What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual.

The term “phishing” evolved in the mid-1990s by "Social Engineers" who would "fish" for account information from users on America On-Line.

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

By hijacking the **trusted brands** of well-known banks, online retailers, and credit card companies, phishers are able to convince **recipients** to **respond** to them.

Stop.Think.Connect.

Prevention Tools

- **Enable anti-phishing features in browsers.**

  Firefox – Phishing protection

  https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work

  Internet Explorer – SmartScreen

  http://windows.microsoft.com/en-US/windows7/SmartScreen-Filter-frequently-asked-questions-IE9#

- **Prevent security risk in mail clients.**

  Disable HTML email:

  •Outlook > Trust Center > Trust Center Settings > E-Mail > Read email as plain text

- **Web of Trust (a safe browsing tool)** www.mywot.com

- **Disconnect.me (Protect your online Privacy)**

  https://disconnect.me/

- **Consumer Awareness Program**

  http://stopthinkconnect.org/

- **APACS in the UK**

  http://www.banksafeonline.org.uk/

Phishing

Don’t Get Hooked!

How to recognize a phishing e-mail?

Most financial institutions or online services will not send a request asking that sensitive personal information be sent to them over the Internet. Such a request should be viewed with cautious skepticism. Many scam e-mails utilize some common techniques in order to harvest information from people:

- **"Your account has been (or will be) suspended."** Provides a sense of urgency for you to react quickly to avoid problems with your account, such that you might act in a more hasty manner.
- **"Dear Valued Customer . . . "** A non-personalized e-mail indicating that your account status is in danger is almost always a warning sign that an e-mail is not legitimate.
- **"Click on the following link . . ."** Be wary of links in an e-mail. It is easy to be deceptive in using HTML.
- **"Click on the attachment . . . "** Don't click on the attachment. It's probably a virus, a Trojan, or a key logger. A legitimate request will not have an attachment for you to execute. Don't open any attachment that you were not expecting - even if there is a very compelling case to do so. Many viruses use this technique to spread.
- **"Poor grammar or spelling"** Initial phishing e-mails were easy to spot, as they were full of spelling and grammatical errors. Nowadays, many look as good or better than actual e-mails from an on-line bank.

- **Pay attention to the URL of a website.** Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

What to do if you receive a Phishing e-mail?

DO NOT CLICK on any links (or attachment) in the e-mail – no matter how urgent the instructions may be. These links are designed to take you to a site where malware will attempt to install itself on your machine. If it is a notification from a legitimate business – you should be able to contact them via telephone or e-mail to confirm that the notification is legitimate.

Don't take the bait!

- **Many viruses pretend to be legitimate programs and security tools**. Clicking on links or attachments in unexpected e-mails is a common method of infection.
- Since **the exposure of passwords from social networking** services, scammers have been improving their techniques for trying to craft more and more believable e-mails. These are all intended to infect your computer with malicious programs designed to **commit identity theft** or **steal intellectual property.**

What should I do if I have been caught?

- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- CHANGE your passwords immediately.
- Watch for other signs of identity theft.
- Consider reporting the attack to your local authorities.