SCDCA Spotlight

# E-Mail Scams: Phishing

SC Department of Consumer Affairs ♦ 800-922-1594 ♦ www.scconsumer.gov

# Don't Get Hooked by Phishing Scams

National banks and retailers recently informed millions of consumers about the possibility of their e-mail addresses being stolen. The notices come on the suspicion that fraudsters hacked into the computer system of an advertising agency used by these companies. While no personal identifying information was accessed, scam artists may use the stolen data to attempt to "phish" personal or financial information from unsuspecting consumers.

Phishing is a scam where an internet fraudster sends an e-mail that claims to be from a business you have a relationship with. The message asks you to "confirm," "update" or "verify" your personal information - for example your account number or social security number - or your online account username or password. A website link for you to visit or telephone number for you to call may also be included in the e-mail. Don't be fooled. Even though the website looks authentic or the phone number seems accurate, they are bogus! Websites can be easily spoofed and internet technology can disguise a telephone number so you do not know where the scammers really are.

Fraudsters also engage in "spear phishing." This is a spin on traditional phishing where scam artists have some inside information, such as the consumer's name or knowledge of who the consumer does business with, which they use to seem more legitimate in their request for personal data. Don't get hooked! If you receive an e-mail asking for your personal or financial information, follow these steps to protect yourself:

- **Do not reply to an e-mail or pop-up message that asks for personal or financial information.** Legitimate companies don't ask for this information via e-mail.
- **Do not click on any links in the message or cut and paste the link into your browser.** Phishers can make the link look like it's going to one place, when it really sends you to a different site. If you want to go to the company's website, open a new internet browser session and type in the correct web address yourself.
- **Do not call a phone number contained in the e-mail.** If you are concerned and want to call the company, call the number on your financial statement or on the back of your credit card.
- **Use antivirus or antispyware software and a firewall.** Make sure to update them regularly. Phishing e-mails may contain software that can harm your computer or track your activities on the Internet.
- **Track your finances.** Always review your banking statements as soon as you receive them. Also review your credit report regularly. You are entitled to a free credit report from each one of the three major credit reporting agencies annually. You can obtain your report by visiting www.annualcreditreport.com or calling 877-322-8228. Check your statements and credit report for unauthorized purchases/accounts and incorrect information.

SCDCA aims to protect consumers from inequities in the marketplace through advocacy, complaint mediation, enforcement and education. For information on how to minimize the risks of identity theft or to file a complaint, visit www.scconsumer.gov or call toll-free, 1-800-922-1594.