10 Tools to Protect Against hishing Attacks

Phishing *is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.*

1. Treat all emails as suspect

Email is not 100% verifiable – they can be forged or spoofed to look like they are from a legitimate source such as a banking institution.

2. Read email subject lines and salutations for suspect phrases

"Dear Valued Customer. Urgent! Your attention is needed! Congratulations! Dear Account Holder." These are just a few of the common subject lines phishers use to grab your attention. If your banking institution did want to contact you by email, don't you think they would address you by your name? Read every email very closely!

3. Do NOT open attachments!

Simply opening an attachment could infect your computer with harmful viruses, worms, trojans[i] and malicious software.

4. Do NOT use forms embedded in email

If you receive an email asking you to fill out personal information such as: a username and password, date of birth or Social Security number-be cautious, it could be a scam. You have no way to verify where your information is really going and who is receiving it.

5. Watch out for emails written in poor English

Many scams originate from countries where English is a second language such as various Soviet countries, central and south Asia, and Nigeria. A legitimate businesses email would most likely not have spelling and grammatical errors.

6. Do NOT click on URL's[ii] and links in emails

If you receive an email which includes a link directing you to a webpage or website (i.e.: a banking institution) do not click on it. Scammers often recreate false sites which mirror the real ones. By clicking on these URL's and links embedded within an email you may be directed to a false, unsecured website.

7. Verify URL's & the presence of encryption before entering personal information

You can always ensure you're directed to a legitimate website by typing it in yourself. Also check for signs that the site is protected and encrypted. Does the website have a "secure padlock" in the lower right corner which signifies the website is secure and encrypted[iii]? Does the website start with, "https" indicating the site is secure?

8. Continue to monitor your credit report for unauthorized activity

You are entitled to one FREE credit report each year. www.annualcreditreport.com ***or check with your banking institutions for additional services on credit/fraud monitoring.***

9. If you are a victim-report any suspicious activity immediately

Contact your local police department, financial institutions and the Federal Trade Commission for reporting suspicious activity and obtaining assistance.

10. Keep your computer operating system up-to-date

Always run updates for software/security upgrades. Consider the use of antivirus, firewall[iv], malware[v] software.

California State University, Northridge
Police Department
Crime Prevention & Community Relations Unit
(818) 677-5820 or 7922
http://www-admn.csun.edu/police/crime

[i] A **trojan**, is malware (see malware below) that appears to perform a desirable function but in fact performs undisclosed malicious functions. Therefore, a computer worm or virus may be a Trojan horse. The term is derived from the classical story of the Trojan Horse of the Trojan war.

[ii] **URL** (**U**niform **R**esource **L**ocator) is the common way to get to a Web site is to enter the URL of its home page file in your Web browser's address line.

[iii] This padlock feature is only used on Internet Explorer web browser.

[iv] A **firewall** is a device or set of devices configured to permit, deny, encrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

[v] **Malware**, also known as *Malicious Software*, is software designed to infiltrate or damage a computer system without the owner's informed consent.