Welcome to the Aquarium

Here for your education is a collection of actual phishes received by University users. These historic phishes have been annotated to show you how to spot the tell-tale signs of a bona fide phish. Send me your phish and perhaps we can find it a good home here in the Aquarium.

2012-04-19

From: Dr Steuart Henderson  
Sent: Thursday, April 19, 2012 11:11 AM  
Subject: Webmail Centre

It was noticed that you have exceeded your Email Quota Limit of 450MB and you need to expand your quota. In less than 48 hours if you haven’t upgrade your Email Quota Limit, your email account will be disable.

To expand your email quota limit to 5GB, use any of the below web links:

http://www.citrusolutionla.com/forms/use/Admin/form1.html

Thank you for your understanding.

Copyright ©2012 Helpdesk Support Webmail Centre. This email as been signed and verified by Webroot Email Security Service.

Comment [LC1]: Sender is from Australia.  
Comment [LC2]: Bad English, sense of urgency  
Comment [LC3]: Who/what the heck is “citrusolutionla”? A juice bar in California?  
Comment [LC4]: So our email is being administered by the University of Maryland?  
Comment [LC5]: This is just plain silliness.  
Comment [LC6]: The sender’s email address is not at “tamucc.edu”  
Comment [LC7]: No name

2012-03-07

This is perhaps the most clumsy and obvious phish that one will encounter:

From: Tamucc Helpdesk  
Sent: Wednesday, March 07, 2012 3:15 PM  
Subject: Verify Account

Attn: The school webmail system is undergoing an Account upgrade process. You are required to provide your webmail account username and password for verification or your account will be deleted from the
school webmail database
Username: 
Password: 
Tamucc Helpdesk.

2012-03-08
Not as ham-fisted as #1, but not much better either.

From: Adam May [mailto:cb10apm@brunel.ac.uk]
Sent: Thursday, March 08, 2012 12:35 PM
Subject: OWA Account to be disabled in 24 hours

Dear User,

As part of our regular maintenance done on the exchange mail servers, Microsoft System Administration is currently working to improve on the security, functionality and performance of all our Microsoft Outlook Webmail Access Accounts as we periodically review certain Accounts which are vulnerable to Unauthorized Access or has not been used/accessed over a period of time will be deleted to conserve storage. However, your Account has been detected and queued up to be deleted from our DB. Please note that the mail in the deleted mailboxes will NOT be recoverable.

To remove this limitation and initiate your Account Update and activation process, please click here <https://docs.google.com/spreadsheet/viewform?formkey=dFFmcURY2nTdThjZHOfWiiRUfTWixH206EQ> and complete the request Form.

Thank you for your co-operation
Webmail Management Team

2012-04-12
A little more sophisticated.

From: TeXaS A&M University CORPUS CHRISTI [loja@precolandia.com.br]
Sent: Thursday, April 12, 2012 8:45 AM
Subject: Dear islander.tamucc.edu user

Dear islander.tamucc.edu user

Due to anonymous registration we are shutting down some unused account, to avoid your account been deleted from our data base kindly click on the link to upgrade and reconfirm your email account.

https://docs.google.com/spreadsheet/viewform?formkey=dFNVeWsxMmd5MzIaG14Rm11WVJTVC6EQ

We apologize for any inconveniences.
Email service Term