely generic or broad? Does it start with "Valued Customer" or "Dear [insert title here]"?

5. Is the email asking for personal information?
Is the email asking for personal details? Are they asking for credentials? Are they asking you to go to a website and update your information?

6. Beware of urgency.
Urgent requests for information, money, or participation and input are clues that point to a possible phishing attempt.

7. Check the email signature.
Most legitimate emails will include a block signature at the bottom of the message.

8. Be careful with attachments.
Do not click on any email attachment if you have any suspicion whatsoever that an email was fraudulent or if it came from an unexpected sender.

9. Don't believe everything you see.
If something seems abnormal or strange, it's better to be safe than sorry. Report it!

10. How to report it.
Send the questionable email AS AN ATTACHMENT to either of these email addresses (they go to the same group of people): rspam@uabmc.edu or phishing@uabmc.edu
There is no shame in suspecting something that later turns out to be "real"; false positives are better than false negatives.

(If interested see original version of this at https://www.oneuabmedicine.org/web/guest/-/top-10-tips-to-avoid-phishing-attempts)

Was this helpful? Do you have suggestions for a future Tip of the Week? Do you have any other comments?
Let us know at dopmHelp@uabmc.edu

To see an archive of past Tips of the Week: http://www.uab.edu/medicine/dopm/help/totw