Dear Johns Hopkins Community:

Some of the most damaging malware nowadays is delivered through phishing messages. Government agencies along with multiple news outlets recently reported that ransomware, a type of malware, is targeting U.S. hospitals. One of the best ways to manage ransomware is for the user community to avoid phishing attacks.

Please be cautious about any communication that asks you to perform an action such as following a link, opening an attachment, or entering login or other personal information. Attackers often use phony but realistic looking websites or email messages that appear to be from trusted businesses and brands in order to steal information or encrypt computer systems.

Valid Johns Hopkins logins almost always start with "login" followed by .microsoftonline.com or by .johnshopkins.edu.

Protect yourself and our organization from ransomware and other email scams by remembering these Do's and Don'ts:

- DO look carefully at a sender's full email address.
- DO be cautious about opening attachments, even from trusted senders.
- DON'T open an Office document (e.g., Excel, Word) for which the sender asks you to "enable a macro" or some other program.
- DON'T reply to an email, or click on links or open attachments, unless the email is from a known, trusted, and verified sender.
- DON'T click on "verify your account" or "login" links in any email.
- DON'T send passwords or any sensitive information via email.
- DON'T post your cellphone number on an internet-visible site.
- DON'T call a phone number in an unsolicited email or give sensitive data to a caller.
- DO look carefully at the URL of any site to which you are being sent.
- DO send information about phishing, spoofing, and other suspicious emails to IT at "spam" followed by @jhu.edu.
- DO send information about suspected successful fraud or theft to the corporate security department at EBPublicSafety followed by @jhmi.edu.

I appreciate your cooperation in helping to protect our collective information and networks.

Sincerely,

Darren Lacey
Chief Information Security Officer
Johns Hopkins University and Medicine