DON'T LET ANYONE TAKE YOU PHISHING

FEBRUARY 2004 EJEMS

BY WILLIAM E. OTT

Internet scammers, hackers, identity thieves, and other online deviants have developed sophisticated and dangerous new schemes to get unsuspecting people to reveal their confidential personal and financial information. This new ploy is known as "phishing" and it isn't the type that you want to be involved with.

Phishing, also called "carding," or "spoofing" is a high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, ATM and debit card PIN numbers, home address, date of birth, and other sensitive information.

Typically you receive an e-mail from what appears to be a legitimate company such as eBay, PayPal, EarthLink, CitiBank, AOL, American Express, Amazon.Com, or many others that you might really do business with. The e-mail tells recipients that they need to "update" or "validate" their billing information or security information to keep their accounts active, and via a clickable link directs them to a "look-alike" web site of the legitimate business, further tricking the user into thinking they are responding to a bona fide request. Unknowingly, the user submits their financial information - not to the businesses - but the scammers, who use it to order goods and services and obtain credit and effectively steal the user's financial identity.

To avoid getting caught by one of these scams, the Federal Trade Commission (FTC), the nation's consumer protection agency, offers the following guidance:

- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine.
- Avoid emailing personal and financial information. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any 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.
- Report suspicious activity to the FTC. Send the actual spam to uce@ftc.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft.
- Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam. The Federal Trade Commission works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Phishing alone is bad enough, but recently even more insidious activities are being attached to the scam e-mails. The identity scammers are teaming up with virus writers, hackers, and spammers to place malicious attachments or cookies on users PCs. These cookies allow the hackers to determine PCs that are not secure and are capable of being controlled remotely. Once compromised PCs are found the hackers and spammers can then use them unknowingly to the use to become “spam bots” or “zombies.” These are PCs that are used to send out spam and to attack other computers or websites in a coordinated attack known as a denial of service attack (DOS) or distributed denial of service attack (DDOS). In the hacker and spammer world there appears to be a sub economy taking place where the identity thieves also receive a small payment from the hackers for every PC they turn over to the hacker that can be compromised.

The unsuspecting user may not know anything is wrong until their ISP turns off their connection because of spamming or zombie attack complaints from other people that reportedly originated from your PC or you get a visit from some nice people in dark suits and unmarked Crown Victorias carrying FBI credentials and search warrants.

If you receive one of these phisher e-mails, and the chances are if you haven’t yet, it is only a matter of time until you do, don’t click the link obviously. Companies do not use this approach for financial and security issues. If there is any question about your account status if you receive an e-mail seeming to be from a company you do business with, go to their site and log in using your own bookmarks or by typing the address into your browser directly. Again, do not click the link in the e-mail. The best thing to do is not open the message and simply delete it.

Protecting yourself from these types of scams and attacks is becoming more and more of a challenge but you can greatly minimize the risks by keeping your

operating system, e-mail client, and browser current with all patches, using a personal firewall software package like ZoneAlarm or BlackICE on your PC, and also using a hardware firewall appliance on DSL or cable Internet connections. When reviewing your e-mail stay alert. Remember you are still more likely to get a virus or worm from a 'trusted' friend or colleague that has become infected and unknowingly is sending out infected e-mail to replicate the infection to others. If you receive an unsolicited or unexpected attachment from a friend or colleague, call or e-mail separately to confirm what it is before opening it.

This type of clever attack to allow identity theft or to compromise PCs and networks is going to continue and will become more and more sophisticated. Some of these operations are teenagers, but more and more it is either organized criminal groups in the US or it is run by offshore criminal groups. They hope to get your information and then immediately either spend your credit card to the limit or obtain loans in your name. The websites that the phishing e-mails lead to are frequently only up for a matter of a few hours and then they disappear.

If you are responsible for your agencies computers and network all of this is of concern to you. Many times the fraudulent websites are actually hosted on unsuspecting business and government servers that are improperly secured. The phishers and hackers will create a small website on the unsecured system, capture user data there in a table allowing it to run for just a few hours, then they get their data and turn off the site and move on to another location. It is very much a high tech cat and mouse game. Stay vigilant, keep those PCs and network as secure as you can and stay aware of the emerging threats.

I welcome your comments, criticisms, feedback, and ideas. You may contact me at ejems@cpcstech.com

William Ott is president and chief consultant of CPCS Technologies, a NC-based technology consultancy providing services to the public safety and defense communities. He's been involved in EMS since 1981, in field, education and administrative capacities

William E. Ott

Digitally signed by William E. Ott
DN: CN = William E. Ott, C = US, O = CPCS Technologies, OU = Management
Reason: I am the author of this document
Location: Cary, North Carolina
Date: 2004.02.19 12:54:23 -05'00'