From: Schriever, James W
Subject: Computer Based Crime Prevention Tips
Date: Thursday, October 22, 2009 9:06:17 AM

Computer based crime prevention tips.

Master Patrol Officer James Schriever, CIO, Central Patrol Division, 816-759-6313, Cell 816-719-8350

Computer Based Scams: Phishing & Spoofing

In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to unsolicited E-mail - that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.

Hacking

Hacking is the illegal access by unknown and unauthorized party(s) to a computer system to destroy or disrupt the system or to use it to carry out illegal activities.

Hacking Prevention: Firewall Protection Software

Using a computer without a firewall is like going on vacation and leaving the front door to your home wide open. A firewall creates a protective barrier between your computer and the Internet, essentially making your connection invisible to Internet hackers. A firewall keeps others from seeing that important confidential information. This barrier helps prevent others from being able to intrude into your computer or home network and retrieve important information like credit card numbers or passwords.

Internet Extortion

Internet extortion involves hacking into and controlling various industry databases, promising to release control back to the company if funds are received, or the subjects are given web administrator jobs. Similarly, the subject will threaten to compromise information about consumers in the industry

database unless funds are
received.

Phishing and Spoofing

Phishing and spoofing are somewhat synonymous in that they refer to forged or faked electronic documents.

Phishing is a high-tech scam that uses spam or pop-up messages to deceive consumers into disclosing their
card numbers, bank account information, social security numbers, passwords, or other personal information.

Phishers send an email or pop-up message that claims to be from a business or organization that you deal with
– for example, your Internet service provider (ISP), bank, online payment service, or even a government
agency. The message usually says that you need to "update" or "validate" your personal information, such as
user names, passwords, credit cards, social security numbers, and bank accounts.

The email might threaten some dire consequence if you don't respond. The email often directs you to
visit a "spoofed" or fake website that looks just like a legitimate organization's site, but it isn't. What is the
purpose of the bogus site? To trick you into divulging your personal information so the operators can steal
your identity and run up bills or to commit crimes in your name.

How does phishing work?

A phishing scam sent by e-mail may start with con artists who send millions of e-mail messages that appear to
come from popular Web sites or sites that you trust, like your bank or credit card company. The e-mail
messages, pop-up windows, and the Web sites they link to appear official enough that they deceive many
people into believing that they are legitimate. Unsuspecting people too often respond to these requests for
their credit card numbers, passwords, account information, or other personal data.

Phishing Red Flags

Just as in the physical world, con artists will continue to develop new and more sophisticated ways to trick
you online. The following are just a few phrases to watch for if you think an e-mail message is a phishing

scam. Don’t forget to trust your instincts. If an e-mail message looks suspicious, that probably means that it is.

•• **“Verify your account.”** Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail. Be suspicious of a message that asks for personal information even if the request looks legitimate. If you receive an e-mail from Microsoft asking you to update your credit card information, do not respond to this phishing scam.

•• **“If you don’t respond within 48 hours, your account will be closed.”** Phishing e-mail may be polite and accommodating in tone, but these messages often convey a sense of urgency so that you’ll respond immediately without thinking. Phishing e-mail may threaten to close or suspend your account or may even say your response is required because your account may have been compromised.

•• **“Dear Valued Customer.”** Phishing e-mail messages are usually sent out in bulk and do not contain your first or last name. Although, it is possible that con artists have this information. Most legitimate companies (but not all) should address you by first and last name.

•• **“Click the link below to gain access to your account.”** HTML-formatted messages can contain links or forms that you can fill out just as you’d fill out a form on a Web site. The links that you are urged to click may contain all or part of a real company’s name and are usually “masked,” meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site. Notice in the following example that resting the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company’s Web address, which is a suspicious sign.

•• Another common technique that con artists use is a Uniform Resource Locator (URL) that at first glance appears to be the name of a well-known company but is slightly altered by

intentionally adding,
omitting, or transposing letters. For example, the URL “www.microsoft.com” could appear instead as:
www.mi**co**soft.com
www.mi**rc**osoft.com
www.verify-microsoft.com
Microsoft won several lawsuits against individuals who have used these types of URLs to pose as
legitimate Microsoft properties. However, the practice remains pervasive, so be aware of this
technique

- Scare tactics**.**
- No name**.** The mail doesn’t address you by name but with a generic greeting, such as “Dear
Suntrust.com Customer.”
- It offers forms to fill out with your personal financial information.
- It points to links in the e-mail**,** urging you to click to “validate” or “confirm” your account.

Phishing Prevention Tips:
The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

- If you get an email or pop-up message that asks for personal or financial information, do not reply. And
don’t click on the link in the message, either. Legitimate companies don’t ask for this information via
email. If you are concerned about your account, contact the organization mentioned in the email using a
telephone number you know to be genuine, or open a new Internet browser session and type in the
company’s correct Web address yourself. In any case, don’t cut and paste the link from the message
into your Internet browser — phishers can make links look like they go to one place, but that actually
send you to a different site.
- Use anti-virus software and a firewall, and keep them up to date. Some phishing emails contain
software that can harm your computer or track your activities on the Internet without your knowledge.
Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files.

Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software
that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that
updates automatically.
A firewall helps make you invisible on the Internet and blocks all communications from unauthorized
sources. It's especially important to run a firewall if you have a broadband connection. Operating
systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free
software "patches" to close holes in the system that hackers or phishers could exploit.

•• Don't email personal or financial information. Email is not a secure method of transmitting personal
information. If you initiate a transaction and want to provide your personal or financial information
through an organization's website, look for indicators that the site is secure, like a lock icon on the
browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure").
Unfortunately, no indicator is foolproof; some phishers have forged security icons.

•• Review credit card and bank account statements as soon as you receive them to check for
unauthorized charges. If your statement is late by more than a couple of days, call your credit card
company or bank to confirm your billing address and account balances.

•• Be cautious about opening any attachment or downloading any files from emails you receive, regardless
of who sent them. These files can contain viruses or other software that can weaken your computer's
security.

•• Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or
organization impersonated in the phishing email. Most organizations have information on their
websites about where to report problems.

•• If you believe you've been scammed, file your complaint at ftc.gov, and then visit the FTC's Identity
Theft website at www.consumer.gov/idtheft. Victims of phishing can become

victims of identity theft.
While you can't entirely control whether you will become a victim of identity theft, you can take some
steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new
accounts are likely to show up on your credit report. You may catch an incident early if you order a free
copy of your credit report periodically from any of the three major credit bureaus.

Spoofing

Every Internet user should know about spoof emails that appear to be from a well-known company but can
put you at risk.
In Spoofing scams, the spoofer creates a false or shadow copy of a real website or email in a way that
misleads the recipient. All network traffic between the victim's browser and the shadow page are sent
through the spoofer's machine. It allows the spoofer to acquire personal information, such as passwords,
credit card numbers, and account numbers.
Even though the email looks like the real thing, complete with authentic logos and working Web links,
it's a fake. The website where you're told to enter your account information is also fake. In some instances,
really slick phishers and spoofers direct you to the genuine website and then a pop up a window over the site
that captures your personal information. The information entered does not go to the legitimate site, but rather
to the spoofer's account. The information you entered will most likely be sold to criminals, who'll use it to ruin
your credit and drain your account.
Although they can be difficult to spot, they generally ask you to click a link back to a spoof web site
and provide, update or confirm sensitive personal information. To bait you, they may allude to an urgent or
threatening condition concerning your account.

What Spoof E-Mails are After

- Password
- Personal identification number (PIN)
- Credit card validation (CCV) code

•• ATM/debit card or credit card account number
•• Social security number
•• Bank account number

Even if you don't provide what they ask for, simply clicking the link could subject you to background installations of key logging software or viruses.

Spoof Prevention Tips

•• Make sure your computer has the most current anti-virus software and has a personal firewall. Antivirus software should be frequently updated to guard against new viruses. Make certain you download updates as soon as you're notified that they are available. A personal firewall can help prevent unauthorized access to your home computer.

•• Don't click on links in unsolicited e-mails, especially those asking for personal information. Even if you don't supply it, just clicking can enable thieves to access your computer, record your keystrokes, and capture passwords you use to log on at various websites.

•• Setup a login cookie. Many websites offer to "remember" your User ID. This way, when you return to the site to sign on, your User ID will be visible in the Sign on box. A spoof website will not be able to display your User ID. Note: never set up a login cookie on a public or shared computer.

•• Create hard-to-use passwords. Use at least six characters and a mix of letters and numbers. Don't use all or part of your online user ID or email address, or the names of your children, spouse, or pet.
And use different password for each of your online accounts.

•• Change your PIN and password frequently. Every 30 to 60 days is recommended.

•• Keep track of your account. Report suspicious transactions or irregularities immediately.

Pharming

In the newest form of phishing, called "pharming," a virus or malicious program secretly planted in a consumer's computer hijacks the computer's Web browser. When a consumer

unknowingly types in the
address of a legitimate Web site, they're taken to a fake version of the site without realizing it. Any personal
information provided at the phony site, such as passwords or account numbers, can be stolen and fraudulently
used.

Prevention Tips:

•• Never respond to an unsolicited e-mail that asks for personal financial information.

•• Report anything suspicious to the proper authorities. Alert the credit union or government agency
identified in the suspect e-mail through a Web address or telephone number that you know is
legitimate.

•• Contact the Internet Crime Complaint Center at www.ifccfbi.gov —a partnership between the FBI
and the National White Collar Crime Center—if you think you have received a phishing e-mail or
have been directed to a phishy-looking website.

