



**Romel Cabiling** ▾



[Home](#)

[Home](#) > [My courses](#) > [Social And Professional Issues](#) > [03 Computer Hacking](#) > [Lesson Proper for Week 3](#)

# Lesson Proper for Week 3

## DEFINITIONS OF HACKING

The computer ethicist, Duncan Langford (1995), states that in the 1960s and 1970s the term 'hacker' was used to describe an individual working with computers who was technically gifted. From a traditional perspective, therefore, a hacker was considered to be an expert, skilled programmer, rewriting code to customize and improve it. In the early days of computing there was no implication that someone known as a computer hacker would act illegally.

Nonetheless, the social and computing environment has changed greatly since the 1960s, and the use of the term 'hacker' has expanded and its definition broadened. Forester and Morrison

(1990) outline several different definitions of the term 'hacker', which include:

- A person who enjoys learning the details of computer systems and how to stretch their capabilities, as opposed to most computer users who prefer to learn only the minimum amount necessary
- Someone who programs enthusiastically, or who enjoys programming, rather than just theorizing about it
- A person who is able to create programs quickly
- An expert on a particular program, or one who frequently does work using it, or on it
- A malicious inquisitive meddler who tries to discover information by poking around. For example, a password hacker is one who tries, possibly by deception or illegal means, to discover other people's computer passwords.

Today, hacking is often defined in terms of individuals who seek to gain 'unauthorized access' to computer systems, and the currently broadly accepted view of a hacker is someone who uses specialized knowledge of computer systems to obtain illegal access to them. Langford defines hacking as obtaining and exploiting unofficial access to a computer system.



The connotations of the term 'hacker' have clearly shifted away from the earlier benign meaning, towards a legal definition which is used by the authorities. Although the term suggests something malicious or subversive, this is not always the case. Typical malicious actions now covered by hacking include: breaking into public and private databases to steal, corrupt or modify data, defrauding banks, stealing credit card details, finding out private information, and spreading viruses.

The technical means of hacking have become ever more sophisticated. Information on how to accomplish hacking is often posted on specialist bulletin boards. Hackers may use a succession of computers as staging posts, to route a continuing series of attacks on different systems. In his book *The Cuckoo's Egg*, Clifford Stoll describes how, in the 1980s, US military computers were attacked by a hacker located in Germany. This was accomplished through a whole series of staging posts as the German hacker broke into dozens of US computers, including military systems, looking for information to sell to the Soviet Union.

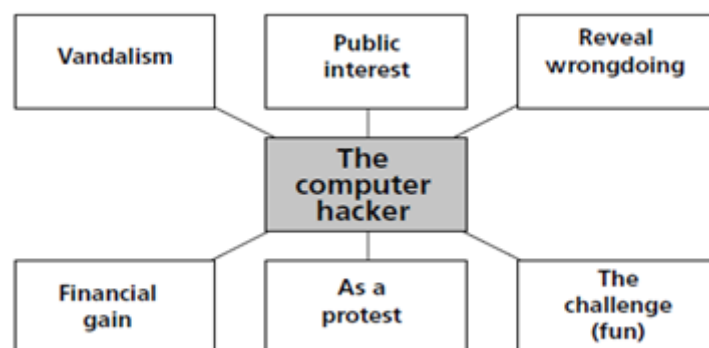
One of the more notorious and widely publicized security breaches happened to the *New York Times* on 13 September, 1998. Their website server was invaded by a group of belligerent hackers who posted pornographic material and printed this threatening message for all to see:

*'FIRST OFF, WE HAVE TO SAY ... WE OWN YOUR DUMB ASS. S3COND, TH3R3 AR3 SO MANY LOS3RS H3R3. ITZ HARD TO PICK WHICH TO INSULT MOST.'*

The site was closed for nine hours while IT personnel cleaned up the offensive messages and plugged the security breach.

In 2001, Raphael Gray, a teenage hacker from Wales, broke into several online stores and stole thousands of credit card numbers. He then published the numbers on the web and, using one of the stolen card numbers, dispatched a shipment of Viagra tablets to Microsoft boss Bill Gates. His actions sparked an international investigation that brought the FBI to the door of his parents' home in Pembrokeshire.

