



PHISHING ANYONE?

Phishing is a scam where internet crooks send spam or pop-up messages to steal personal and financial information from you.

- \$ Don't reply to email or pop-up messages asking for personal or financial information
- \$ Don't click on, or cut and paste a link from a message into your Web browser
 - Crooks make links look like they go one place, but send you to their site
- \$ Scammers send emails that seem to be from a business, then ask you to respond via email or call a phone number to update your account information
 - Voice Over Internet Protocol Technology changes the area code you call so it will not show where the scammers really are

AVOID GETTING HOOKED!

- \$ Use anti-virus and anti-spyware software, as well as a firewall, and keep them updated
- \$ NEVER email personal or financial information
- \$ Review credit card and bank account statements to check for unauthorized charges.
- \$ **Be cautious** about opening emails you receive, regardless of who sent them.

If you've been scammed, visit the Federal Trade Commission's Identity Theft website at

www.consumer.gov/idtheft.