DAGRI PAST PAPERS

SIR ARTHUR LEWIS COMMUNITY COLLEGE

EXAMINATION SESSION: December 2017 Final Examination (Alternate)

TUTOR: Mrs. P. Erlinger-Ford, Mrs. S. Eristhee, Mrs. L. Sargusingh-Terrance, Miss G. Severin, Mr. V. Lucien, Mr. T. Weekes, Miss Z. John, Ms. N. Fevrier, Mrs. Gale Stephens, Ms. R. Anthony

PROGRAMME TITLE:

COURSE TITLE: Communication Studies 103

COURSE CODE: COM 103

CLASS (ES): Year I

DATE: Wednesday 31st January, 2018

TIME: 9:00 a.m.

DURATION: 2 ½ hours

ROOM:

INVIGILATORS:

INSTRUCTIONS:

1. Students are reminded to read **ALL** questions and instructions in each section very carefully.
2. ANSWER **all** questions from Section A which are worth a total of 25 marks.
3. ANSWER **one** question from Section B. Section B is worth 35 marks.
4. **NB:** Bags, books, as well as writing paper not given by the invigilator should be deposited at the front of the examination room or as otherwise indicated.
5. **NB:** All cell phones are disallowed in the examination room.

SECTION A: READING COMPREHENSION (25 marks)

Security and Privacy for Computers and the Internet

There was a time when security and privacy issues related to computers were easily managed: You simply locked the computer room door. Those centralized days are, of course, long gone. Now, in theory, anyone can hook up to any computer from any location. In light of data communication access, the first issue is security. The vast files of computer stored information must be kept secure - safe from destruction, accidental damage, theft, and even espionage.

A second issue is privacy. Private data - salaries, medical information, Social Security numbers, bank balances, and much more - must be kept from prying eyes. The problems are many and the solutions are complex. The escalating expansion of the Internet has only heightened the existing problems and added new problems of its own.

Computer Crime

It was 5 o'clock in the morning, and 14-year-old Randy Miller was startled to see a man climbing in his bedroom window. "FBI," the man announced "and that computer is mine." So ended the computer caper in San Diego where 23 teenagers, ages 13 to 17, had used their home computers to invade computer systems as far away as Massachusetts. The teenagers were hackers, people who attempt to gain access to computer systems illegally from a personal computer, via a data communication network.

The term *hacker* used to mean a person with significant computer expertise, but the term has taken on the more sinister meaning with the advent of computer miscreants. In this case the hackers did not use the system to steal money or property. But they did create fictitious accounts and destroyed or changed some data files. The FBI's entry through the bedroom window was calculated: The agents figured that, given even a moment's warning, the teenagers were clever enough to alert each other via computer.

This story - except for the names - is true. Hackers ply their craft for a variety of reasons but most often to show off for their peers or to harass people they do not like. A favorite trick, for example, is to turn a rival's telephone into a pay phone, so that when his or her parents try to dial a number an operator interrupts to say, "Please deposit 25 cents." A hacker may have more sinister motives, such as getting computer services without paying for them or getting information to sell.

You will probably not be surprised to learn that hackers have invaded Websites. These vandals show up with what amounts to a digital spray can, defacing sites with taunting boasts, graffiti, and their own private jokes. Although the victims feel violated, the perpetrators view their activities as mere pranks. In reality, such activity is antisocial and can result in great expense.

Of all targets that hackers might choose, one would expect the venerable *New York Times* to be far down the list. But no, the *Time's* Website was seriously invaded. Hackers plastered messages across the screen, forcing the *Times* to shut down the site entirely.

The *Times* was not chosen randomly, however. The hackers, it seems, were displeased with articles in the newspaper about fellow hacker Kevin Mitnick, who had been convicted on a series of computer-related theft and forgery charges. (When arrested, he was in possession of over 10,000 credit-card numbers taken from a customer database of an Internet service provider site.) The messages placed on the *Time's* site demanded his release. Mitnick, however, remains in prison.

Hackers and Other Miscreants

Hacking has long been thought the domain of teenagers with time on their hands. The pattern is changing, however. A recent government survey showed that the computer systems of over half of the largest U.S. corporations had been invaded, but not by teenagers. Most intruders were competitors attempting to steal proprietary information. Even more astounding, federal investigators told a U.S. Senate hearing that the U.S. Department of Defense computers are

attacked more than 200,000 times per year. Most worrisome is the emerging computer attack abilities of other nations, which, in a worst-case scenario, could seriously degrade the nation's ability to deploy and sustain military forces.

