National Cyber Security Awareness Month
(October 2008) Newsletter Series (2 of 4)

Social Engineering

"Those who cannot learn from history are doomed to repeat it."
~ George Santayana

Remember the number 80 the next time you feel the urge to click on an email attachment or follow a web link that you are not sure you should. That is the number of computers that were infected as a result of 80 or more of us clicking on infected attachments on Monday September 8th 2008. Another number worth remembering is $50,000, as this is the estimated cost to the University associated with remediation and cleanup efforts.

Last week's newsletter focused awareness on malware. This week's newsletter will focus on Social Engineering. Social Engineering is simply someone attempting to trick you into doing something you would not otherwise do. We covered this subject somewhat last spring with the rash of Phishing incidents (See entitled "Phreaking, SPAM, Phishing, Botnets, Pharming, Vishing, SMiShing & SPIM oh my"). Technology can play a role in protecting us but only to a point. What will truly help is for us to educate each other on how to better spot Social Engineering schemes. I'm a big advocate of learning from history (as the alternative implies that we must learn by making our own history). So let's look at a short history of Social Engineering Scams.

Social Engineering in Higher Education

University of Illinois Chancellor Email Spoofed – University of Illinois officials are working to track down who sent a fraudulent email message purportedly from Chancellor Richard Herman.

University of Tennessee student accused of social engineering his way into Alaska Governor Sarah Palin's yahoo account.

University of Otago mass SPAM – Over this past summer four Otago university staff members responded to a spear Phishing scam with their email IDs and passwords which were later used to send out 1.5 million SPAM messages.

University of British Columbia campus police tricked into ignoring alarms during an art heist.

University of Nottingham student committed suicide after falling victim to an online scam.
Kansas University students targeted by vishing attack.

North Carolina State University Psychologist found that computer users have a hard time distinguishing between fake Windows warning messages and the real thing.

Indiana University Hit man Spam– Back in 2007 an unknown individual gained access to an Indiana University student's e-mail account and used the Indiana University e-mail account to send out as many as 2,000 e-mails claiming to be a "hit man" hired to "terminate" the e-mail recipients.

Yale admissions scammed by former Columbia student

University of California Berkeley students created fictitious booster to throw off UCLA athlete.

Other Social Engineering Examples

Weight loss scam – weight loss trial participants duped out of deposit.

Malicious "anti-spyware" sites – Site offered a free scanner that would alert computer users to infections on their system. In reality, the user was installing malware onto their computer.

Spoofed YouTube site – Spam purporting to show a video clip posted on YouTube directed recipients to a site that showed a YouTube logo and a message implying that they should click on another link and hit “run” to see the actual video. When they did malware was installed.

Fraudulent e-cards – Sent out especially around holidays such as Valentine’s Day, these messages announced that the recipient had received an e-card from someone. If the recipient clicked through to the website, they downloaded malware in the background.

Free Games, Psycho Kitty and other youth-oriented applications and sites – Targeting younger demographics these websites look appealing and fun but actually infect visitors’ computers.

Pharmaceutical spam – The spam messages directed recipients to credible-looking sites offering drugs. The sites were well designed, and included legitimate-looking information, cleverly forged logos and seals of approval, from pharmaceutical industry watchdogs. These criminal websites usually fulfill the orders with counterfeit or inferior pharmaceuticals.

MP3 attachment spam – Messages purported to be song samples from well known recording artists, but instead the audio files actually contained advertisements that pushed a stock scam.

Looking at these lists someone may be thinking, who would ever fall for such obvious scams. Well let's see, how about corporate executives and cyber security experts just to name two apparently gullible groups.

Now that we have a better understanding of the type of social engineering attacks that historically have worked, my hope is that we will think twice before we click!! Next week's newsletter will focus on a number of the ramifications of falling for social engineering attacks.

Regards,

Michael Rodriguez CTSO @ Western Illinois University
MA-Rodriguez@wiu.edu