Consumer Advisory Bulletin-October 2005

Warning: Internet "Phishing" Scams

Con-artists use phony e-mails and web sites to obtain victims' account numbers. Scams may be disguised as hurricane appeals.

Identity thieves are constantly trying to trick victims into giving them crucial information over the Internet, such as credit card numbers, bank account information and private passwords. It can even happen with phony hurricane appeals. It's called "phishing" (sounds like "fishing.") Crooks hook and trick victims into giving up sensitive information. Once they steal your information they can drain accounts or run up credit card charges.

The "bait" or lure usually is an official-looking e-mail message that appears to be from your bank, your Internet service provider, or some other major company -- or perhaps a hurricane-aid group like the Red Cross. The message asks you to click on a link to a web site in order to make a donation, or perhaps to "update" or "validate" or "verify" your account or Social Security Number. The message usually sounds persuasive and urgent ("Your donation is crucial," or, "Your account will be closed if you don't reply at once.")

The problem: clicking on the link sends you to a phony web site - a web site that looks remarkably like the real thing but is completely fabricated by the con-artists. Then the "spoof" web page asks you to enter and send your private data -- probably to overseas crooks. The "phishing" scam has been used imitating the Red Cross, banks, AOL, eBay, PayPal, CitiBank, Best Buy, UPS, and many others. Be careful, and don't get caught!

How to avoid being hooked by a "phishing" or "spoof e-mail" scam:

- **Don't reply to e-mails that ask for your personal information.** If there's any question, contact the company by phone at its regular number on your statement. Call or look up web sites yourself for bona fide hurricane-relief organizations.
- **Don't send personal information by e-mail - it's just not safe.** Use only secure web sites -- indicated by a padlock icon or "https" web address.
- **Always examine your account statements for unauthorized charges.** Report any suspicious activity to the business, and to the Iowa Attorney General's Office. Put a security alert on your credit bureau files. For more details and information on avoiding identity theft, visit the Attorney General's web site.

If you think you have been cheated by a "phishing" scam, contact the Attorney General's Consumer Protection Division, Hoover Building, Des Moines, Iowa 50319. Call 515-281-5926, or 1-888-777-4590 toll-free. The Web site is: www.IowaAttorneyGeneral.org

Return to Consumer Advisories