FEEDBACK TUTORIAL LETTER

1st SEMESTER 2019

ASSIGNMENT 1

INFORMATION ADMINISTRATION 3A

IAD710S
Dear Student

This letter serves to give feedback on Theory Assignment 1 that was part of the First Tutorial letter.

With regard to the answers you have provided, I will give general remarks on each question as well as the correct answer.

**QUESTION 1**

Most of you understood this question fairly well and answered it good. Compare your answer with the correct one below:

**Hacker**
The term hacker was originally a complimentary word for computer enthusiast. Now it has a derogatory meaning and refers to someone who accesses a computer network illegally. They claim to improve security.

**Cracker**
A cracker also accesses a computer or network illegally, but has the intention of destroying data, stealing information or performing other malicious actions. Both hackers and crackers have advanced computer and network skills.

**Script kiddie**
A script kiddie has the same intent as a cracker, but does not have technical skills and knowledge. Script kiddies are often teenagers that use prewritten hacking and cracking programs to break into computers.

**Corporate spies**
Corporate spies have excellent computer and network skills and are hired to break into a specific computer program and steal its proprietary data and information. The reason for this is to gain competitive advantage.

**Unethical employees**
Unethical employees break into their employer's computer for a variety of reasons. Some want to exploit security weaknesses; others seek financial gains from selling confidential information, and disgruntled employees may want revenge.

**Cyber extortionist**
A cyber extortionist is someone who uses e-mail as a vehicle for extortion. These perpetrators send a company a threatening e-mail message indicating they will
expose confidential information, exploit a security flaw, or launch an attack that will compromise the company’s network, if they are not paid a sum of money.

Cyber terrorist
A cyber terrorist is someone who uses the Internet or network to destroy/damage computers for political reasons. The extensive damage might destroy the nation’s air traffic control system, electricity-generating companies or a telecommunications infrastructure. Cyber terrorism usually requires a team of highly skilled individuals, millions of dollars and many years of planning.

QUESTION 2
In general this question was also answered well, although some of you misinterpreted it completely.

The correct answer is:

Virus spreading through E-mail
Unscrupulous programmers create a virus program that deletes all files. They hide the virus in a picture and attach the picture to an e-mail message.

They use the Internet to send the e-mail message to thousands of users around the world.
Some users open the attachment and their computers become infected with the virus

Other users do not recognise the name of the sender of the message. These users do not open the e-mail message – instead they immediately delete the message. These users’ computers are not infected with the virus.

QUESTION 3
This question about computer Cookies was answered satisfactory. Most of you did not provide enough facts for the sum total of the question.

Compare your answer with the correct one below:

Cookies
A Cookie is a small text file that a Web server stores on your computer. Cookie files contain data about you, such as your user name or viewing preferences.
E-commerce and other Web applications often rely on cookies to identify users and customise Web pages.

Cookie files typically contain data about you, such as your user name or viewing preferences.

Many commercial web sites send a cookie to your browser, and then your computer’s hard disk stores the cookie. The next time you visit the Web site, your browser retrieves the cookie from your hard disk and sends the data in the cookie to the Web site.

Web sites use cookies for a variety of purposes:

Most Web sites that allow for personalisation use cookies to track user preferences. Some Web sites use cookies to store users' passwords, so they do not need to enter it every time they log in to the Web site.

Online shopping sites generally use a session cookie to keep track of items in a user's shopping chart.

Some web sites use cookies to track how regularly users visit a site and the Web pages they visit while at the site.

Web sites may use cookies to target advertisements. These sites store user's interests and browsing habits in the cookie.

Many commercial Web sites send a cookie to your browser, which is stored by your computer's hard disk.

The next time you visit the Web site, your browser retrieves the cookie from your hard disk and sends the data in the cookie to the Web site.

QUESTION 4

In general, this question about Spoofing was not answered well enough. Read carefully before you answer.

The correct answer is:

Spoofing is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network.

Several types of spoofing exist.

One type – IP spoofing, occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source.
Perpetrators of IP spoofing trick their victims into interacting with the phony web site. For example, the victim may provide confidential information or download files containing viruses, worms, or other malware.

The spoofing process can be used to steal passwords.

They typically launch a spooper program that mimics the mainframe computer’s login screen on an unattended terminal in a public lab.

When an unsuspecting student/user inserts an ID and password, the program responds with an error message and remembers the secret codes.

**QUESTION 5**

Most of you provided good answers to this question.

Compare yours with the one below:

Informational Accuracy

Intellectual Property Rights

Codes of Conduct

Information Piracy

[4]

**TOTAL: 50**

**GENERAL**

Keep the following in mind when you answer an assignment:

1. Always remember to **read** each question carefully before you answer it.
2. Think about the question first and then decide what the answer should be and how you should formulate it.
3. Rather write too much than too little.
4. Look at the mark allocation at each question - that should give you an idea of how many facts you need to provide.
5. Apply the knowledge that you have and make the questions your own.
6. Think practically.

7. Do research and read more about the contents of the questions you need to answer.

8. Read my remarks at your answers in the assignment and try to avoid the same mistakes in the next assignment.

After all, your assignments were satisfying. Keep on studying and read about the subject whenever you can.

Best regards

[Signature]

G. du Plessis
Marker-tutor: Information Administration 3A Theory