Why do hackers hack? The motives behind hacking are varied (see Figure 2.1) and complex. One suggestion is the satisfaction gained from the intellectual challenge involved, breaking into systems simply to see if it is possible – the challenge has been said to be similar to solving an elaborate crossword. The guessing of passwords and bypassing of file protections pose intriguing problems that some individuals will go to enormous lengths to solve, according to Forester and Morrison, (1990).



**Figure 2.1:** Computer ‘hacking’ may be undertaken for many reasons.

A motive commonly stated by hackers themselves is the exposure of loopholes and vulnerabilities in computer systems. Hackers also expose bugs in software and alert software developers so that fixes (or ‘patches’) can be made. Hackers in this sense are like unpaid security consultants. In fact, some may be employed by security companies or intelligence agencies as consultants; others may go on to start their own computer security firms.

There is an international community of these ‘professional’ hackers, some of whom attend conferences, where competitions are staged in which contestants are invited to break into rigged computer systems.

There is the playful side of hacking, where it is no more than a practical joke, albeit a disruptive or offensive one, but no harm is intended. The malicious side of hacking – as we will discuss shortly – involves the creation and distribution of viruses, or the defacing and disruption of websites. In many instances, it has involved acts of vengeance, particularly by disgruntled employees against former employers, or by individuals with grudges.

Hacking can also be conducted as a form of political activism, to make a protest, to get a particular message across, or to correct a perceived injustice. Then there is the national security aspect, where hackers are employed by government agencies or by the military to engage in espionage, sabotage or cyber war with other countries. Hacking can also be conducted on behalf of law enforcement agencies for the purposes of crime prevention and detection, or increasingly, counter-terrorism.

Finally, there is the straightforwardly criminal aspect, where hacking is a tool to commit crimes of theft, fraud, extortion or forgery. These will be covered in greater detail in the next chapter.

## **DESTRUCTIVE PROGRAMS**

Traditionally, hacking involved knowledge of programming and a certain degree of skill. Nowadays, hacking software can easily be obtained from the Internet, and hacking accomplished with rudimentary knowledge. Software can be downloaded to crack passwords or serial numbers for software installation, or to bypass other protections and security measures. Individuals, often describing themselves as hackers, anonymously release destructive software known collectively as computer viruses (because of the manner and ease with which they spread).

Let us first consider the nature of a computer virus. Quite simply, a virus is a self-replicating piece of programming code inserted into other programs to cause some sort of unexpected, and usually undesirable, event. Viruses can be transmitted by downloading a program from another computer, or can be present on a disk. The virus lies dormant until circumstances (typically a particular time or date, or the user activating another program) cause its code to be executed by the computer. Some viruses are playful in intent and effect, while others can be harmful, erasing data or causing a computer’s hard disk to require reformatting. Viruses can attach themselves to the computer’s operating systems, and other key programs, using up memory, and corrupting or erasing files. Measures for preventing and removing viruses in the form of anti-virus software will be discussed, along with other security technologies, in the next chapter.



Examples of viruses include:

- Trojan horses
- Worms
- Time or logic bombs
- Denial-of-service.

### ***Trojan horses***

The term 'Trojan horse' comes from Homer's *Illiad*. In the Trojan War, the Greeks presented the citizens of Troy with a large wooden horse, in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city. In the computing field, a Trojan horse is a program in which malicious or harmful code is disguised inside some apparently harmless programming or data (perhaps an image or sound file, or e-mail attachment).

The victim is tricked into executing the program code by opening the file or attachment, initiating a malicious sequence of events. This may include damage to files, programs or the hard disk, or modification of data. It may enable unauthorized access to a computer, through a 'back door', in such a way as to gain control of that computer. Trojan horses can involve the insertion of false information into a program in order to profit from the outcome – for example, a false instruction to make payments to a bogus company.

### ***Worms***

A worm, like a virus, is self-replicating code, that situates itself in a computer system where it can do harm. Like most computer viruses, worms usually come in Trojan horses. Worms, however, tend to take the form of stand-alone code. In other words, they do not require a specific host computer, but run independently, travelling across networks. Worms tend to exist in memory and are non-permanent, whereas viruses tend to reside on disk where they are permanent until eradicated.

In addition, worms are network-orientated, with segments of the worm inhabiting different machines. Worm programs entail the deletion of portions of a computer's memory, thus creating a 'hole' of missing information. Crucially, they use up system resources, slowing down a network, or shutting it down completely.

