CONSUMER AFFAIRS TABLOID

Keeping you in the "KNOW"

287-2489 Army Community Service Financial Readiness Branch Jul – Sep 13

Excerpt from: Federal Communications Commission
www.fcc.gov/guides/caller-id-and-spoofing

Caller ID and Spoofing

Caller Identification, or "Caller ID," allows you to identify a caller before you answer your telephone.

Caller ID service, however, is susceptible to fraud. Using a practice known as "caller ID spoofing," callers can deliberately falsify the telephone number and/or name relayed as the Caller ID information to disguise the identity of the calling party. For example, identity thieves who want to collect sensitive information such as your bank account or other financial account numbers, your social security number, your date of birth or your mother's maiden name, sometimes use caller ID spoofing to make it appear as though they are calling from your bank, credit card company, or even a government agency

Don't give out personal information in response to an incoming call. Instead, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to find out if the entity that supposedly called you actually needs the requested information from you.

Excerpt from: Federal Bureau of Investigation

Internet Social Networking

Internet-based social networking sites have created a revolution in social connectivity. However, con artists, criminals, and other dishonest actors are exploiting this capability for nefarious purposes.

Click-jacking - Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social networking sites. Disable scripting and iframes in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

Click on the following link to read the complete article: www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

ASK BUCKSAVER

Dear Bucksaver:

HELP! There is a message on my computer from the FBI stating I violated a law by accessing an illegal site. My computer is frozen and now I must pay a fine. Signed: Should I pay?

Dear Pay

The FBI would not ask you to pay a fine by clicking on a link. This is a virus known as Reveton/Citadel ransomware, which is designed to extort money from its victims. Even if you pay your computer will not be unlocked. You need to contact a computer professional to remove the malware

Have a question for Bucksaver? Send an email to the e-mail address listed below with Dear Bucksaver in the subject line.

Excerpt from: Fort Hood National Bank
www.fhnb.com/en/fraud/pharming.php

Pharming is a technique thieves use to obtain your personal financial information without your knowledge.

Here's how ***pharming*** works: A thief would first infect your computer with a virus either by sending you an e-mail or by installing software on your computer when you visit his/her Web site. The installation typically occurs without your knowledge; however, it could also be installed as part of something you choose to install from a Web site. Once your computer is infected, the virus would send you to a fake site that looks almost identical to your chosen Web site. Then the pharmers "harvest" your user name, password and other personal information without you even realizing it.

To help minimize the risk posed to you through pharming, here's what you should do:

- Run up-to-date antivirus protection and anti-spyware regularly on your computer.
- Install personal firewalls.
- Do NOT enter information onto pages without a lock or key icon at the bottom of the browser. This icon only appears when you go to a Web site that uses security certificates.
- Look for anything unusual in the Web site's address or URL.
- Browse the Web site for incomplete links, as identity thieves might not have correctly created all the different links and layers.
- If the Web site looks irregular or requests different login information than before, this might be a red flag that you are experiencing a "pharming" attack. If you feel uncertain about a site, telephone the company for verification.

Federal Deposit Insurance Corporation (FDIC)
Don't Be an On-line Victim: How to Guard Against Internet Thieves and Electronic Scams www.fdic.gov/consumers/consumer/guard

From the Files of Fort Hood's Consumer Affairs Office

287-CITY

Spoofing: It happened to me!

A couple of weeks ago I received a phone call from my wireless provider stating the network was scheduled to go down for eight hours and that I needed to write down a validation code to be reimbursed for the time lost. I asked why he was calling from Canada as that is what my caller ID stated. He said he was from the call center and not calling from Canada. He then asked me to state my name and say yes so he could record it. I immediately ended the phone call.

He called back but this time he spoofed my wireless provider's call center phone number. I told him not to call back. I suspect when he called the first time he forgot to spoof. Next, I called my wireless provider who verified they did not call and then I called the Federal Trade Commission to file an official complaint.

Back issues of the Consumer Affairs Tabloid are available on the Financial Readiness Branch section of the Army Community Service website at www.hoodmwr.com/acs. Have questions? Contact: melody.a.squires.civ@mail.mil or call (254)553-4702.

Army Community Service
Financial Readiness Branch

"Fort Hood Soldiers & Families Are Financially Fit"

Bldg 121
761st Tank Battalion Ave
Fort Hood, TX 76544
Phone: (254) 287-8979

Hours of Operation:
Monday through Friday
7:30 a.m. to 4:30 p.m.
Except Federal Holidays

Bldg 12020, Suite 400
31st and Battalion
Fort Hood, TX 76544
Phone: (254) 553-4698

Hours of Operation:
Monday through Friday
08:00 a.m. to 5:00 p.m.
Except Federal Holidays

E-Mail:
usarmy.hood.imcom-fmwrc.list.acs-frb@mail.mil

For more information
Call 254-287-6483

Website:

www.hoodmwr.com/acs/frb.html

Access your free credit report:
www.annualcreditreport.com
1-877-322-8228