



CyberAngels

A program of Guardian Angels
keeping it safe

Phishing

Don't Be Lured By "phishing"!

"Phishing" is the use of e-mails or pop-up boxes that contain links to sites that ask you to enter or confirm information, such as personal information, financial information, passwords, or other sensitive information. Here's an example:

Dolores receives an e-mail that appears to be from her bank asking her to click on the link provided to update her account information. She clicks on the link and a web site opens that looks just like her bank's web site. She enters her information into an online form, hits send, and believes she has taken the appropriate action. In fact, she has just handed her personal information to a scammer! The e-mail was a phishing e-mail.

The sites these scams link to often look like the legitimate business they pretend to be. But the sites are phony and the scam is used to lure you into providing information that can be used by criminals to steal your identity.

How do you recognize "phishing"? First and foremost, never click on links in e-mails or pop up boxes that ask you to verify or update personal information. Legitimate businesses do not ask for this information through e-mail links and pop-up boxes. Type the name of the link to businesses you deal with online yourself or add the links to your Favorites.

Additional Resources

CERT: [Avoiding Social Engineering and Phishing Attacks](#)

DOJ: [USA/Canada Report on Phishing](#)

DOJ: [Special Report on "Phishing"](#)

FTC: [Spam Page](#)

FTC: Report phishing e-mails to the FTC at spam@uce.gov

OnGuard: [Phishing](#)