HACKING WETWARE - SOCIAL ENGINEERING

All computer systems are made up of three essential systems which are all co-dependent. These three are:

- Hardware, this is the actual physical components making up the computer system
- Software, these are the logical programs which give the hardware it's functionality
- Wetware, this encompasses the users of the above two systems.

Wetware is the weakest link in this setup. These days you need at least some technical expertise to perform an attack on the hardware or the software systems. Hacking people -or conning them- is a lot easier. You ask any IT person who has been around the block once or twice; "What is the easiest way to get someone's password?", and I am certain they will answer something along the lines of "Ask them for it". And you know what? It works! This is called "Social Engineering" which can be nicely defined as manipulating people to gain information or access you should not have. The weakest link in any setup is always the people using it or looking after it. So lets look at this problem in more detail.

Why is there a problem?
Attackers can perform these types of attacks over the phone, with email or direct contact. Basically anyway that they can "access" the people using the system. But how do they use that access? thats the catch...

- *If you look nice or sound nice you must be nice.*
  Like it or not, people judge other people by how they look, act and sound. If you look like a technician, act like one and sound like one, then people will generally assume you are one. You will be surprised how often just being confident and acting like you belong somewhere gets people to think that perhaps you actually have got a right to be there. Now think about the people who tend to have a large degree of access around your systems, like cleaners.
- *Confidence counts.*
  We mentioned this previously, but it is very important. Even the best costume and the most blatant name-dropping will not help if the social engineer seems nervous. When a person appears confident and assured about who they are, what they are doing and where they are going to, they are very seldom questioned.
- *Default trust.*
  People generally trust other people until they are given a reason not too. This is a very normal and common behavioral pattern, otherwise we would spend our days huddled in a corner. But that still does not stop attackers from using this trait to their advantage.
- *People like to help.*
  We are all conditioned from an early age to try to help where we can, society encourages this behavior. Again this is a normal and good behavioral pattern, but it is also one exploited by attackers.
- *People like to feel important.*
  Not everyone is a CEO or Lead Scientist or some other VIP, in fact for every one of these people there are probably a couple hundred everyday workers. But everyone wants to feel important, we all want to feel special, listened to, to have attention paid to us. So when an attacker preys on these feelings, they can generally find easy targets.

They won't catch my staff...
Social engineering can include a person trying to go in "cold", in other words, without knowing anything about your company and it's people. Sometimes they may even succeed, but generally they do a bit of research in order to make their "attacks" more realistic, more tailored. How do they do this? Quite easily as it turns out...

- *Corporate Knowledge.*
  Companies very often publish contact details with names on their websites, sometimes with addresses. Sometimes you find an address book. Searching for published articles relating to or about the company, can also yield a wealth of information. Running searches through online usergroups can also give out details. Heck, if you trawl through online resume sites, where someone currently working at the company has posted their resume, you will be surprised at what you find.
- *Corporate Trash.*

Do you know what you throw away? All those print-outs, think about whats on them. Old IT equipment, imagine seeing whats on those old tapes or hard-drives. What about old intra-company literature? With phone lists and name lists.

- *Networking.*
  When your staff go out to lunch or to a pub after work, who do they talk to? What do they say? What about when your staff go to conferences? Thats a prime place for attackers to chat to people and find out more.
- *Ask.*
  What do your staff do when someone phones looking for the IT manager because they want to send a CV through, then they ask for the email address as well? Generally just asking for information with a semi-plausible reason will get you the information you want.

But so what?
The scope for social engineering attacks is limited only by the attackers imagination and the gullibility of people, this means that it is a very diverse field and the attacks can have different "payloads". They are also a class of attacks which are difficult to fully list, but lets take look at some of the more common types of these attacks...

