FCC Computer Security Notice

COMPUTER SECURITY WEEK 2002

SOCIAL ENGINEERING

In order to counteract the increasing amount of computer software and hardware used to prevent hackers from gaining entry into systems, hackers have employed methods to bypass these technical security measures altogether.

Social Engineering, often referred to as "people hacking," is an outside hacker's use of psychological tricks on legitimate users of a computer system to gain information (usernames, passwords, personal identification codes (PINS), credit card numbers and expiration dates) needed to gain access to their systems.

Despite the automation of machines and networks today, there is not one single computer system in the world that is not dependent on human operators at one point or another. There will always be people who have to provide information and maintenance.

Social Engineering has existed in some form or another since the beginning of time, primarily because most of us are helpful and trusting people. It's human nature.

Methods of Attack - Some Social Engineering techniques include: telephone scams, hoaxes and virus e-mail. For the most part, Social Engineering techniques are identical to those used by con artists. Other activities such as "Dumpster Diving" have been used to glean information from trash. People such as temporary employees and cleaning crews are sometimes used to walk through a building, checking out all the post-it-notes stuck to monitors and looking for passwords. Other techniques include dropping a bogus survey in the mail offering a cash award for completion and asking some seemingly subtle questions that are designed to reveal personal information.

Despite the immeasurable security threat Social Engineering brings to the computing community, very little is ever said about it. The primary reason for the lack of discussion about Social Engineering can be attributed to shame.

Most people see Social Engineering as an attack on their intelligence, and no one wants to be considered "ignorant" enough to have been duped. This is why Social Engineering gets put in the closet as a "taboo" subject. No matter who you are, you are susceptible to a Social Engineering attack.

So what can we do to combat Social Engineering and keep our users data safe and secure?

The first thing to be accomplish is increased security awareness. All FCC staff needs be aware of how much the public knows about your position. In addition, be aware of how much information about you is available on the Internet. People will search the Internet for your name and attempt to impersonate.

Be sensitive to anyone asking you for your passwords, or any other sensitive information. Proceed with the greatest amount of caution possible when responding to inquiries.

Keep in touch with the organizations that you can trust for current and dependable information regarding security issues.

Keep up to date with current news and read about security events posted on reputable websites.

Social Engineering is an exploit method that can only grow more dangerous as people "forget" to make security their priority.

COMPUTER SECURITY TIP OF THE WEEK:

IT IS COMPUTER SECURITY WEEK HERE AT THE COMMISSION. KEEP AN EYE OUT FOR THE COMPUTER SECURITY WEEK EVENTS ON THE NEWLY DESIGNED CSP WEBSITE.

YOU CAN REFERENCE ADDITIONAL INFORMATION ABOUT COMPUTER SECURITY WEEK AT:

- The Computer Security Week Website: http://intranet.fcc.gov/omd/itc/csg/index.html