

Phishing...

is a scam where Internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims. To avoid getting hooked:

- Don't reply to email or pop-up messages that ask for personal or financial information, and don't click on links in the message. Don't cut and paste a link from the message into your Web browser — phishers can make links look like they go one place, but that actually send you to a different site.
- Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice over Internet Protocol technology, the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card, or type in the web address yourself.
- Use anti-virus and anti-spyware software and update them all regularly.
- Don't email personal or financial information.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.