Cheatography

Identity Theft: Phishing 101 Cheat Sheet

by [deleted] via cheatography.com/2754/cs/7531/

Introduction

Phishing are emails that are specifically designed to attract the user to open a link or document that will launch a virus or attack on the user's computer with the intent to steal data or demand a ransom..The message are typical disguised as important must read messages.

What are phishing’s telltale signs? Although phishing emails have become more sophisticated, some criminals still make spelling and grammar mistakes. More subtle clues are URLs with spelling errors or the wrong domain — .com versus .org, for example. Here's a handy guide to phishing vocabulary, and ways that stolen data can be used.

Credit: http://www.hhnmag.com/articles/6921-phishing--

Phishing Vocabulary

Phishing: An electronic communication from what looks like a trustworthy source that seeks to obtain victims’ sensitive information — computer username and password, or credit card, Social Security or bank account numbers — for malicious intent.

Spear phishing: Phishing targeted at specific individuals. Attackers first gather intelligence about the target to make the deception more believable and increase the likelihood of success. The criminal might connect with the victim on social media to glean information and foster trust.

Whaling: Spear phishing targeting a high-profile person, such as a hospital executive.

Social engineering: A non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.

Nation-state actors: Targeted intrusions into your specific computer network by an organized group of hackers to collect information from any organization with valuable data, like hospital medical records.

Hacktivists: Computer hackers who join groups like Anonymous in order to demonstrate their dissatisfaction with powerful organizations such as corporations and governments that fail to share their views.

Malware: An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware and other malicious programs. It can take the form of executable code, scripts, active content and other software.

Phishing Red Flags

Get smart on Phishing! Learn to read links!

Phishing are fake messages intended to lure you to fake websites that are made to look like e.g. a bank website, but in reality set up by data thieves. If you fill in forms on those sites, you will give all your information to criminals and invite indentity theft, credit card fraud, cleaned out bank accounts etc. This is called "phishing"

Learn how to identify links to fake sites, so you will not be fooled! http://www.bustspammers.com/phishing_links.html

Ways Cyber Criminals Use Data

Medical record theft: Cyber criminals steal patients’ health records to sell them on the black market.

Medical identify theft: Criminals use patients’ stolen health record information to gain personal access to medical treatment, to acquire prescription drugs for personal use or sale, or to make false claims against patients’ insurers.

Identity theft: Criminals sell or personally use employees’ or patients’ credit cards, bank or Social Security numbers to open and max out credit cards, clean out bank accounts and commit tax fraud.

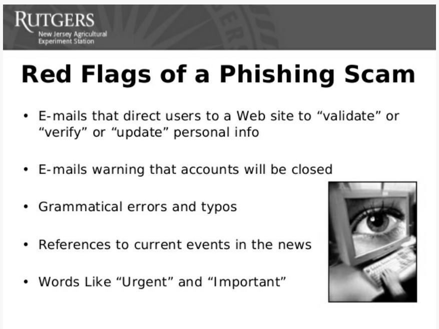
Industrial espionage: Criminals steal a hospital’s intellectual property in areas such as medical technology innovation, clinical research and business practices.

Protection Against Phishing

Avoid eMail Attachments. Never open attachments from unknown source or known companies that you do not usually correspond with.

Firewalls: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Spam Filters: These filters prevent unsolicited emails from clogging your inbox with these downloads. Spammers are often attempting to steal personal data by sending spoofed spam emails which mimic legitimate companies’ domain names.



RUTGERS
New Jersey Agricultural Experiment Station

Red Flags of a Phishing Scam

- E-mails that direct users to a Web site to “validate” or “verify” or “update” personal info
- E-mails warning that accounts will be closed
- Grammatical errors and typos
- References to current events in the news
- Words Like “Urgent” and “Important”