



Don't Get Hooked by Phishing

Identity theft is one of the fastest growing crimes in the United States. One of the sinister techniques that thieves use to steal your identity is called phishing.

Phishing is a practice that online fraudsters use to "fish" for confidential passwords and financial data from the "sea" of Internet users using email. Phishing has two major components:

- Spoofing occurs when thieves create a near exact replica of an existing website
- Spamming occurs when you receive unsolicited email also known as junk email. A typical email will tell you that you need to update your account information for a financial institution account. The email contains a link that when "clicked" will take you to the spoofed web site where you are asked for some personal and financial information. Once you enter in this information, the identity thief has access to it.

Phishing occurs when identity thieves use spoofing and spamming to lure you into providing personal and financial information on the Internet.

WHAT YOU CAN DO:

- Delete unknown email messages and don't download attachments or click on links included in the email
- Don't send personal or financial information via email
- Make sure that you are on a secure, encrypted website before entering personal or financial information. A secure site is usually designated by the URL beginning with "https" where the "s" stands for secure. Also, look for the closed padlock at the bottom of the screen, which indicates secure.
- Use anti-virus software on your PC or laptop and keep it updated
- Add a firewall to your computer especially if you use broadband service