Phishing – How to Avoid Getting Hooked!

From the Desk of Shawn Ridenour, Help Desk Director

Here are some examples of recent PHISHING emails.

Example 1: Notice that it is from an account named HELP DESK. However, the email address associated with the account named HELP DESK is controldesk01@admin.in.th. All formal communications from the SE Help Desk will originate from an account named * Help Desk * with the email address helpdesk@se.edu. In addition, this phishing email has all the key indications that it is a phishing scam. Note this dead giveaway: “you must reply to this email immediately and enter your current E-mail and password here and send to (help_desk@admin.in.th) (E-mail:........Password:........ confirm password:........) Failure to do this within 48 hours, your account will be deactivated from our data base.”

-----Original Message-----
From: HELP DESK [mailto:controldesk01@admin.in.th]
Sent: Monday, February 20, 2012 11:17 AM
Subject: What is Password Expiration?

What is Password Expiration?
For the purposes of increasing security on the EIMS system and to introduce users to their directory-based identity (Enterprise ID), a password expiration policy has been implemented that affects your EIMS Directory Name and email address and/or your Enterprise ID. Distribution List and Service Account passwords are not included in this policy.

How often will my password expire?
Your password will expire every 120 days. If you do not change your password before it expires, you will no longer be able to access your Enterprise ID or Enterprise-based accounts.

How can I change my password?
To change your password, as well as update your directory information, select your site’s Personal Administration Tool from the appropriate linking PAT. To maintain your account, you must reply to this email immediately and enter your current E-mail and password here and send to (help_desk@admin.in.th) (E-mail:........Password:........ confirm password:........) Failure to do this within 48 hours, your account will be deactivated from our data base. Remember to re-set your password after this 48 hours update.
Example 2: Notice that this account is sent from John Doe (I removed the actual employee’s name) an actual Southeastern employee. Do not be fooled by this. It is common for proprietors of phishing scams to utilize an exploited account to then send phishing emails to others within the organization. This provides some degree of legitimacy to the phishing email. Otherwise, notice how easy this email is to identify as a phishing scam. It has all the trademarks of a phishing scam. Also, notice the dead giveaway of, ‘Auburn, Alabama 36849’. Obviously, the SE Help Desk is located in Durant, OK and not Auburn, AL.

From: jdoe@se.edu  
Sent: Monday, February 20, 2012 2:33 AM  
Subject: Exceeded Email Quota.

Important notice from the helpdesk  
Your E-mail box has reached its maximum limit of 20 GB of storage and  
Your account will be disabled if you do not update now.  
To upgrade your account, please click the link below:  
CLICKHERE  
Your account will remain active after we have confirmed your account successfully.  
| Auburn, Alabama 36849  
© Copyright 2011 Regulation

Example 3: Below is the phishing email that was most successful against our SE computer users. Notice that it comes from a seemingly legitimate account named, ‘Southeastern Oklahoma State University Webmail Administration’. However, as with the earlier examples notice that the email address associated with the account is rmfeltz@quadro.net. Again, all formal communications from the SE Help Desk will come from an account name * Help Desk * with the email address helpdesk@se.edu. Also, notice that the email was ended with the line, ‘@2012 all right reserve-Southeastern Oklahoma State University Webmail Administration’. The customization of this phishing email specifically for Southeastern is a growing trend. Do not be fooled by these tactics. This email still contains the trademark signs of a phishing email. It is attempting to get users to click the link and provide their login credentials.

From: Southeastern Oklahoma State University Webmail Administration. [rmfeltz@quadro.net]  
Sent: Thursday, February 16, 2012 5:05 AM  
Subject: PLEASE CONFIRM SECURITY CHECK

ATTENTION:  
Thur 16 Feb 2012 08:16:22 MYT from 41.206.151.183, your account was recently accessed with this details, please if u recognize this details,ignore this message, or use this web link to reconfirm your
account details to prevent spammers and unauthorized users to gain access to your account;

http://www.wrdom.com/dom/use/WebmailCustomerCare/form1.html

@2012 all right reserve-Southeastern Oklahoma State University Webmail Administration.

Example 4: Here is one more example. This one is similar to the second example with a slight variation.

Your mailbox is almost full
20GB 23GB
Current size Maximum size

Dear Webmail user,
Your Webmail Quota Has Exceeded The Set Quota/Limit Which Is 20GB.
You Are Currently Running On 23GB Due To Hidden Files And Folder On Your Mailbox.
Please Click the Link Below To Validate Your Mailbox And Increase Your Quota.

http://pastehtml.com/view/bmhoe6pn2.html

Failure To Click This Link And Validate Your Quota May Result In Loss Of Important Information In Your Mailbox Or Cause Limited Access To It.

Webmail Upgrade Support Team 2012

These are all examples of phishing scams that were successful against SE users. All Southeastern IT professionals ask that you be aware of these phishing scams and do your part to avoid getting hooked. Thank you!