What is Phishing?

Phishing is an Internet scam where fraudulent emails and websites are used to trick recipients into surrendering their personal or financial data for malicious purposes. Phishers often use well-trusted brand names of banks, online retailers, or credit card companies to fool recipients into believing that the email is genuine and from a legitimate source. These emails often ask recipients to visit a website where they are asked to update their personal information such as social security number, credit card number, address, bank account number, login name, password, etc.

The links in these emails are frequently labeled with the trusted websites link (for example, "https://www.ebay.com"), but the underlying link action points to an untrusted site (such as "http://xxx.xxx.xxx.xxx/untrustedAction.cgi"). The untrusted web site is a replica and is only set up to steal personal information.

Phishing Examples

Please keep in mind that these are real Phishing scams and these emails do exist!

Example 1: Your account at eBay has been suspended

An email which look like it's from eBay.com saying your eBay account has been suspended and you must follow the provided link to login and reactivate your account. The Phishers are trying to get you to click on the link and give them your eBay login name and password.

Example 2: Update your Paypal information

An email which look as if it's from Paypal asking you to update your personal information. It then ask you to follow the link on the email to login to your account. The Phishers then capture all information entered on that page such as Paypal username, password, address, phone number, as well as back and credit card information.

Example 3: Notification of US Bank Internet Banking

An email which look as if it's from US Bank saying, "as a prevention measure, we have temporarily limited access to some features." It then ask you to click on the link and login with your username and password. Again, the Phishers captured your username and password as well as your bank account information.

More examples can be found at http://www.antiphishing.org

Tips on Not Becoming a Victim

1. Be suspicious of any email asking for personal information.
2. Never use links provided in the email. Go to the website directly by typing the address in your browser's Address/Location field and login from there.
3. If you are not sure, call the company in which the suspected email came from.
4. Always ensure that you are using a secure website when providing personal information. Keep in mind that just having a lock
symbol in the browser status bar and "https:" in the address is not enough to determine whether you can trust a website. You should verify the certificate and ensure that you trust the company. Many scam sites purchase and use legitimate secure certificates.

Other Resources

- http://www.antiphishing.org/
- http://www.onguardonline.gov/
- http://www.ftc.gov/bcp/edu/microsites/spam/consumer.htm

Department of Chemistry
University of Washington
109 Bagley Hall
Box 351700
Seattle, WA 98195-1700

Main Office: 206.543.1610
chemdesk@uw.edu

Advising: 206.616.9880
advisers@chem.washington.edu

Source URL: https://chem.washington.edu/what-phishing