Don't Get Lured into a Phishing Scam

By Michael Guillot, Security Director

Con artists now use email to try to hijack your personal financial information. In a scam known as "phishing," swindlers claim to be from a reputable company and send out thousands of fake emails in hopes that consumers will respond with the bank account information, credit card numbers, passwords or other sensitive information.

These emails can look quite convincing, with company logos and banners copied from actual Web sites. Often, they will tell you that their security procedure has changed or that they need to update (or validate) your information, and then direct you to a look-alike Web site. If you respond, the thieves use your information to order goods and services or obtain credit.

Consumer Tips

To avoid becoming a victim of a phishing scam, the American Bankers Association offers these tips:

- Never give out your personal financial information in response to an *unsolicited* phone call, fax or email, no matter how official it may seem.
- Do not respond to email that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the email's validity using a telephone number or Web address you know to be genuine.
- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.
- When submitting financial information to a Web site, look for the padlock or key icon at the bottom of your browser, and make sure the Internet address begins with "https." This signals that your information is secure during transmission.
- If you have responded to an email, contact your bank immediately so they can protect your account and your identity.