Security threats and defenses

Technology, Information Technology

Security Threats and Defenses Need for security measures. Social engineering has caught on among many professionals. The techniques in use are based on cognitive biases, which are attributes of man decision making. Social engineers are aiming at exploiting these biases by creating attack techniques. Consequently, every company is at a risk of being attack by one of the many techniques in use.

Preparing employees to recognize and respond to social engineering techniques will at help to protect the company in many ways, which include:

1. Use strong passwords.

By using strong passwords in the computer network, they will protect the company from against unauthorized access to company's confidential information and identity theft.

2. Protecting confidential information

The employees will not only learn about the importance of protecting information but will also familiarize themselves with laws and policies which strongly prohibit sharing of confidential information such as passwords to computers.

3. Making sure that virus protection s up to date.

This will protect the company from losing valuable data and information due to virus invasion.

4. Others include being wary of suspicious mails, using secured applications and backing up data.

As the level of technology advances, social engineering techniques in use are advancing to. These techniques include:

1. Phasing

This involves obtaining private information fraudulently. The victim receives communications via emails from legitimate institution such as a bank. The mail comes with a form requesting for many details including ATM’s card PIN.

2. Interactive Voice Response

The victim required to verify some information and directed to call the bank via a free toll number. The login will be rejected severally ensuring the victim keys in passwords multiple times.

3. Diversion theft

This is a trick exercised by professional thieves to con companies. It persuades the responsible person for deliver to deliver it elsewhere.

4. Pretexting

Pretexting aims at engaging a victim in a manner that leads to the victim divulging information or engage in activities which he/she could not be involved in under ordinary circumstances.

5. Shoulder surfing

Some social engineers will take advantage in public places such as cyber cafes. They memorize access codes after looking over someone’s shoulder (Basole, 2008).

Reference

Basole C. R. (2008). Enterprise mobility; applications, technologies and strategies. Amstadam ; IOS press.