Don’t Get Hooked by a Phishing Attack

If you have Internet access, you may be under attack--a phishing attack, that is. This high-tech scam involves three components:

Spoofing is creating a replica of an existing Web site.

Spamming is unsolicited, or “junk” e-mail.

Phishing is the act of using spoofing and spamming to lure unsuspecting victims, hoping to deceive you into disclosing your Social Security number, credit card and checking account numbers, passwords, or other sensitive information.

The Federal Trade Commission recommends the following tips to help you avoid getting hooked:

1. If you get a pop-up or e-mail message requesting personal or financial information, don’t reply or click on the link in the message. Legitimate companies won’t ask for this information.

2. Be cautious about opening attachments or downloading files from e-mail messages.

3. Never send personal information via e-mail. Look for a closed padlock at the bottom of your browser window, or a URL that begins with “https”--the “s” stands for secure. However, some phishers forge these security icons.

4. Review statements for accuracy as you receive them. If they’re late, call the company to confirm billing address and balance.

5. Use antivirus software and keep it up-to-date. Run a firewall, particularly if you have a broadband connection. Take advantage of free software “patches.”

6. Report suspicious activity to the FTC at www.ftc.gov, and forward suspicious messages to spam@uce.gov.