September 2014

Attention All CABQ Staff,

Be aware, there is another phishing email circulating to staff.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication such as email.

As always, take caution when you receive an unsolicited email with a link asking for login or other personal information.

Best practices to protect your information are:

- Never give out your password to anyone
- Do not reply or provide personal information to an unsolicited email
- Do not click on email attachments from an unsolicited source
- Do not post personal information anywhere online.
- Do not provide personal information to an anonymous phone caller
- Use caution in Social Media sites. Do not share personal information with anyone online.

Here is an actual phishing email received within CABQ:

From: *George Benoit [mailto:GBenoit@southlandind.com]*
Sent: *Thursday, September 11, 2014 4:40 AM*
To: *Undisclosed recipients*
Subject: *ITSERVICEDESK!!! IMPORTANT SECURITY INSTALLATION*

Outlook new security updates will begin installation on the new microsoft web access (SME/SSL) server protection validation protocol, this will ensure all communications within the organization and outside organization are fully encrypted from third party unauthorized connections which sometimes causes mail undelivery to outlook webmail of an individual, therefore disabling server filters.

*To enable security updates to be installed successfully, webmail authentication is necessary**

Click here for ITsecure SSL/1134 page and validate connection access.
http://(unknown url)

Please bear in mind you might experience loss of mail connectivity to access webmail and delayed mail delivery for sent message during this time frame, all access will be restored on complete installation. Thanks for your corporation.

ITservicedesk Management.

What are the signs to look for?

There are many signs to look for to help identify a phishing attempt.

This list identifies some of the typical method which can be seen to help identify a phishing attempt on an email. Most Phishing emails will have several items listed.

1) **From:** Unknown email sender[mailto:unknown domain name]
2) **To:** Sending to everyone, shotgun the email out to everyone
3) **Subject Line:** Seems important or urgent, designed to grab your attention
4) **Topic:** Typically a threat or scare tactic is employed to emphasize the urgency to act or designed to intimidate the recipient. This can come in the form of an "either, or" senario.
5) Asking you to authenticate or put in your personal information and password.
6) Gives you the url to enter your credentials
7) Makes it look official. Has an official name or title
8) Often times, misspelled words or incomplete sentences.

Let's take a look at the phishing email again:

Below is the same email in which signs are highlighted in red.

From: George Benoit [mailto:GBenoit@southlandind.com] (unknown sender)
Sent: Thursday, September 11, 2014 4:40 AM

*To: Undisclosed recipients (*no specific recipients, trying to get to everyone)

Subject: ITSERVICEDESK!!! IMPORTANT SECURITY INSTALLATION (Seems important to grab your attention and make you want to act immediately)

Outlook new security updates will begin installation on the new microsoft web access (SME/SSL) server protection validation protocol, this will ensure all communications within the organization and outside organization are fully encrypted from third party unauthorized connections which sometimes causes mail undelivery to outlook webmail of an individual, therefore disabling server filters. (Subtle threat, either update or your email could be compromised)

*To enable security updates to be installed successfully, webmail authentication is necessary** (wanting you to type in your credentials)

Click here for ITsecure SSL/1134 page and validate connection access.
(some url http:fakewebsite.com/) (Link to a fake website to steal your credentials)

Please bear in mind you might experience loss of mail connectivity to access webmail and delayed mail delivery for sent message during this time frame, all access will be restored on complete installation. Thanks for your corporation. (Stall tactic makes you think all is well. Your credential have been stolen and your email has been compromised at this point)

ITservicedesk Management. (Sounds official but doesn't seem right. When in doubt, call the service desk to verify)

The phishing emails can be crafty and are tricky to spot initially. With time and knowing what to look for, the phishing attempt will be quickly identified.

If you are in doubt, do not click on the link, call the ITSD Service Desk at 768-2930 and verify.