SPAM - Phishing E-mails

Due to the increase in spam/phishing e-mails coming into our Inbox lately, this week's e-mail will cover this topic. (The latest, widespread spam email coming through says it's seeking a response to a Better Business Bureau complaint.)

🙂 **I know I tend to give lengthy explanations, so before I do, I'll give my short answer on this topic first:**

When in doubt of an email, never click on the link inside the e-mail. If you know the sender, verify the validity of an e-mail by calling him/her. You can also check the Cornell phishbowl, ask your local IT contact, or just delete the message. Forward any suspect e-mails to security-services@cornell.edu (and you can cc me on the e-mail as well).

Now, I'll go through more background information, do's and don'ts, and things you can do.

Cornell E-mail Security System

As part of the email system at Cornell University, they utilize an email security system that checks all arriving emails for viruses, suspect attachments and spam. Any email containing a known virus is automatically deleted to ensure no system or user is at risk of infection. (This does not mean a virus can't slip through so always be aware of unexpected attachments.)

Spam email is tested against certain spam signatures that are updated regularly.

If an email is deemed to be spam or "possibly spam" the subject line of the email will be tagged with [PMX] and then forwarded to the original recipient. Notice the pound (#) signs after the PMX in the subject line, the more pound signs the higher the spam rating. The higher the spam rating the more likely it is spam.

Filter Tagged PMX Messages

You can filter these e-mail messages marked with PMX into your Junk folder. So instead of having them clutter up your Inbox, you can check your Junk folder once in a while to verify that there are no legitimate e-mails, and then permanently delete them.

How-to video: http://screencast.com/t/qKqmW7phwKr

Click here for Step by Step Instructions for creating a filter.

Good Guidelines To Follow:

- Do NOT open attachments you are not expecting (even if you know the sender).
- Do NOT click on links provided in emails you are not expecting or have not requested, e.g. emails from companies advertising services or products.
    - **Checking a Link:** In any e-mail, it's always a good idea to hover your mouse over the link to see if the link displayed is the actual website that it's going to take you to. It's very easy to disguise a link. For example, I can include this link to http://www.google.com but in reality it's taking you to the Cornell phishbowl.
        - Go ahead and hover your mouse over this link now.
            - In your e-mail message, a little box shows you the true web address you will go to if you click on it.
            - In your web browser, if you look in the lower left corner, you can see the true web address.
    - No one (Cornell, the helpdesk, me…) should ever ask for your NetID password. It is against Cornell policy.

Cornell Help and Resources:

- **Cornell Phishbowl**
  http://www.it.cornell.edu/security/safety/phishbowl.cfm Lists some examples of phishing emails seen on campus. Do NOT assume a suspect email is safe, just because it is not listed here. There are many variants of each, and new ones are being sent out each day.
    - *Keep Cornell Alert! *If the email does not have "PMX" in the subject line and you don't see the message in the phishbowl, forward the suspect message to security-services@cornell .edu. (You can also cc: me if you would like me to be aware of it.)
    - **Verified Cornell Communications**
      http://www.it.cornell.edu/security/safety/verified.cfm List of e-mails IT Security has verified came from Cornell departments.