Title:
Phishing with a Net

Word Count:
1258

Summary:
Being hacked or being cracked makes little difference to those on the receiving end. Understandably, their first impulses are to get mad and want to vent. The Cyberiter's contention is that, most of the time, they're lashing out in the wrong direction. After all, crooks are crooks; that's their job. Prevention is your job, so know the fundamentals of diligence.

Keywords:
phishing, hacking, cracking, internet scams, internet fraud, spyware, computer security, Cyberiter

Article Body:
When geeks gave us the Internet and the means to use it, they also gave us a new segment of vocabulary ...

I've often thought it a shame that a few of them didn't make their way to a campus literature or marketing department and see if a student of poetry or sizzle could assist them in assigning names to their innovations. For example, did the manual cursor operator have to be called a 'mouse?'

Geeks have overtaken sports-speakers when it comes to coining bad phrases. I've never understood why basketball types say a player 'kicks out' a ball to a teammate on the perimeter when his feet never touch it. Worse yet, I've always wondered if a gridiron football player would really want to dive on the ball if the carrier truly 'coughed it up!' That bit of literal imagery is more revulsive than handling a mouse. Do these guys really think about what they're saying?

There is one instance, though, where the geeks thought it through and got it right. 'Phishing' is a perfect connotation for cyber-cons who troll for prey.

The word's spelling distinguishes this nefarious activity from a sporting endeavor, but it's still a game. The definition that's been developed for it is "a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging

personal data such as account numbers and passwords, credit card numbers and Social Security numbers."

Another term that alludes to the emotive consequences of cyberobbery is the perjorative sense of 'hacker.' That bit of etymology seems to be a work in progress. The accepted definition refers to "individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data." However, the added qualifier is, "Hackers, themselves, maintain that the proper term for such individuals is cracker."

Being hacked or being cracked makes little difference to those on the receiving end. They just know they've been had. Understandably, their first impulses are to get mad and want to vent. My contention is that, most of the time, they're lashing out in the wrong direction. After all, crooks are crooks; that's their job and they're out there in numbers. That's not going to change anytime soon.

These victims need to take a hard look at themselves.

The economics of law enforcement --- in cyberspace or elsewhere --- limits what can be investigated and prosecuted. Thus, smart spoofers often keep their 'take' per scam campaign at levels sufficiently low that the cost of prosecuting them is not viable. Then, they change their coordinates, plus their identities, and do it again.

So, obviously, the most important factor in cyber-diligence is self-precaution. Most steps are basic, as evidenced by the checklist on the USA government's Federal Trade Commission website:

"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."

If you use e-currency or e-payment services, be aware that they are usually not

liable for any of your losses if you've been hacked or cracked due to identity-theft issues. All reputable services have support divisions that investigate any complaints of spoofing --- for example, Paypal asks you to mail them at spoof@paypal.com if you receive a suspicious message using their name --- and if anyone is going to pursue, or at least keep on file, complaints of any amount, it will be them.

Virtually all e-currency services offer options of 'virtual' keyboards for logging in to accounts. They may be a bother, but they are very effective at adding a formidable obstacle for cyber-invasion. Then, whether or not you took this step to access your account, make sure you take the time to actually log out of your account, as opposed to merely clicking away to your next site.

I note that the Longer Life site has two very good preventive products as sponsors, Kaspersky Labs and Identity Guard. They are first-class products and well worth your while to consider.

This stuff doesn't take long to research or to implement and you don't have to be a geek to do it. You don't even have to know their their terminology. Instead, when you're done, you can confidently refer to a familiar term in both sports and banking:

Safe.