Variations on an Identity Theft Theme

Technology brings us all kinds of convenience and entertainment. It also creates new ways for crooks to take advantage of consumers. The scams and the lingo change all the time. Here's an abbreviated technology fraud dictionary to keep you in the know.*

Pharming
This secretly plants a virus or malicious program in your computer and hijacks your web browser. Pharming crimeware misdirects users to fraudulent sites or proxy servers. When you type in the address of a legitimate Web site, you're sent to a fake site without knowing it. If you give your password or account information on the fake site, thieves will use your account fraudulently.

Pharming can occur *four* ways:
* Static domain name spoofing (misspellings: *vvestcu.org* vs. *westcu.org*)
* Malicious software, or malware (viruses and Trojans redirect you to the false site)
* Domain hijacking (hacker hijacks legitimate site and redirects all traffic)
* DNS poisoning—most dangerous (you enter correct URL, but poisoned server redirects)

Phishing
In this scam attempt, you receive an e-mail prompting you to reveal personal details—say, your Social Security number, passwords, or credit card information—by clicking on a link to a bogus Web page mimicking that of a legitimate company. These e-mails and linked sites used to have an amateurish look that was easy to spot; now, they often are indistinguishable from the real thing.

A clear tip-off that it's a fake—typically the greeting will be generic and not addressed to you by name. Another characteristic is a sense of urgency or alarm, say, that your account is about to be closed. Delete the message and report it to the credit union or other financial institution immediately.

Pretexting
This isn't new, but another scam aided by technology. Sometimes referred to as "social engineering," it occurs when someone tries to get personal private information without authority to do so. The scammer may ask for private information while impersonating an accountholder by phone, mail, e-mail, or even by phishing—using a phony Web site or e-mail to collect data.

SMiShing
This is phishing via SMS (short message service) and it’s targeted at mobile phone users who use text messaging. One of the first known SMiShing attacks looked like this: “We’re confirming you’ve signed up for our dating service. You will be charged $2 a day unless you cancel your order.” The message included a Web link that routes you to the main phishing page, where you’re prompted to download a program—a Trojan horse that turns your computer into a zombie controlled by hackers and used within a larger network to steal personal account information and perform other malicious activities. Be cautious about deregistering from a service when you’re sure you didn’t make a formal arrangement with the sender.

Social Network Phishing

Social networks such as Facebook, MySpace, LinkedIn, and Twitter are becoming the newest medium for phishing attacks. Crooks fool people into clicking fake links or opening dangerous files because they believe it came from a friend.

You receive a message, wall post, or “Tweet” from someone in your social network directing you to a site with “a funny video about you,” or something similar. The link brings you to a fake site—that appears legitimate—designed to steal login information or infect your computer with a virus. These attacks spread rapidly due to the viral nature of social networks.

Spamming

This involves using electronic messaging systems to send unsolicited, undesired bulk messages, often through e-mail. If you respond to the e-mail, the spammer then knows the e-mail address is valid and may target you for scams.

Spimming

Spim is spam—unsolicited bulk e-mail—delivered by IM, instant messaging. Not yet as common as spam, it reaches more people all the time. IM can be especially useful for spammers and dangerous for recipients because they may be more likely to click on links, bypassing virus software available on computers. Block messages from anyone not on your buddy list as a defense.

Spoofing

A spoof is an attempt to fool. Web spoofing is the act of secretly tricking your Web browser into talking to a different Web server than you intend. E-mail spoofing involves forging an e-mail header to make it appear as if it came from somewhere or someone other than the real source. Either can seduce you into supplying information to an unintended recipient.

If you hold your mouse over a link, the status line displays the corresponding URL. Be suspicious if the status line URL is different from what you think you should see. If Web pages you're familiar with suddenly prompt you to fill in private information, think carefully before you comply. If possible, call or send mail to the official source to verify that this change is legitimate. As always, when in doubt, do not enter any information you feel uncomfortable providing.

Vishing

Vishing uses Voice over Internet Protocol (VoIP) phones instead of a misdirected Web link to steal your personal information. Instead of an e-mail blast, the thieves use a "war dial" attack over a VoIP system to blanket an area. A recorded message tells you, for example, that your credit card has been breached and tells you to call a number immediately. The number connects to a VoIP phone that can recognize telephone keystrokes. When you dial, another message states "this is account verification; please enter your 16-digit account number." The same rules apply—don’t bite, and notify the "vished" entity right away. Even caller ID can be spoofed, so don't think you're secure if you believe the number looks legitimate. A similar telephone message can arrive by e-mail—again, don't bite.

CUNA
Credit Union
National Association

** Adapted from Credit Union Copy & Art Express*