- *Ask and ye shall receive.*
  We have touched on this before but you will be surprised at what you can get by asking. Imagine this; a smartly dressed person walks into your company and speaks to your receptionist. They say they are from XXX technology company, and that you are actually one of their biggest clients, and his company has asked him to send some small token of appreciation to the IT team, but he doesn't want to mess up. Can he just have phone list so that he gets the spelling of their names right? If he gets this, he now has names, numbers, possibly email addresses and whatever else. This information can be used in many ways.
- *Impersonation.*
  This is a classic class of attack. Here the attacker impersonates someone in order to perpetrate the attack. Imagine this; one of your staff gets a call, the lady on the other end knows them by name, identifies herself with a known name and phone number of an IT person. She then says that she has heard that the staff members internet/email/whatever has been slow and she would like to take a look at it. Could she have his username and password to just check it out. She can also mention the names of some people around him to further the illusion that she is from the company. If she gets this information, she now has a valid username and password to get onto the system.
- *Mislead.*
  This is similar to the impersonation, but with a twist. Here the attacker gets access or information by misleading someone about their intent. Imagine this; a person comes into the building and says that he is a fire inspector and he is here to inspect the premises for compliance with the new building code 12ID1T. If you do not mind he just needs to go to some areas of the building and take some air samples and readings. He walks around, and can see any documentation lying around which could include passwords, phone lists, pretty much anything printed and not nailed down. And if he is not watched, then he may even take them with.
- *Anger.*
  This attack takes a different tack, it uses emotion to throw a person off balance and thus give out information. Imagine this; a lady phones the receptionist, and starts off loud and very angry complaining about poor service and loss of time and anything else. She demands to speak to the manager, in fact, she wants the managers direct line, email address and cellphone number just so that she knows she will be able to get in touch with him, or else she will involve the papers or lawyers or who knows what. The poor receptionist will most likely give her the details just so that she does not have to deal with it.
- *Flatter.*
  Same as the above approach just from the opposite angle. Here the attacker makes the staff member feel important and therefore more helpful. Imagine this; a junior technician gets a call from some guy, he says he is part of the audit team busy working with finance, and the finance director told him that if he needed any help he was to call the technician direct because he knew what he was doing and would be able to help. Now he is trying to get onto the wireless network just to share some files quickly, could he please have the wireless key to connect, thats it. He does not want to take the technician away from doing other more important work. How often do you think the technician will give up the wireless key?

- *Terminology*.
  This attack can stand on its on, but is more often used to make other social engineering attacks more successful. Company staff are used to certain people having certain nicknames, or certain processes being called something. Every company has its own slang and culture, if the attacker can use the same slang and references it gets straight away puts people off their guard. I like to think of it as putting the attack into context.

It cannot get worse..
Yes it can. A lot worse. Remember that the information gained from social engineering attacks may not of itself mean a compromise, but it can be easily used to make a normal cyberattack more successful. For example, if you have a list of names, it makes choosing usernames to bruteforce a lot easier. If you have the titles of people, you can further refine your attempts. Social engineering can at worst result in an easy compromise, and at best can make a normal attack more focused and successful. Social engineering attacks have spawned many other areas which are complete topics and attacks in their own right;

- *Phishing*, using email to harvest a persons sensitive details using crafted emails, websites and anything else.
- *ID thef*t, using information about a person to impersonate them in order to steal money, credit, even -in one case- a house.
- *Privacy Invasion*, selling personal information to other people for purposes ranging from marketing to robbery.
- *Dumpster divin*g, going through a companies trash in order to steal information.
- *Malware*, using cleverly crafted emails or web pages to get users to install software -or allow it to be installed- which gives an attacker access.
- *Social engineering viruses*, all those fake virus emails, prank emails, etc. Not only do they waste considerable resources in bandwidth, disk space, etc. But if a user actually listens to them they can get the user to cause damage to their own machine.

What do I do?
This one is difficult, you see the only real protection is education. The problem is that (and I know I am going to get nailed for this), some people are either too thick to listen or just do not want to listen. Assuming you are one of those lucky and blessed people who do not have to worry about these 2 classes of people, then you must educate your users. Teach them what information they should never give out, teach them to always make sure about who they are talking to, phoning a person back is a helpful step. Also consider the idea of a chokepoint applied to social engineering, instead of asking the users to think, just tell them to redirect all queries to one person, and make sure that person knows what they are doing. Lastly, when doing a penetration test on your network, remember to test the staff as well.

Final Words
Social engineering attacks are not a nice neat package of attacks, there is no easy answer or fix (Well actually there is no real easy fix for any class of attacks, but the vendors would like you to think otherwise). There is no software or appliance you can buy to sort the problem out. This is when a company's commitment to information security is tested, because only with proper management support, proper policies in place, training and vigilance will you have a chance of stopping these attacks. Have fun and learn.