Hackers ply their craft by surprisingly low-tech means. Using what is called social engineering, a tongue-in-cheek term for con artist actions, hackers simply persuade unsuspecting people to give away their passwords over the phone. Recognizing the problem, employers are educating their employees to be alert to such scams.

Hackers are only a small fraction of the security problems. The most serious losses are caused by electronic pickpockets who are usually a good deal older and not so harmless. Consider these examples:

- A brokerage clerk sat at his terminal in Denver and, with a few taps of the keys, transformed 1, 700 shares of his own stock, worth $1.50 per share, to the same number of shares in another company worth 10 times that much.

- A Seattle bank employee used her electronic fund transfer code to move certain bank funds to an account held by her boyfriend as a "joke"; both the money and the boyfriend disappeared.

- A keyboard operator in Oakland, California, changed some delivery addresses to divert several thousand dollars' worth of department store goods into the hands of accomplices.

- A ticket clerk at the Arizona Veteran's Memorial Coliseum issued full-price basketball tickets for admission and then used her computer to record the sales as half-price tickets and pocketed the difference.

These stories point out that computer crime is not always the flashy, front-page news about geniuses getting away with millions of dollars. These people were ordinary employees in ordinary businesses - committing computer crimes. In fact, computer crime is often just white-collar crime with a new medium. Every time an employee is trained on the computer at work, he or she also gains knowledge that - potentially - could be used to harm the company.

The Changing Face of Computer Crime

Computer crime once fell into a few simple categories, such as theft of software or destruction of data. The dramatically increased access to networks has changed the focus to damage that can be done by unscrupulous people with online access. The most frequently reported computer crimes fall into these categories:

- *Credit-card fraud.* Customer numbers are floating all over public and private networks, in varying states of protection. Some are captured and used fraudulently.

- *Data communications fraud.* This category covers a broad spectrum, including piggybacking on someone else's network, the use of an office network for personal purposes, and computer-directed diversion of funds.

- *Unauthorized access to computer files.* This general snooping category covers everything from accessing confidential employee records to the theft of trade secrets and product pricing structures.

- *Unlawful copying of copyrighted software.* Whether the casual sharing of copyrighted software among friends or assembly-line copying by organized crime, unlawful copying incurs major losses for software vendors.

Keeping a Secret

Employers wish that computer passwords were better-kept secrets. Here are some hints on password use.

- Do not name your password after your child or car or pet, an important date or your

phone number. Passwords that are easy to remember are also easy to crack. If a hacker can find out personal details about a victim, he or she can deduce a password from this information about 40 percent of the time.

- Make passwords as random as possible. Include both letters and numbers. The more characters the better. Embed at least one no alphabetic character, and consider mixing uppercase and lowercase letters. Example: GO*TOP6.

- Keep your password in your head or in a safe. Astonishingly, an occasional thoughtless user will scribble the password on paper and stick it on the computer monitor where anyone can see it.

- Change your password often, at least once a month. In some installations, passwords are changed so seldom that they become known to many people, thus defeating the purpose.

- Do not fall for hacker phone scams - "social engineering" - to obtain your password. Typical ruses are callers posing as a neophyte employee ("Gosh, I'm so confused, could you talk me through it?"); a system expert ("We're checking a problem in the network that seems to be coming from your workstation. Could you please verify your password?"); a telephone company employee ("There seems to be a problem on your phone line"); or even an angry top manager ("This is outrageous! How do I get into these files anyway?").

Most people are naturally inclined to be helpful. Do not be inappropriately helpful. Keep in mind that you will be - at the very least - embarrassed if you are the source of information to a hacker who damages your company.'

White-Hat Hackers

Faced with threats on every side, most network-laced companies have chosen a proactive stance. Rather than waiting for the hackers and snoops and thieves to show up, they hire professionals to beat them to it. Called *white-hat hackers or* tiger teams, or sometimes "intrusion testers" or "hackers for hire," these highly trained technical people are paid to try to break into a computer system before anyone else does.

Using the same kind of finesse and tricks a hacker might, white-hat hackers exploit the system weaknesses. Once such chinks are revealed, they can be protected. The hackers' first approach, typically, is to access the company's system from the Internet. The quality of security varies from company to company. Sometimes security is fairly tight; other times, as one hacker put it, "It's a cake-walk."

Sometimes companies will hire one company to establish security and then hire white-hat hackers to try to defeat it. The company may not even alert its own employees to the hacker activities, preferring to see whether the intrusions are detected and, if so, how employees react.

From H. L. Capron, *Computers: Tools for an Information Age,* 6th Edition

After reading the selection, answer the following questions with A, B, C, or D.

