J.E. CHOSTNER
District Attorney
(719)583-6030

OFFICE OF THE DISTRICT ATTORNEY
TENTH JUDICIAL DISTRICT, COLORADO

STACIE HARRIS
Paralegal II
(719)583-6675

Scam Alert – Phishing

by Stacie Harris, Economic Crimes Unit

What is a "Phishing "? This is a type of scam in which people use fake e-mails to steal your financial information online. There really is no complete safe defense against this scam, other than to recognize and be aware of the dangers in case you are targeted.

Everyday, thousands of people receive e-mails that look like they're from reputable companies like Citibank, Ebay, Amazon, or even your very own banking institution. These bogus emails will tell the recipient that their account information has been compromised, or needs to be updated, and will ask them to go online to "verify" the numbers to their credit cards, bank accounts, social security, passwords or PIN codes to keep it from being suspended or closed. The victim is prompted to click on a link in the email taking them to a website that is known as a "spoof page", which has been created to look exactly like the real website that it is mimicking. The minute the scammer obtains your personal information, they will either open up bank accounts or charge cards in your good name and change the address. It may be a few months before you discover these charges have even been made.

In past years, the Consumer Reports National Research Center has estimated that people have lost $630 million to these phishing scams. Kim Kleman of Consumer Reports states, "Our latest survey finds the median cost per victim is $850. That's five times what it was just a year ago".

Never Trust an E-Mail Sender. Did you know that over 95% of phishing attacks use a spoofed e-mail address? The sender of an e-mail can choose any name/supposed address that they want. The best rule of thumb is never even open an e-mail if you don't know who the sender is or you have never done business with this place. Some scams are easier to spot than others. A dead giveaway is bad spelling and grammar. If you do open a spoof e-mail, do not open any attachments connected to it. Although some may be harmless, this is the greatest way that viruses are spread. 90% of computer viruses are distributed by e-mail. These attachments may also try and infect your computer with programs that steal information without your knowledge.

There are three basic steps when it comes to computer security.

1. **Get an antivirus program**. An antivirus program will scan every file in case it is infected with a virus. If one is found, it can then remove it from your system. New viruses appear everyday, so be sure you keep this updated.

2. **Get a spyware removal program.** This type of program can pick up programs that the antivirus program can miss. There are some programs out there that are not known as a virus, but are just as harmful. Some can even record every keyboard press you make, thus capturing important information such as passwords and credit card details. Again, this is also a program that you need to be sure and keep updated.

3. **Update your operating system.** Did you know that Microsoft Windows is not flawless. There are security holes and other issues that are regularly discovered that a hacker could get inside your computer and steal information. Microsoft does fix every weakness they find. So be sure that you have all the latest updates at http://windowsupdate.microsoft.com .

If you do receive an email from what appears to be a company that you have been doing business with, please remember that the real company will never e-mail you asking you to give out personal information. Contact the company by means that you know are safe, for example, the phone number located on the back of your credit cards or your bank phone number that you obtain through your phone book. If you have even the slightest suspicion or apprehension about an email that you receive, then don't give out any of your personal information. Just delete the email. The sooner it's off your computer, the better.

If you think you might have become a victim to a phishing scam, don't panic. First, you do need to act quickly by contacting your real bank or company and tell them what has happened. They will assist you in resolving any problems associated with your account. You will also need to change your passwords or any details that you may have given out to the scammer. You can also report the matter to the FBI's Internet Fraud Complaint Center at www.fbi.gov as well as visit the Federal Trade Commission site at www.ftc.gov for assistance regarding identity theft.

IDENTIFY A SCAM
~ BEFORE A SCAM IDENTIFIES YOU! ~