

Illuminating PC Tips

Note: Illuminating PC Tips are posted on www.MyWFN.com by Joanne Osmond.

Rather than send a weekly PC Tip, it makes more sense to send tips when someone asks me a question or I come across something important. I will continue to look for easy to understand tips on how to take care of your PC in magazines and newspapers. The tip below comes from one of my favorites, *Fast Company* August 2004 page 32 “SOMETHING PHISH-Y” by Scott Kirsner!

“Phishing” is a new word in my vocabulary and isn’t in Word’s standard dictionary. It is scary that new words are invented to describe the dangers on the Internet. Phishing is any e-mail communication that looks legitimate, but its purpose is to defraud you of account information and the money in your account.

The e-mail reads something like this...”There is a problem with your account and we need you to verify your social security information. Please click on this link to confirm your Social Security Number.” The link will lead you to a cleverly disguised web site that will ask for information such as your bank account number, credit card information, or password. Any information you enter at the fake site will be captured by scammers who use it to steal your identity, drain your account, or both.

Over 57 million people in the United States received phishing attempts last year. So what should you do to protect yourself?

- Do not let your children use your credit cards on the Internet.
- If you think the request may be legitimate, retype the URL. What you think is a link to your bank because it looks right on the screen may be just a label. The actual link is to the phony site. To see where the link really goes, right click on the URL and Check Properties, Edit Hyperlink, or something similar.
- Check out the web site www.antiphishing.org to see the latest versions of the phishing epidemic.

Don’t fall for the scare tactics; you have a lot to lose.