Security Awareness Tips

Phishing Emails

In order to better help identify emails received from external sources, DoIT has stamped "[External]" at the beginning of each subject line.

This should help you to determine emails that are Spam, or Phishing attempts and simply delete them. If you receive emails posing as system admins and it wants you to provide credentials or click on a link; you will now know these are not coming from an internal administration email.

Below are a few clarifications, tips, and examples to protect employees from being "phished" or scammed:

"Internal"- email addresses generally coming from a trusted email source, like NAME@illinois.gov

"External" - emails that do NOT have a @illinois.gov address.

NEVER enter your username and password in an email to ANYONE and avoid clicking on links from an external sender. If you receive an email from someone, even a legitimate looking "internal" email, and they ask for you to enter your username and password…it is a scam.

Below are some examples of phishing scams our employees have recently received. It important to remember that a legitimate email will not ask you to click on a link to "fix" a problem with your computer or email.

Examples:

To: Undisclosed recipients:
Subject: EMAIL: Confirm your email session

Hello

We need you to confirm your email session. This is a routine check to ascertain the devices you are logged on.

CLICK HERE to confirm your email session

Failure to do so may lead to log off of all email accounts

Thanks

Mail Support System.

Subject: RE: System Administrator.

Your Mailbox Is Almost Full "CLICK HERE<https://formcrafts dot com/a/21929>" Update Your Mail Box And Increase Your Account.
Thanks System Administrator.

Subject: RE: Important Staff Information

Your mailbox is full.

400MB **400**MB

YOUR EMAIL ACCOUNT HAS BEEN SUSPECTED. TO RE-ACTIVATE CLICK UPDATE-MY-ACCOUNT TO AVOID LOSING YOUR ACCOUNT.

ITS HELP DESK

If you receive an email like this in the future, please click the Submit Spam link in the upper right corner of the Outlook toolbar. In the event that you inadvertently enter your username and password via a phishing email, please contact the DoIT Security Team as soon as possible at DoIT.Security@illinois.gov.

Thank you for your assistance to strengthen our cybersecurity efforts.