Security :: Spam and Phishing Scams

Phishing [1] scams are attempts by hackers and cyberciminals to steal personal information or hijack computing resources for nefarious purposes. The most common (and most successful) phishing scams are emails that appear to come from a legitimate source (for instance, HSU Technology Help Desk, your bank, eBay, PayPal), and which contain a link that directs you to equally legitimate-looking web pages. These emails almost always ask you to verify some detail about your account by going to this legitimate-looking web page and entering your account credentials or other personally-identifiable information.

If you provide personal information on these sites, you risk losses through fraudulent use of your credit cards or bank accounts, even full-blown identity theft. If you give out your HSU User Name [2] and Password, you're giving out easy access to the entire HSU network. More often than not, this results in HSU network resources being used to distribute spam, which in turn leads to email from humboldt.edu being blocked by ISPs and major companies. This means that until the particular situation is discovered and rectified by HSU and resolved, anyone with an email address in the domains that have blocked humboldt.edu will not receive email sent from Humboldt State University.

The reality is that no bank or other financial institution, or the HSU Technology Help Desk, or Microsoft, is going to send this kind of request by email, because they know that it's an insecure way to transfer confidential information. These emails and websites are simply fronts for stealing your identity or using your computer's processing power to send spam. If no-one ever believed them, they would stop sending them. But because there's always someone who acts on these requests, they keep coming.

Here are just a few examples that have been directed at Humboldt State University users [3].

What You Can Do

To avoid becoming a victim of a phishing scam, just stop and think any time you find yourself tempted to click on a link in an email. Does the email contain spelling mistakes? If you hover your mouse over the link, does it display a different URL than you would expect from that sender? Check the web address in the address bar. If the website you are visiting is on a secure server, it should start with "https://" ("s" for security) rather than the usual "http://"; look also for a lock icon on the browser's status bar. And never, ever, volunteer your HSU User Name and Password in an email.

Keeping your antivirus software up-to-date will go a long way towards protecting you against phishing attacks. Take advantage of HSU's Sophos Anti-Virus [4] campus-wide license to protect both work and home computers at no cost to you. You can also educate yourself about identifying fraudulent messages - check out these games and quizzes for a fun way to learn more:

- http://www.opendns.com/phishing-quiz/ [5]
- http://wombatsecurity.com/phil.php [6]
- http://www.sonicwall.com/phishing/index.html [7]
- http://www.onguardonline.gov/games/phishing-scams.aspx [8]
  [9]

If you do accidentally send your HSU User Name and Password via email, immediately change your password in the Account Center [10] and call the Technology Help Desk at (707) 826-HELP (4357) so they can take action to prevent problems.

What HSU is Doing to Help

The Gmail spam filtering [11] uses a variety of mechanisms to identify and block messages containing certain key words and phrases that indicate spam, and to lock accounts out of the network that appear to be being used for spamming. Google's spam filter also makes extensive use of Real Time Black Lists (RBLs) [12] - independently-maintained lists of IP [13] addresses known to regularly send spam. If any organization does block the humboldt.edu domain, ITS reaches out to them to re-restablish a connection, and is continuously updating anti-phishing strategies to best protect everyone.

Related Topics

Data Protection [14], Security [15]

Source URL: http://www.humboldt.edu/its/security-phishing

Links:
[1] http://www.humboldt.edu/its/glossary/5#term202
[2] http://www.humboldt.edu/its/glossary/5#term99
[3] http://www.humboldt.edu/its/security-phishingexamples
[4] http://www.humboldt.edu/its/security-virusprotection
[5] http://www.opendns.com/phishing-quiz/
[6] http://wombatsecurity.com/phil.php
[7] http://www.sonicwall.com/phishing/index.html
[8] http://www.onguardonline.gov/games/phishing-scams.aspx
[9] http://www.washingtonpost.com/wp-srv/technology/articles/phishingtest.html
[10] http://accountcenter.humboldt.edu
[11] http://www.humboldt.edu/its/security-spam
[12] http://www.humboldt.edu/its/security-rbl
[13] http://www.humboldt.edu/its/glossary/5#term250
[14] http://www.humboldt.edu/its/category/quicklinks/data-protection
[15] http://www.humboldt.edu/its/category/quicklinks/security