SPOTLIGHT: PHISHING SCAMS

DON'T GET HOOKED BY PHISHING SCAMS

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.

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.

- **Know what you're buying and what it will cost.** Read the seller's description of the product, including the fine print! Factor in shipping and handling into the total cost of your purchase.

- **Check out the terms and conditions.** Can you return the item for a refund if you're not satisfied? Who pays the shipping costs? Is there a restocking fee? Print and save records of your online transactions, including all emails to and from the seller.

- **Pay by credit or charge card.** They offer the best consumer protections. Under federal law, you have the right to dispute charges under certain circumstances and withhold payment temporarily while the creditor is investigating. And if your card is used without your authorization, your liability generally ends at the first $50.

- **Use antivirus or antispyware software and a firewall.** Make sure to update them regularly.

For more information on protecting yourself from identity theft, visit www.consumer.sc.gov and click Identity Theft Resources.

IDENTITY THEFT UNIT
education. guidance. enforcement.

South Carolina Department of Consumer Affairs
293 Greystone Blvd., Ste. 400 • PO Box 5757 • Columbia, SC 29250
(800) 922-1594 • www.consumer.sc.gov

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS