Social Hacking (also known as Social Engineering)

Introduction

Very sophisticated technology can sometimes be defeated by the simplest of means. As long as there are people who will lie, cheat or steal and people who are honest that do not generally come into contact with them, there will be vulnerability. Social hacks use lies and trickery. They are used to accomplish specific access goals or play pranks. They may be perpetrated by malicious thieves or saboteurs or by social misfits. Common social hacks include Emails trying to get you to give up your password by some means.

Some common social hacks are not very technical at all.

- Shoulder Surfing. Someone watches over your shoulder as you enter passwords.
- Telephone calls, possibly seemingly internal calls if you are at work, claiming to be a network administrator who needs something from you. This might not be as obvious as a password, which would alert you, but perhaps ask you to type something at your computer. Perhaps something like IPCONFIG and then read them a certain number that shows up. At this point, this social hacker will have your IP address. This can help them gain access.
- Dumpster Diving. A not very glamorous way of saying, “going through your trash.”

Taking Action

- Shred anything that even possibly has identifying information on it. At work and at home. Shred information which someone could use to feign legitimacy within your organization or to someone who knows you. Even if you do not actually throw out your password, with a few bank statements someone can learn a lot about you. Being careful with your bank statements and sensitive documents at work isn't enough. Anything that someone else could use to help convince others they are legitimately you is potentially dangerous.

- Be aware of who is nearby when you enter passwords to access your system or login to sensitive areas.
- Do not offer any information over the telephone or via Email regarding any aspect of your computer or your company's computer or system. The exception to this is if you have a high degree of confidence you know with whom you are dealing. (Or you initiated the contact in the first place.) In any case, it's a rare situation when a network administrator would actually need access to your password.
- Be careful what you feed your computer. If, for example, you receive a floppy disk or CD ROM in the mail and it's of suspicious origin, do not put it in your computer. Unless you can be confident of the origin, it's possible this could be a trap. It's a fairly involved thing for an attacker to do, but neither all that complicated or expensive.
- Be wary of free software offered via junk Email, chat spam or instant message spam. Downloading and installing it could result in a virus.
- Be careful whom you let have access to your computer, even to repair it. Your friend's friend may be a computer wiz, but he may also enjoy snooping. Make sure you have a reasonable trust level regarding anyone to whom you are going to hand over access.
- A frequent attempt at social hacking is to get an Email claiming that you need to log into "the system" for one of many reasons. For example, an AOL Email may claim you need to log in immediately to test your privacy settings. A link will take you to a log in page which looks just like AOL. You may log in and subsequently get an official looking diagnostic page and thank you. But if you look carefully at the web address (that is, the Uniform Resource Locator (URL)), you will notice it is not an AOL address. Or you may be tricked even further. The website may automatically bounce you back to the real service's log in screen. At that point, you will not even be aware your password has been compromised.

- Do not be fooled by fake companies. Though more involved, it's easy enough to get a temporary 800 number and pose as a legitimate company. Any social engineering scheme can gain great legitimacy if the attacker seems to be part of a real entity.
- Be suspicious of being hustled or conned. For example, if your company policy is to escort people from the security door to where they are going, make sure someone is doing that. Remember that illusion and misdirection are used not only by stage magicians, but con artists as well.

Beyond the Basics

Remember that social hacking is essentially no different than any confidence scheme. Any con game is a matter of using your good will and trusting nature against you. Most of us are conditioned–ideally–to be somewhat open to new people and ideas. This is a healthy thing most of the time. If you are being targeted for real by a social hacker, it's not such a good thing. It's difficult to present social hacking techniques and not be accused of either being paranoid or spreading paranoia. There's an old expression though, which goes, "You are not paranoid if it is true." What you need to think about from a security perspective is what your own situation is and do you have any significant risk level..

Are you likely to be heavily gamed in order to get access to your home computer, either in place or after being stolen? Probably not. Then again, are you a high net worth individual? "No," you say. Are you sure? "No," relative to what? What about your company?

Additional Resources

Internet

SANS InfoSec Reading Room

Many papers on computer security, including social hacking. Note: this site uses .pdf files embedded in a web page. It may not work for some browsers.
www.sans.org/rr
SecurityFocus

A true and truly scary story about a real life social hack test. If you think it was a fluke, check the links at the bottom of the page for more.
www.securityfocus.com/infocus/1527
Computer Emergency Response Team (CERT)
Advisory on social engineering
www.cert.org/advisories/CA-1991-04.html
University of Dayton School of Law
Definitions and descriptions of several forms of computer crime.
cybercrimes.net