Social Engineering

Social engineering involves manipulating **people** so that they give up confidential information, allowing other people to gain access to a system.

In terms of cyber security, people (users) are often the weakest element in terms of keeping a system secure. Technological systems might be extremely secure, but if people make mistakes the system can become vulnerable very easily.

Some elements of social engineering involve using technology; some simply involve people.

The three types of social engineering you need to know about are:

- blagging
- shoulder surfing
- phishing

Blagging (pretexting)

Blagging could be as simple as someone calling a company and claiming to be someone who has forgotten their log in details. By "blagging" their way, they may be provided with log in credentials or confidential information.

Blagging involves inventing a scenario to try to get a target victim to give up information. This might be done using an e-mail, a phone call or face-to-face.

The information revealed might be as precise as log in or bank account details or may be general information which might allow a hacker to piece together useful information to gain access. Or it could gather valuable information to sell – for example, quizzes on social media sites which can reveal marketing preferences.

For example, reception staff might be trained to never confirm that any individual works for an organisation.

Organisations need to provide training to reduce the risks of users falling for blagging and to put in place routines to reduce the risks that staff will give up information. They can employ **penetration testing** to check their security routines.

Shouldering (shoulder surfing)

This is looking over someone's shoulder to observe information. Most commonly, this would be log in or PIN code details (e.g. at a cashpoint machine). This can be done physically or by using cameras – which have the advantage that they can be replayed.

Users leaving computer systems unlocked when stepping away from their desks is a similar problem.

ATM fraud is a major problem. Shouldering can be combined with stealing or cloning cards.

Organisations can make sure people know the risks of shoulder surfing. They can also pay attention to the layout of work areas to make sure the risks are reduced. At banks there are sometimes lines to stand behind at ATMs or signs are posted to make people aware of the issue.

Phishing

Uses e-mail or text messages in order to "**phish**" for information. The bait for the phishing attempt will usually be a link or button to click.

In many ways, phishing is a form of blagging done electronically.

Phishers will often pretend to be the users bank, online account (e.g. PayPal or Facebook) or services such as postal companies with parcels to deliver. By clicking the link you might download malware or be sent to a pharming operation.

Spam filters will often identify phishing e-mails and firewalls can be configured to stop people responding to them. Educating users about the issue is also important – when specific threats are identified this can identify particular e-mails to avoid.

Spam filters are a lot more advanced now than they used to be and will pick up many phishing e-mails.

Many finance companies make it clear that they will never send e-mails asking for passwords and log in details and will only ever contact users by phone if there is a problem with their account.

Users can also be made aware that phishing e-mails often contain give-aways: such as not being personally addressed or being poorly written with standard English grammar mistakes.

The FBI estimates that phishing attacks which claimed that companies owed money for computing parts cost American companies $676 million in 2018.

Activities:

a) Write a definition of the term **social engineering** [3 marks]
b) Summarise the **three** types of social engineering scam and how they can be managed
c) Describe the ways that users can identify phishing e-mails [4 marks]
d) Research examples of recent phishing attacks. What makes them effective and what have organisations done about them?
e) Obidos Travel has seven customer service operatives. Explain **three** things that the organisation should do to ensure that they deal with the threats from social engineering [6 marks]