
Phishing Awareness…
Don’t Get Hooked!

What is Social Engineering?

- An act of using deceptive techniques to gain the trust of someone in order to get them to expose information they normally would not disclose.
- Social Engineering methods may include:
  - **phone call:** where they masquerade as someone who they are not
  - **e-mail:** that has malicious program attached or link to a web page. The attached file or web page would contain a virus, and executing it would lead to infection.

In a phishing attack…..

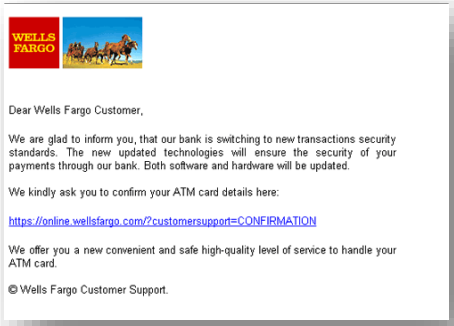
- ….the social engineer is trying to gain access to more than just an account or control of a computer system.
- The goal usually is to attain personal information in order to defraud people.

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.

How to recognize a phishing email?

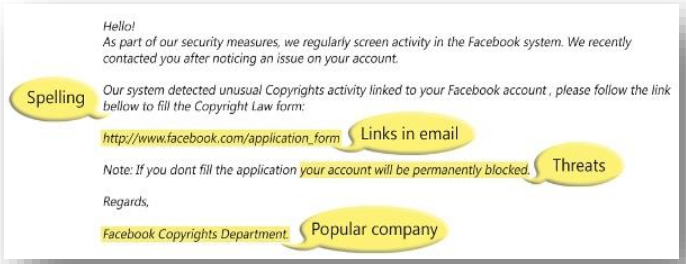
- Most financial institutions/online services will not send a request for sensitive personal information to be sent over the Internet. Such a request should be viewed with cautious skepticism.
- Many scam e-mails utilize some common techniques in order to harvest information from people:
  - **"Your account has been (or will be) suspended."** - sense of *urgency* for you to react
  - **"Dear Valued Customer…"** - A non-personalized e-mail that inform your account status is in danger.



How to recognize a phishing email?

- **"Click on the following link . . ."** Be wary of links in an HTML e-mail. It might be a fake link

- **"Click on the attachment . . . "** *Don't click or 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 or services.
- **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).

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**.

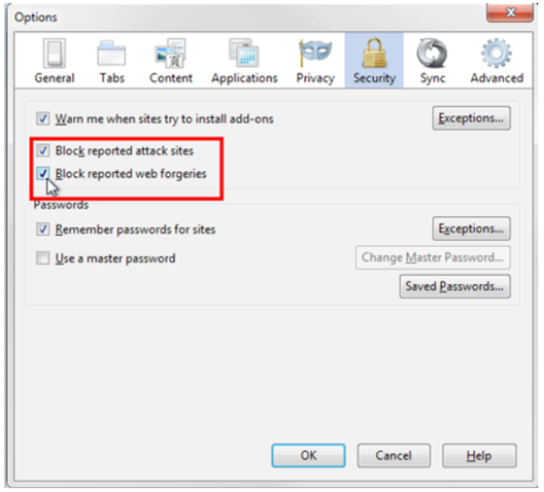
What to do if you receive a Phishing e-mail?

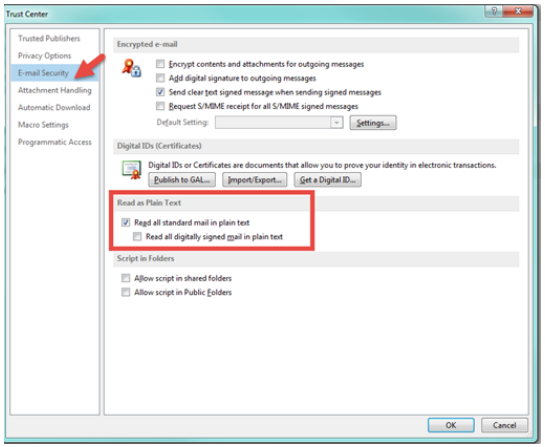
- **DO NOT CLICK on any links (or attachment(s)) in the e-mail** – no matter how urgent the instructions may be.
- These links are designed to take you to a site where malware will attempt to install itself on your machine.

