Lorain County Community College

Phishing & Spam: A Brief Discussion

What is phishing? It is defined as the activity of defrauding an online account holder of financial information by posing as a legitimate company. These scams are extremely dangerous and will lead to serious data breaches. There are too many scams out there to list, but, here are a few popular ones:

- *Nigerian Price Scam*: "The scammer will tell you an elaborate fake story about large amounts of money 'trapped' in central banks during civil wars or coups, often in countries currently in the news. Scammers may ask for your bank account details to 'help them transfer the money' and use this information to later steal your funds."[1]
- *IRS Data-Entry Scam*: "Spoofing our nation's tax collection agency is a tried and true tactic, and this phishing email from August played on the recipient's excitement to receive a tax refund by linking to a page for the recipient to specify payment information for refund, provided he/she enters login credentials."[2]
- *Ransomware Phishing*: "Back in May, we received a round of phishing that used fake MAILER-DAEMON email delivery failure notices to trick recipients into running an executable that installed a variant of Cryptolocker. A few weeks later, we received a fax-themed phish that led recipients to Cryptowall. Upon examining the bitcoin wallets of the attackers, we found they had collected over $130k in ransom payments."[2]

[1] https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams

[2] http://phishme.com/top-10-phishing-attacks-2014/

Spam- it's not just a processed meat enjoyed by soldiers during WWII.

Spam is often characterized by unsolicited electronic messages, emails, or even advertisements. It isn't limited to the online world; have you ever received a flyer in your mailbox and immediately ripped up because it was irrelevant to you (no, bills don't count)? While it isn't necessarily something "bad" or "malicious" up front, spam can be annoying to deal with. The real problem with spam is if you entertain the ads or emails. This could lead to even more spam emails and potential theft of personal information. The real problem behind spam emails/calls are the kind that phish for information, as discussed earlier.

In conclusion, the easiest way to avoid spam and phishing is ***common sense***. Even though you may still receive unwanted spam, it is up to you to ignore and delete it. Here is a rule of thumb for phishing- no legitimate business/company you are associated with will ask you to give them your personal information in an email.

- When it comes to links in emails, always try and type the URLs that they provide. Many spam/phishing emails use masked URLs that *look* like legitimate emails, but, redirect to more malicious site. If an email seems off from one you normally receive, be extremely cautious. Research the sender, the email, etc.
- Look for the SSL encryption "lock" icon in the address bar in a browser. This will help you to identify what is and isn't a secured website. Secured websites generally have a lower chance of data breaches or attacks than those that are not secured.
- Set up a dedicated spam email address that you can provide when entering contests, forms, etc. This email is the one that will have a majority of your spam sent to. After you set up a separate email like this, you can alleviate the amount of spam you receive to your primary email. This also reduces the risk of getting a phishing email to your primary email.

TwoForty7 Group
IT with Class