Email Scams

Mary Brown is a Program Coordinator in a busy administrative unit at UConn Health. She is always diligent about checking her emails and staying on top of the work of her unit. Today she received an email identified as one from UConn Health's IT team, notifying her of a required update. The title was Urgent – your action required, the sender address simply Information Technologies. When she opened the email, the message read: Dear Brown, You are required to log in to read an urgent message from IT. This message was followed by a link that directed her to "log in here".

Mary assumed this was a broadcast message generated by UConn Health's IT team (which is why her last name was used, rather than her first). She paused momentarily and wondered about the sender name of "Technologies" since she knew that UConn Health's department is referred to as Information Technology. Then she remembered a message that is circulated at least a few times each year from the IT Department at UConn Health. That message told employees that IT will never send emails with links or attachments requiring you to enter log-in information and warned against doing so. She decided that she should contact IT and ask about the email. Did she do the right thing?

Answer:

The answer is a resounding YES, Mary did the right thing. Her caution paid off too. The email with the link was a malicious attempt to gain access to Mary's log-in information that the scammer could then use to access UConn Health systems. This could have had severe implications for the institution and our systems.

This type of scam is called a "**Phishing"** attempt and is usually an attempt to fraudulently obtain private information (in this case Mary's log-in information for access to UConn Health systems). There are some important lessons employees should all remember when using email. Smart email practices are actually prevention strategies that will help to keep UConn Health's systems free from hackers and scammers.

There are many examples of medical centers falling victim to various malware attacks. As recently as February 2016, a hacker gained access to California-based Hollywood Presbyterian Medical Center's electronic medical record (EMR) system. The medical center was forced to pay off the hackers who held the hospital's data for ransom in order to obtain the information necessary to regain access to the EMR. Attacks such as these can be initiated by phishing scams.

What can one person do?
Be suspicious of any email message that asks you to enter or verify personal information via a link/attachment or response to the email. Never reply to or click the links/attachments in messages like this. If you think the message is legitimate, go directly to the company's website or contact the company to see if you really do need to follow the directions in the email message.

Be wary of any email that urges immediate action, threatens to cut off your access or requires you to enter personal information.

The following types of messages may give you clues that they are phishing attempts:

- A message directly from a company UConn Health does business with that doesn't seem to relate to the work you do with the company.
- Messages with sensitive topics where more than one person is in the To: or cc: line. This includes requests for log-in information, personal information or account info for work that you are doing.
- Messages requiring a reset of your username or password.
- Messages with an attachment but no text in the body.
- Messages with many misspelled words or misplaced word tense use.

The best practice when you recognize a phishing attempt is to delete the email message from your Inbox, and then empty it from your deleted items folder. This ensures you won't be able to click on a link or attachment accidentally. Notify the IT Department immediately.