- If it is a notification from a legitimate business – you should be able to contact the business via telephone or e-mail to confirm that the notification is legitimate.
- If it is from your banking institution, go directly to their website for up to date information.

What can you do to reduce your risks?

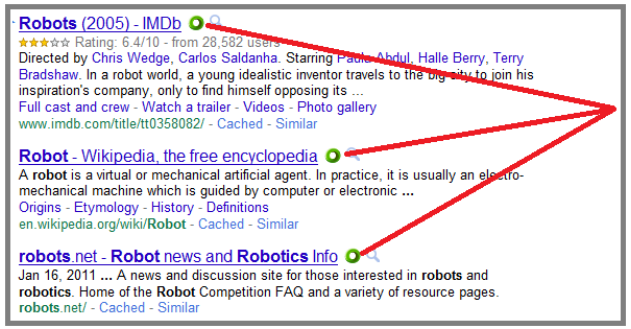
- Enable anti-phishing features in browsers:
  - **Firefox** – Phishing protection
    - https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work
  - **Internet Explorer** – SmartScreen
    - http://windows.microsoft.com/en-US/windows7/SmartScreen-Filter-frequently-asked-questions-IE9#
- Prevent security risk in mail clients, ie.:
  - Disable HTML email: **Outlook > Trust Center > Trust Center Settings > E-Mail > Read email as plain text**

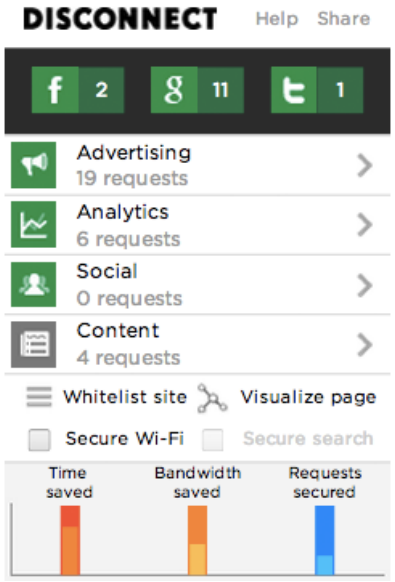




Other Tools you can use

- Safe Browsing Tool
  Web of Trust (www.mywot.com)
  - Allows you to see if a link is a known safe website or not
- Protect your online Privacy
  Disconnect.me (https://disconnect.me/)
  - Allows you to control your personal information that is analyzed by websites.





What to do if you think you've fallen victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

- 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.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft.
- Consider reporting the attack to your local authorities.

Additional information

- How to Avoid Phishing Scams
  - http://www.antiphishing.org/resources/overview/avoid-phishing-scams

- FBI's Common Fraud Schemes information page
  - http://www.fbi.gov/scams-safety/fraud

- STOP. THINK. CONNECT. - a consumer awareness program
  - http://stopthinkconnect.org/

- Bank Safe Online from our research partners APACS in the UK
  - http://www.banksafeonline.org.uk/

- Federal Trade Commission "Avoid ID Theft: Deter, Detect, Defend", a campaign to advise consumers on techniques to neutralize identity theft

- Site Jabber Blog, a consumer protection service which helps people avoid fraudulent websites and find ones they will love.

- Good collection of articles on "Identity Theft & Data Breaches" hosted by the Privacy Rights Clearinghouse.
- Wombat Security Technologies have developed this cute little game to help customers recognize phishing attacks. Play the first round of AntiPhishing Phil and see how knowledgeable you are.