R 70

Cyber Security – Social Engineering - Reading

WARNING: This sheet discusses ways in which computers and networks are misused. It is illegal to use these techniques yourself.

Social Engineering

It is not easy to break into computer systems by hacking passwords or other security methods. However, all computer systems are accessed by people who are often the weakest part to the security of any system. Social engineering involves getting hold of **confidential** information by social means. People are manipulated into giving information away which they shouldn't.

Blagging (pretexting)

Blagging (**pretexting**) is impersonating another person in order to try and get confidential information. A blagger may impersonate a family member, police officer, colleague at a company, bank manager, or anyone else who they feel may give them credibility.

Many phone calls in the UK are made as a form of blagging to attempt to find personal information about the receiver. This can often seem innocent, such as finding out the version of operating system you have, but the information will then be sold to other companies with your address so that they can try to sell you other products. Some blaggers may tell you that your computer has problems and they need you to **download** software to fix it. This then gives them full access to your computer. Blagging and phishing attacks are a common way for **ID theft** to occur.

To obtain a **password** a hacker might contact the reception of a business and claim to be assisting with a virus and need to test that it is fixed. They ask if the receptionist would run a program or put them through to someone who can. By using fear or other techniques they can get people to give them passwords or help them to break into systems.

Phishing

Phishing is a type of **social engineering** technique where someone attempts to find out sensitive information such as usernames, passwords or credit card details. The word was created as the technique often uses bait to catch a victim.

Phishing techniques will often use **fake websites** or **spam** to lure victims into giving away personal information. By changing the way links appear in an email many people believe they are visiting an official site. For example, a bank called "Jones Online Bank" may have the **subdomain** jonesoffers.jonesonlinebank.com for offers. A hacker could buy the **domain name** jonesoffers.com and then create the subdomain jonesonlinebank.jonesoffers.com. They could then record all usernames and passwords attempted and use these on the real bank site.

Pharming

When a **web address** is entered it is converted to an **IP address** by a DNS server. **Pharming** changes the domain name to go to a different IP address which contains a fake website. This can then be used to obtain personal information.

Shouldering/Shoulder surfing

Shouldering simply involves standing near someone as they enter a PIN at a bank machine or their password at a computer. It is easy to see what has been entered.