Phishing / Spoofing

What is Phishing or Spoofing?

"Phishing" or "Spoofing" emails are made to look like they are sent from reputable companies but are actually **sent by** cyber-**criminals**. These types of emails are sent to trick consumers into divulging sensitive information so that unlawful charges can be made on the consumers' accounts. **Responding to "phishing" or "spoofing" emails will put your accounts and personal information at risk**; they will link you to an imitation copy of a legitimate web page to trick you into providing sensitive personal information including passwords.

Identifying a Phish or Spoof Email

Phishing emails will usually urge you to "update" or "validate" your account information and will often threaten some dire consequence for not responding to them. Be on the lookout for poor grammar or typographical errors. Many phishing emails are translated from other languages or are sent without being proofread, and as a result may contain bad grammar or typographical errors.

What do I do if I get a Phishing Email?

If you get an email that asks for sensitive information, do not reply or click on the link in the message. When possible, you should avoid clicking links in the email. Instead of clicking the link, type the URL into the address area of your Internet browser. ***At no time should you cut and paste the link included in the message.***

Information courtesy of Juno.com

What Should I do if I Have Become a Victim of Phishing or Spoofing Fraud?

If you have responded to a scam message and given out your details, you should **report it immediately** to the legitimate company that you do business with. If you have given out any bank or credit card information, you should contact those companies as well. To learn more about what to do if you have given out your personal financial information, please visit:

Anti-Phishing Working Group: http://www.antiphishing.org/consumer_recs2.htm

-or-

Federal Trade Commission: http://www.consumer.gov/idtheft/index.html

The Federal Trade Commission has issued a warning about these Identity Theft scams. They suggest the following:

- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine;
- Avoid emailing personal and financial information;
- Always keep your password secure. Never share your password with anyone;
- Always review your credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your credit card or bank statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

For more information on how to avoid email scams, please visit the Federal Trade Commission's website at http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

Information courtesy of Juno.com