How to identify “phishing” emails!

NMC has seen a recent increase in the number of “phishing” emails in our nmc.edu and mail.nmc.edu accounts. What are “phishing” emails? They are emails that typically: 1) attempt to gather sensitive personal information (i.e usernames, passwords, and credit cards) 2) try to have you launch an virus/malware executable file onto your machine or 3) use popular topics to trick people into clicking on links.

Sometimes it is difficult to determine what emails are “phishing” vs. emails that are “legitimate”. Below are several recommended steps to take to determine if you have a “phishing” email:

1. Am I familiar with the sender? Does the sender identity match the email topic?
    - If the Subject is “Payroll” but the From: field appears to be from someone in the library, that should raise a red flag.
2. Does the From: name match the email address? Is there a generic greeting?
    - If the email says From: Bill Gates, but the email address says steve.jobs@gmail.com.
3. In the email, are there spelling errors, grammar errors, or broken English?
4. Are there links in the email that appear “phishy” (check by hovering over the link)?
    - An email from your bank that has links that go ANYWHERE other than to your bank’s website are probably not actually from your bank and should raise a red flag.
5. Does the email require immediate attention?
    - Even something that requires immediate attention allows you enough time to call independently and verify authenticity of the email.
6. Is the email requesting personal information, such as passwords, bank account numbers, social security numbers, etc?
    - Neither NMC nor any reputable company will EVER request that you document this sort of information in an email. If you receive an email that does, this is a huge red flag.
7. If the email is requesting you reply, does the reply email address make sense?
    - If you receive an email that says it is from NMC’s Help Desk, but the reply address is a @hotmail.com address, this should be a big red flag.

These steps are not the only way to determine if an email is legitimate or not, they are simply guidelines. If an email “feels” wrong, there’s a good chance it IS wrong and should be treated with caution.

In addition, the following links provided by Google, Microsoft, Apple, and the U.S. Government provide more detailed information. The U.S. Government link includes a section on “How to avoid being a victim.” Please take the time to review these materials as “phishing” can cause a lot of harm to your financial well-being, technology hardware, and peace of mind:

- https://support.google.com/accounts/answer/75061?hl=en
- http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx
- http://support.apple.com/kb/HT4933
- http://www.us-cert.gov/ncas/tips/ST04-014

If you are a victim of a “phishing” attack (i.e. you divulged sensitive personal information or ran a malicious .exe file on your computer) or have further questions about “phishing”, please notify the NMC Technology Help Desk immediately at 231.995.3020 or www.nmc.edu/help.