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 – Forged Email Addresses

by Stacie Harris, Economic Crimes Unit

Have you ever received an email that says the sender is…YOU?

Technology has given scammers more avenues of operation to commit their frauds. For every scam that law enforcement agencies worldwide shut down, several more pop up to take its place.

Email addresses are being forged not only for phishing expeditions to obtain personal identifying, but also to send out junk mail and/or viruses at an alarming rate.

Although spammers like to target businesses, every day people such as ourselves are not completely safe from this. Once your computer has been infected with a virus, a spammer can then forge your email address to show as the "From" address for their outgoing emails. In doing so, they make you look like the culprit sending out junk emails (spam) or viruses. This tactic makes it more difficult, if not completely impossible, to trace who really sent the email.

When you receive a forged email from what appears to be a reputable business that you've heard of, this makes it easy to gain your trust. That email is either to attempt to sell you something in order to gain your personal information, or to infect your computer to propagate the viruses. Since you believe the email is from who it says it is, you may complete the transaction thinking you are doing business with a known company, when in fact you are not. Never click on the link in these type of emails to take you to the company website. More than likely, these type of links are bogus websites out to steal your personal information. Always do a search through a reputable search engine (Yahoo, Google, Dogpile, etc.,) to locate the web address for the company in which you are wishing to do business with.

For computer users not related to business use, if you receive an email from somebody that you don't know, DO NOT open it. I know that curiosity sometimes get the better of us, but most of these type of emails have programs written to them that once you open the email, it sends a reply to the sender validating your email address. Your email address will then be added to what they like to call a "sucker's list". This list is sold to other spammers for them to send you more junk email than you know what to do with.

If you're a business owner, not opening an email could well be a lost chance of a sale. In this type of situation, you must rely on your virus protector, your domain registrar and DNS service supplier to protect you and your business. Contact your domain registrar & DNS service suppliers to guide you on the safety for your business website. If you have or become a victim of a forged email address, your domain registrar and DNS service may recommend that you place an explanation on your webpage of what is happening so that those that have become victims understand you are a victim as well.

For all computer users, remember, if you utilize the internet, you put your computer and your personal information at risk every time you log onto the internet. Make sure to use a good virus protector that also is capable of removing spyware and adware. You must also remember that your virus protector is good as long as you keep it updated on a regular basis.

Report all computer internet crimes to www.ic3.gov.

~ IDENTIFY A SCAM BEFORE A SCAM IDENTIFIES YOU! ~