PENNSYLVANIA STATE POLICE
COMMUNITY AWARENESS BULLETIN
CAB 04-12 October 19, 2012

APPLE ID PHISHING SCAM

(U) Phishing is the criminally fraudulent process of attempting to acquire sensitive information, such as usernames, passwords, and credit card information, by disguising electronic communications to appear as if the request came from a trusted source. Techniques utilized to "phish" for information include accessing webpages and installing key loggers, root kits, and other forms of malware.[i] Phishing often involves spoofing, which occurs when a forged email appears to be sent from someone other than its true source. The spoofed emails are used to gain the potential victim's trust and convince him to provide personal information, including passwords, credit card numbers, and bank account information.[ii]

(U) Recently, Apple users have received emails that appear to be part of a phishing scam. The message informs the recipient that his Apple ID has been temporarily suspended and instructs the user to click on a link to a remote site that requests his account and password information. The remote site is not authentic and is used to collect the victim's sensitive and personal information.[iii] A typical message states:

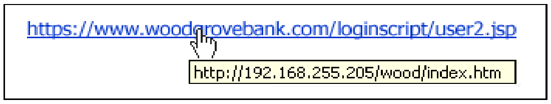
> *Your Apple ID has been temporarily suspended! Somebody else just tried to sing [sic] in into [sic] your Apple account from another IP address. Please re-confirm your identity today or your account will be suspended due to concerns we have for the safety and integrity of the Apple Community. Please click here to Activate your Apple ID [link].*

CONCLUSION AND RECOMMENDATIONS

(U) This particular phishing scam attempts to collect usernames and passwords, although it is unknown how the perpetrators will exploit the information they obtained. Internet users should safeguard all their login information and never give it to anyone. Legitimate companies will never ask for your login information by email. Individuals who have already fallen victim to this particular scam should immediately change their Apple password.[iv]

(U) General signs indicating a phishing scam are:

- Misspelled words and poor grammar in the body of the email. Notice that in the example provided above, users are advised that someone tried to "**sing** into" their account, not "sign in."
- Links located in the message. Before you click on any link, hover over it with your mouse, but do not click. If you see a string of numbers instead of the website name, it is most likely illegitimate.



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

- Threats located within the message. Emails will state that your security is compromised or that your account will soon be suspended.
- Popular companies are typically chosen to be the front for a phishing scam, e.g. Apple, Microsoft, Facebook, etc.[v]

(U) The United States Computer Emergency Readiness Team (US-CERT) provides the following recommendations to minimize the chances of becoming a victim of an email scam:

- Set your email to automatically filter spam.
- Install anti-virus software and keep it updated.
- Install a firewall, set it to the highest level, and keep it updated.
- Do not open an email attachment or click on a link in an email from someone you do not know.
- Do not click on an email attachment that ends in .exe. It is an 'executable' file and, once downloaded, can do what it likes in your system.
- When links sent in an email take you to a webpage and require you to login, do not provide any information. Always type in the domain name yourself or use your bookmarked links.
- Require emails from IT or Help Desk personnel to always have a name and contact number.
- If a "single sign-on" system is used, consider requiring additional and different passwords to access personal information stored in databases.[vi]

(U) Individuals should report phishing scams to US-CERT at phishing-report@us-cert.gov and the Internet Crime Complaint Center (IC3) at www.ic3.gov.

[i] Wolfe, D. (2009). Cybersecurity attacks on the critical infrastructure. *Proceeding of the 2009 Unrestricted Warfare Symposium.* Retrieved 10/18/2012 from http://www.jhuapl.edu/urw_symposium/proceedings/2009/Authors/Wolf.pdf.

[ii] Internet crime schemes. (n.d.). *Internet Crime Complaint Center.* Retrieved 10/18/2012 from http://www.ic3.gov/crimeschemes.aspx.

[iii] Kovacs, E. (2012, October 10). Experts warn users to beware of "Apple ID Cancelled" phishing scam. *Softpedia*. Retrieved 10/18/2012 from http://news.softpedia.com/news/Experts-Warn-Users-to-Beware-of-Apple-ID-Cancelled-Phishing-Scam-298468.shtml.

[iv] No sanctuary for Apple users: New phishing scam. (2012, October 15). *Northern Arizona University*. Retrieved 10/18/2012 from www.nau.edu/its/news/applephishscam.

[v] How to recognize phishing email messages, links, or phone calls. (n.d.). *Microsoft.* Retrieved 10/18/2012 from http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx.

[vi] Recognizing and avoiding email scams. (2008). *US-CERT*. Retrieved 10/18/2012 from http://www.us-cert.gov/reading_room/emailscams_0905.pdf.