

Phishing Awareness Keeps You Off the Hook

June 2006



The vast Internet ocean is filled with useful resources and exciting possibilities. There are always things that catch your attention. Some of them warn you of threats to your security. Some open the door to riches. Almost always when you let your guard down and take the bait you will find yourself cooked and cleaned – just another victim of phishing. This is a very real threat not only to soldiers as individuals, but also to the operational security of the Army.

Phishing is usually an unsolicited email that prompts an action such as divulging secure information, downloading potentially dangerous files, or sending money to an unknown source. One of the original, and now classic, phishing scams was that of the Nigerian banker or businessman that wanted you to send money with the promise of reaping great returns on your investment. The number of people that responded to this scam was astounding and a new cyber criminal activity took off.

Like real anglers, Phishers try a wide variety of bait and lures to get their victims to bite. They prey on greed, fear, and especially for military targets, obedience to authority. The Nigerian email proves that greed will always catch a few gullible victims who are looking for easy cash. But as the cyber community has become more aware of potential dangers, phishing techniques have become more sophisticated.

Fear bait usually deals with credit card, bank or other money transfer systems like PayPal® or Ebay®. You will receive an unsolicited email saying that your account has been or is about to be suspended and you need to update your security and credit card or bank information in order to prevent this action. The email directs you to a web site where if you entered the information, would immediately send it to the Phishers. You might get a message saying your account was now activated or that might be the last you hear of it until you realize your account has been compromised.

When this scheme first started it was often easy to recognize a bogus email. The wording and spelling would be off, it would be a broadcast email, or the site they directed you to would barely look like the official one. These are still valid clues that will help you avoid such schemes. However, Phishers are becoming increasingly creative and focused. They now take the time to create more official looking and sounding emails and design sites for gathering data that look almost exactly like the real site.

The use of phishing techniques has reached a point that it is more than simply attempts to rip off Internet users. Very disciplined attacks by well-organized, "Phishers" are being directed at U.S. military installations and defense facilities. Official looking emails appear to come from a senior officer or other authority figure not known to the recipient, instructing the recipient to download and install software. This is often portrayed as a critical security measure that must be immediately deployed. What is actually happening is that the software is either a Trojan Horse that will destroy systems and networks or data mining software that will now be past firewall defenses.

The bottom line is that anyone that gets caught by these phishing scams will lose. They will lose money, resources or security. Awareness, caution and common sense are the best defenses. This type of cyber attack requires the cooperation of its victims. There are ways to guard effectively against phishing. Be wary of any unsolicited email that requests secure information or instructs you to download software. It is extremely rare that any financial institution including PayPal and Ebay will ask for such information. Check official websites for information on how to recognize fraudulent emails and sites. This includes military websites. Always get confirmation from a trusted source before downloading and installing software. Above all, be wary. If something doesn't seem quite right it probably isn't.

When a soldier falls victim to a phishing scheme it may result in more than just a compromised credit or bank account. Information could be given out that could put family, friends and fellow soldiers at risk. Downloaded software can jeopardize missions and lives. Don't end up on the hook. A little common sense and caution will keep you from being a Phisher's catch of the day.