Term 4 Theory Notes

Social engineering tricks

Social engineering is a technique used to gain access to a facility's systems, data and anything else by exploiting basic human psychology.

Some of these tricks include:

- Phishing is usually done via email where an attacker tricks people into giving out personal information or handing over money. Phishing is used with email spoofing and website spoofing. The most common phishing scam is an email from your bank to say your account has been suspended and that you need to reset the password by clicking on a link that takes you to a website that looks like your bank's website. When you enter your account details; the attacker will have your information.
- Phishing and email spoofing: Phishing and email spoofing attacks try to obtain sensitive information (such as usernames, passwords and banking details) by sending emails to users that look like official emails. These emails will either directly request the sensitive information, or redirect users to an official-looking website from where their information will be stolen.
- Pharming: Much like phishing, pharming attacks create an official-looking website that requests sensitive information. A very common pharming attack allows users to "change" their passwords. Instead of changing their passwords, the user's username and password are recorded and their account is taken over.

Ransomware

Malware that makes data unavailable until you pay the hacker a ransom fee. To protect yourself from ransomware, install an anti-virus and keep it updated.

Click jacking

Click jacking is an attack in which a site appears to do one thing but your clicks are redirected to do something else.

Add on's and server programs can be installed on the browser to protect users on a network.

There are five key things that determine the quality of information:

- Authority: This is based on who created the information. If the video you are watching was not created by someone with knowledge in the field, then the information they are giving you might not be the best out there. Always do research on the people who give you information. Authority also indicates that the information is accurate.
- Accuracy: Look for how complete the information is and compare the information from one source against the information from a few others. If the facts match, you can be fairly sure that the information is accurate. Make sure

Free past papers and study resources: studypapers.co.za

that there is something backing up the facts you receive. Check the source of those facts as well.
- Currency: Check how current the information is. More up-to-date information tends to be more accurate. A technology blog from 2010 will be less relevant, and therefore less accurate, to your research than one from 2017. Information from the last ten years is seen as current.
- Objectivity: Make sure that the author is being objective. Look out for information that is sponsored by a company (that is, if it is a type of long-form advertisement called a sponsored post). This information may be biased towards the facts that the sponsor wants to represent to make their product or information seem like the best.
- Relevance: Lastly, look at how well the information covers the topic you are researching. If the information only covers a small portion of the topic, then it is possibly not the best information to use. You need to look for information that answers about 80% of any question you are trying to find the answer for.

Data protection

It is important to back up your data regularly, since hardware can fail or accounts can be compromised. Backing up data lets you protect and store information.

CREATING A BACKUP

Because a backup is simply a copy of your computer's data, it can be created using the *Copy* and *Paste* functions.

Screen lock pattern

A pattern lock is a security feature commonly used on smartphones and tablets that allows users to unlock their device by drawing a specific pattern on a grid of dots. Instead of entering a numerical PIN or password, the user connects a sequence of dots in a predetermined order to gain access to the device.

Introduction to AI

Artificial intelligence is the simulation of human intelligence in machines that are programmed to think and act like humans. Learning, reasoning, problem solving and language comprehension are all examples of cognitive abilities.

Examples of AI

- Digital assistants (Siri, Cortana)
- Text editing (Grammarly, Quilbot)

Online harassment

Online harassment is a wide range of damaging behaviours such as hateful messages, distributed denial-of-service (DDoS) attacks, defamation and others. The goal of the harasser is to drive the target off the internet or punish them by publishing personal information, sending threats, or promoting harm.

Free past papers and study resources: studypapers.co.za

Malware and security software

MALWARE (MALICIOUS WARE)

Malware is any software that is specifically designed to disrupt, damage or gain unauthorised access to a computer. Examples of malware are:

1. Viruses
2. Worms
3. Trojans
4. Scareware
5. Spyware
6. Adware
7. Ransomware

To prevent your computer from becoming infected with malware, computer experts suggest that you do the following:

- Do not open suspicious emails.
- Do not download suspicious programs or attachments.
- Keep your antivirus application up to date.
- Keep your other software up to date: Hackers can use software weaknesses or vulnerabilities to gain access to your computer.

E-commerce and e-banking

When using online services such as online banking or shopping, you must be careful that your information is not stolen. Your banking or credit card information can be used to make multiple purchases.

Tips for safely using online banking and shopping include:

- Use proper antivirus software and make sure it is up to date.
- Do not log into online banking or shopping sites using public Wi-Fi or on public computers (like those in an internet café).
- Make sure that the operating systems on all your devices are up to date. This is important for both your phone and computer. Make sure that the banking app on your phone is also up to date.
- Change your passwords regularly and make sure they are strong.
- Do not sign into your banking account through a link in an email as this is most likely a phishing attack.
- Sign up for notifications on your bank account for when money comes in or goes out and when your account is accessed online.

ADVANTAGES OF E-COMMERCE

- There is a very wide range of products and services available.
- There are no geographical limitations. It is just as easy to buy something from the USA or Europe as it is to buy it in South Africa.
- It definitely saves you time, for example travel time, waiting time and searching time.
- It is available 24/7.

Free past papers and study resources: studypapers.co.za

RISKS OF E-COMMERCE

- Fraud: Because transactional data is transmitted over the internet, it has become one of the target areas of cybercriminals. Financial information can be hacked or stolen, leading to purchases made by people who are not the rightful owners of that information. Customers sometimes complain that they have not received their packages and it is difficult to determine whether that is true or not.
- Online security: There are many security threats such as malware, spam mail and phishing that can cause you harm.
- Exchanging a product that does not fit the online description can be difficult.

ADVANTAGES OF E-BANKING

- It is convenient, as customers have 24-hour access to the bank, seven days a week.
- It can be done from any location where you have Internet.

RISKS OF E-BANKING

- Fraudulent transactions
- Online theft of your access ID/user ID or PIN/password could happen.
- Banking apps can be compromised.

Anti-virus

All the computers in a network should also have anti-virus software installed to protect them from being infected with malware, viruses and other harmful programs. Anti-virus software constantly scans the programs on a computer and destroys any threats.

Free past papers and study resources: studypapers.co.za