The Email Phishing Threat – Don’t Get Hooked

There has been a tremendous increase in the number of Email Phishing attempts and they are getting more malicious all the time. Please familiarize yourself with the following tips and resources to protect your information at home and at work.

Phishing Attempts are emails designed to trick you into giving up your personal and professional credentials, account information, and other identity information with the intent of stealing your identity, accessing your financial accounts to steal from you, and/or accessing professional information and systems you have access to in an attempt to steal or damage data.

If you have any question regarding an email you receive please contact the Department of Medicine IT Services for assistance:

- Phone: 206-616-8805
- Email: ishelp@medicine.washington.edu

What to do and not to do:

- NEVER open an attachment from an unknown source.
- If the context of the message doesn’t make sense, delete the message or call the sender to verify the email.
- Always be wary of messages that ask you to update your password or confirm your account.
  - This can be tricky, because both AMC and DoM IT notification of password expirations provide a link to update it.
- Report any warning messages from antivirus or other software immediately to the Department of Medicine IT Services. Some malicious websites or popups say the computer has a virus, however the links provided are either malicious or a phishing attempt. DO NOT CLICK ON THE LINK!
- Minimize the confidential information you store directly on your device. Use network storage or UW OneDrive for Business whenever possible.
- Encrypt the data and your devices. The Department of Medicine IT Services can provide assistance and advice for properly securing personal or work devices.
- Keep your operating system and software up to date (stay patched).
- Empty your email “trash bin” (Deleted Items) regularly or set it to empty automatically when you exit the program.
  - This helps by getting rid of email messages that are no longer of use and may have PHI in them.
- Contact the Department of Medicine IT Services for assistance with any devices you use for work, both personal and UW owned. For Department of Medicine workforce members, assistance with device security is provided free of charge.

Educational Tools:
• UW Medicine IT Security Phishing Awareness Announcement:  
  https://security.uwmedicine.org/Home/Communications/Phishing_Awareness_Email_041212/default.asp

• Office of the Chief Information Security Officer phishing video:  
  http://ciso.washington.edu/site/files/Phishing/story.html