1. The best statement of the main idea is

   A. security and privacy of computers and the Internet can be maintained by following a few simple rules of prevention.
   B. millions of dollars are lost each year because of computer crimes by hackers and other miscreants.
   C. computer crime is a growing and serious threat to the security and privacy of computers and the Internet.
   D. in the future computers and the Internet will be protected by white-hat hackers who defeat intrusions.

2. According to the passage, the FBI entered by the bedroom window of Randy Miller's house primarily because

   A. they feared a personal attack if entering through the front door.
   B. the teenagers were gathered in the bedroom.
   C. they suspected that the computers at the U.S. Department of Defense had been invaded.
   D. they wanted to secure the evidence before Miller could alert the other teenagers on his computer.

3. According to the passage, changes in the pattern of hacking show a progressive movement from

   A. espionage to graffiti.
   B. teen pranks to corporate theft and espionage.
   C. stealing proprietary information to turning a rival's phone into a pay phone.
   D. electronically pickpocketing money from companies to spray painting Websites.

4. In a social engineering scam, a password is obtained by

   A. asking.
   B. electronically entering the system.
   C. figuring it out from family records.
   D. reading it off a note on a computer.

5. The term "white-collar" crime refers to

   A. vandalism by teenagers.
   B. theft by workers with office jobs.
   C. spying for defense secrets by foreign agents.
   D. defacing Websites with private jokes.

6. The author implies that the motive for the hacker attack on the *New York Times* was

   A. greed.
   B. a teenage prank.
   C. revenge.
   D. to support Mitnick's imprisonment.

7. The author implies all of the following about credit cards except that

   A. some companies do not have sufficient protection of credit card information.
   B. credit card numbers are housed in many places on the Internet.
   C. money can be made from credit card fraud.
   D. copyright theft is the first largest crime on the Internet and credit card theft is the second.

8. According to the author's advice on keeping your password secure, you should

   A. mix alphabetic and nonalphabetic characters.
   B change it no more than once a year.
   C. use your phone number or family names.
   D. write your password down and keep it in the office.

9. White-hat hackers are hired by companies to

   A. invade the computer security of a rival company.
   B. find ways to infiltrate the computer security of the company that hired them.
   C. locate and prosecute rival computer hackers.
   D. train technical people to become computer hackers.

10. The underlying reason for the author to present the four different examples of electronic pickpocketing is to

    A. show four different ways ordinary people can commit computer crimes.
    B. compare and contrast adult and teenage hackers.
    C. show that people who commit computer crimes are usually detected and exposed.
    D. calculate the revenue that companies lose through computer theft by employees.

Answer the following with T (true) or F (false).

11. The author would be more likely to compare the old key to the computer room to your current password than to your computer's speed and power. _____

12. The author implies that teenage hackers are not serious threats on the Internet and should not be prosecuted. _____

13. The reader can conclude that companies always alert employees when white-hat hackers are hired. _____

14. The reader can conclude that computer hacked that crosses state lines is a federal offense. _____

15. The author implies that security and privacy issues will lead to a gradual decline of Internet popularity. _____

Vocabulary

According to the way the underlined word was used in the selection, select a, b, c, or d for the word or phrase that gives the best definition.

1. "kept from prying eyes"

    A. dishonest
    B. curious
    C. disapproving
    D. illegal

2. "ended the computer caper"

    A. illegal escapade
    B. arrest
    C. investigation
    D. trail

3. "more sinister meaning"

    A. humorous
    B. significant
    C. relevant
    D. evil

4. "with the advent"

    A. coming
    B. violation
    C. assault
    D. domination

5. "computer miscreants"

A. mistakes
B. investigators
C. villains
D. coming

6. "ply their craft"

A. learn
B. perform
C. share
D. desire

7. "defacing sites"

A. canceling
B. locating
C. monitoring
D. disfiguring

8. "by unscrupulous people"

A. unethical
B. ignorant
C. knowledgeable
D. unknowing

9. "used fraudulently"

A. frequently
B. occasionally
C. mysteriously
D. deceitfully

10. "as a neophyte employee"

A. sneaky
B. beginner
C. disloyal
D. careless

SECTION B: WRITING (35 marks)

Select one of the following topics and write an Expository essay of 400-500 words.
Your essay must have a clear **thesis statement**.

1. Discuss the major effects of any virus on an individual, country or society.
2. Classify and explain the different genres of music that attract most young people in the Caribbean.
3. Explain how a natural disaster can act as a serious impediment to one of our main industries in St. Lucia.
4. Why is our diet important?
5. Discuss some of the benefits of computer technology to any business or industry.
6. Compare and contrast any two sports
7. Discuss the contributing factors to stress.
8. How would you define a successful business?