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 – Zombie Computers

by Stacie Harris, Economic Crimes Unit

No, The Walking Dead characters from the television show have not infected your computer, but someone is trying to.

If your computer is running slower than normal and is always trying to access the hard drive, your computer may just be a "zombie". According to Mark Huffman of ConsumerAffairs.com, if a hacker is able to download just a small malicious code onto your computer, your computer could be cranking out thousands of spam emails and sending them all over the world and you might not have a clue.

How exactly does a hacker access your computer? It may be just as innocent as you going to a webpage that has contagious codes written to it, or unwittingly opening a virus-infected email. There are also programs out there that bounce around the web in search of security holes in which to slip through.

According to Byron Acohido and Jon Swartz of USA Today, hackers used to "launch electronic attacks for fun and bragging rights" to create a big nuisance for companies and consumers. Hackers now create these malicious programs and sell the access to spammers, blackmailers and identity thieves for profit scheme fraud.

How does it work? What you might think is a legitimate e-mail from your bank, may just be a hacker attempting to obtain your personal information. You receive an email from what appears to be your bank, telling you that your bank account may have been compromised and verification is needed. The minute you access the bogus web link from the e-mail, it will take you to a website that has the look and feel of an authentic webpage. When you type in your user name and password, the hacker has captured that information and now has access to your account on the real website. You may have just become a victim of a slow phishing scam. This is where small amounts are taken out of your account to avoid detection. Hackers have also used this method to steal account numbers to make long-distance phone calls and sign up for pornographic websites.

If your computer has been taken over by a hacker/spammer and bogus e-mails are being distributed from your account, you could have serious problems with your Internet Service Provider (ISP). They will shut down your internet service and prevent you from sending any further e-mails at all until the virus in your computer has been treated. Although you have every right to be upset for the discontinuation of your service, the ISP has to look at the bigger picture – the network itself and the protection of that network.

So, how do you awaken the undead zombie in your computer? You first have to become a security expert to avoid these scams. Your best protection against fraud is "knowledge". Realize that a bank will not e-mail you and inform you that your account may have been compromised and ask for your login information. If you receive this kind of email, contact your bank by phone immediately (using the number from your phone book - not the e-mail) and report the e-mail to their security department. Chances are they will ask you to forward the actual e-mail to them so that they may investigate the matter further. If you do make a habit of doing your banking, or paying bills online, then make sure that you physically type in the web address and do not access it through the link that you received in an e-mail.

Although, not every antivirus software is foolproof, your computer should have one to help slow down the hackers/spammers progress. Keeping it updated is a major factor. Lots of malicious codes and viruses can make it past the software through e-mails. Hackers rely on tricking the victim into opening an infectious attachment.

Never open an e-mail unless you know who it is from. If you do not know who it is from, delete it.

IDENTIFY A SCAM BEFORE A SCAM IDENTIFIES YOU!