The Department of Justice advises e-mail users to "stop, look and call" if they receive a suspicious e-mail:

•• **Stop.** Resist the urge to immediately respond to a suspicious e-mail—and to provide the information
requested—despite urgent or exaggerated claims.

•• **Look.** Read the text of the e-mail several times and ask yourself why the information requested
would really be needed.

•• **Call.** Telephone the organization identified, using a number that you know to be legitimate.

If you believe that you have provided sensitive financial information about yourself through a phishing scam,
you should:

•• Immediately contact those organizations for which you provided the information.

•• Contact the three major credit bureaus and request that a fraud alert be placed on your

•• File a complaint with the Federal Trade Commission at www.ftc.gov or 1-877-382-4357.

Spam

Spam is a term for the sending of unsolicited bulk email. Unsolicited means the recipient has not granted verifiable permission for the message to be sent. Bulk means the message is sent as part of a larger collection of messages, all having substantively identical content. With improved technology and world-wide Internet access, spam is now a widely used medium for committing traditional white collar crimes including financial institution fraud, credit card fraud, and identity theft, among others.

Those sending spam are violating the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act, Title 18, U.S.C., Section 1037. Violators are also accessing computers and servers without authorization, transmitting viruses, and deploying malicious codes which compromises the computer.

Spam email traffic is estimated to account for approximately 80 percent of all email traffic. The distribution of spam is facilitated through the use of open and misconfigured proxies. Subjects often provide hosting services, sell open proxy information, credit card information, and email lists illegally.

Spam Prevention Tips

•• Use a unique e-mail address - Pick an address that is hard for spammers to guess and easy for you to remember. Also, if chatting online, use a unique screen name that is not associated with your e-mail address.

•• Use multiple e-mail addresses - Consider creating separate addresses or accounts that can be used for online purchases, chat rooms and other public postings. You can also use a free forwarding address.

•• "Mask" your e-mail address - If you post your e-mail address online consider masking your address. There are several ways to correctly mask your address and thwart spammers.

•• Check the privacy policy when you submit your address to a Web site - Always be familiar with a Web site's privacy policy before submitting any information.

•• If it sounds too good to be true, - it probably is. Fraudsters, scammers, and crooks take advantage of
people via unwanted e-mail.

•• Learn more about “pop up spam” - recently a new form of spam has developed via the Microsoft
Windows operating system feature Messenger Service. It is a stream of “pop up” messages that stop
you from using your home computer until you close them.

•• Use tools to help prevent spam - Learn about tools that can filter or tag spam before it fills your
e-mail inbox.

Spyware

Spyware is software that collects personal information from your computer without your knowledge. It can
look at which sites you’re visiting or access information like usernames and passwords. What’s worse, it can look at which sites you’re visiting or access information like usernames and passwords. What’s worse, it can
send this information to a third party without you knowing it. The software may also perform several different
unwanted functions, including the delivery of pop-up ads or harvesting private information. It can serve up
inappropriate ads to you and your children, and can seriously slow your computer down, as it attempts to run
spyware processes instead of the programs you are trying to use.

Spyware is downloaded to your computer from the websites you visit, or invites itself in unannounced
when you agree to download another program. In some cases it is mentioned in the fine text of a user
agreement that you accept before downloading a program and when you agree to download the program, you
inadvertently agree to host spyware.

The clues that spyware is on a computer include:

•• a barrage of pop-up ads.

•• a hijacked browser — that is, a browser that takes you to sites other than those you type into the
address box .

•• a sudden or repeated change in your computer’s Internet home page.

•• new and unexpected toolbars.

•• new and unexpected icons on the system tray at the bottom of your computer

screen.

•• keys that don't work (for example, the "Tab" key that might not work when you try to move to the
next field in a Web form).

•• random error messages.

•• sluggish or downright slow performance when opening programs or saving files.

Virus & Worms

A virus is a program that can cause minor to extreme damage to your computer and use your Internet
connection to spread itself to other computers-usually those of your friends and family. A worm is similar to a
virus; however, a worm is self-contained and does not need to be part of another program to circulate itself.

Trojan Horse

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently
harmless programming or data in such a way that it can get control and do its chosen form of damage, such
as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program
that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part
of a computer virus.

The term comes from Greek mythology about the Trojan War, as told in the *Aeneid* by Virgil and
mentioned in the *Odyssey* by Homer. According to legend, the Greeks presented the citizens of Troy with a
large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged
from the wooden horse and overran the city.

Security professionals are warning of a new type of Trojan horse designed to steal user names and
passwords from Web surfers. The malware, dubbed "rootkit.hearse," uses rootkit cloaking techniques that
make it extremely difficult to detect.

Before it can steal information, however, the software must be downloaded onto a user's system. A
bad guy can accomplish this by tricking the user into downloading the malicious code or by infecting a

computer with some other form of malware. Once installed, it sends the sensitive information to the
fraudulent server.