DenverDA
Mitchell R. Morrissey, District Attorney - Second Judicial District
201 W. Colfax Avenue, Dept. 801, Denver, CO 80202
Bus. Phone: 720-913-9000
Fax: 720-913-9035

Mitch Morrissey
Denver District Attorney

Consumer Fraud Alert

Phishing Scams are Becoming More Destructive

If it seems like you are receiving more threatening emails these days, you probably are. Such emails characterize a typical phishing scam, and these scams are escalating. According to Symantec, the Norton-Anti-Virus firm, phishing scams have grown to an estimated 8 million attempts a day. A *phishing scam* is a legitimate-looking email from a fake business or government agency that typically threatens to take some kind of undesirable action if the reader doesn't respond. Cyber thieves trick email users into disclosing personal and financial information by instructing them to click on an attachment or email link. But just as email users have become more adept at recognizing, and then deleting these emails, phishing scams are becoming more malevolent and not as easy to spot. Increasingly, by clicking on an embedded link, it may introduce malware - a computer virus that allows cyber thieves to gain remote access to a person's computer and the information that is stored on the hard drive. Phony websites with embedded phishing features are also commonplace. Some that have sprouted up recently include "charities" trying to profit off of natural disasters.

Today, it no longer takes a mastermind to hack into a computer. The underground purchase of "phishing kits" is flourishing and this accounts for the disturbing increase in the number and variety of phishing scams. Although personal email users are likely targets, businesses, particularly financial services are seeing the greatest increase in such cyber-attacks.

Phishing scams are becoming more sophisticated, but for the general PC user, prevention strategies have not changed. Never respond to any suspicious email regardless of how urgent, official, enticing, or threatening the message sounds. Never click on a link or open an attachment within that email. Just delete it. When in doubt, call the business or agency to verify the facts using a phone number obtained from a legitimate source. As a general rule, credible establishments do not send out unsolicited emails or ask for personal or financial information, passwords, pin numbers or other sensitive information. If you receive a phishing scam, file a complaint with the FBI at www.IC3.gov

Denver DA's Fraud Line: 720-913-9179

Follow us on Twitter @DenverScamAlert ***February, 2013***