### ***Time bombs and logic bombs***

Time or logic bombs are programs triggered to act when they detect a certain sequence of events, or after a particular period of time has elapsed. They involve the insertion of routines that can be triggered later by the computer's clock or a combination of events. When the bomb goes off, the entire system will crash.



- Time bombs can be activated on a particular date; for example the 'Friday the 13th virus' wakes up whenever a Friday is the 13th of the month, copying itself, and attaching itself to other programs. It increases the size of the programs or files it attacks, using up computer memory, and eventually shutting the computer down
- Logic bomb is activated by a particular event or set of logical conditions. For example, a popular form of logic bomb monitors employment files and initiates systems damage (such as erasure of hard disks) once the programmer's employment has been terminated.

### ***Denial-of-service***

Another hacking tool is a denial-of-service attack in which a server, hosting a particular website, will be targeted with a massive volume of fake traffic in the form of e-mails or requests for pages or other information. These overwhelm the server and block legitimate traffic, effectively shutting down the site. The execution of such an attack usually involves the coordination of many linked machines which are often 'hijacked' for this purpose.

## **HACKER ETHICS**

Early hackers took their position seriously enough to establish their own ethical code, known as The Hacker Ethic (Langford, 1995).

The Hacker Ethic was comprised of five principal values:

- Access to computers, and anything which might teach you something about the way the world works, should be unlimited and total. Always yield to the hands-on imperative
- All information should be free
- Mistrust authority – promote decentralization
- Hackers should be judged by their hacking, not bogus criteria such as academic excellence, age, race or position
- You can create art and beauty on a computer.

### ***Hackers as public watchdogs***

One way in which hackers have been represented is as public watchdogs, revealing information the public has a right to know, and exposing the truth. Given that more and more personal information is now being stored on computers – often without our knowledge or consent – it might be reassuring (the argument goes) to know that some citizens are able to penetrate these databases to find out what is going on. It is not always in the public interest – it is argued – to have information about us withheld.



Hackers can indeed be an intelligent and critical check against governments who withhold information from the public or abuse their power. In this sense it could be argued that hackers represent one means by which we can attempt to avoid the creation of a more centralized, even totalitarian, government. This relates to the third principle of the Hacker Ethic which advocates decentralization of power and information.

### ***Hackers as security consultants***

Another key argument, from a hacker's perspective, is that the breaching of systems can provide more effective security in future, so that other, presumably less well-intentioned, hackers are prevented from causing real harm. Given the possibility of terrorist acts becoming more and more technologically sophisticated, perhaps we can also look to hackers as a resource to be used to foil such acts and to improve our existing security arrangements.

### ***Hacking as trespassing***

If computers are viewed as material possessions, then electronic entry to a computer system can be looked on as similar to physical entry into an office or home. Unless there is a specific invitation, or previous permission to enter, this could be considered trespassing, if not unlawful entry. The typical defense that hackers offer to this charge is that they are entering to test for loopholes in the software. But is this realistic or convincing? This is comparable to having a burglar break into your home in the hope that the burglar may reveal security weaknesses. Indeed, what would most people think of someone who broke into your home and went through your desk, reading any letters and personal material they happened to find?

In such a case, there seems to be a clear legal and ethical case against hacking into someone else's computer system. One counter-argument to this is to suggest that computers cannot be viewed as material possessions owned by one business or another. Langford (1995) argues that, in an undefined global community of computing (such as that represented by the Internet) physical ownership of machines is secondary to the benefit of its users. Exploring this electronic world is somehow above such considerations as 'yours' or 'mine' – electrons belong to no one.

### ***Forester and Morrison (1990) write:***

To some extent this is already happening: in the US, convicted hackers are regularly approached by security and intelligence agencies with offers to join them in return for amelioration or suspension of sentences. Other hackers have used their notoriety to establish computer security firms and to turn their covertly gained knowledge to the benefit of commercial and public institutions.

## **THE COMPUTER MISUSE ACT, 1990**

In the UK, in 1989 a working paper on computer misuse by the Law Commission made several specific recommendations for changes in the law regarding computer hacking. However, despite government promises to legislate, no official measures were taken until 1990. In that year, Michael Colvin MP introduced a Private Member's



Bill on computer misuse that incorporated many of the recommendations from the Law Commission paper, but included greatly increased penalties. In August 1990, the Bill eventually became the Computer Misuse Act.

As summarized in Figure 2.2, the Act introduced three new criminal offences:

- **Unauthorized access to computer material:**

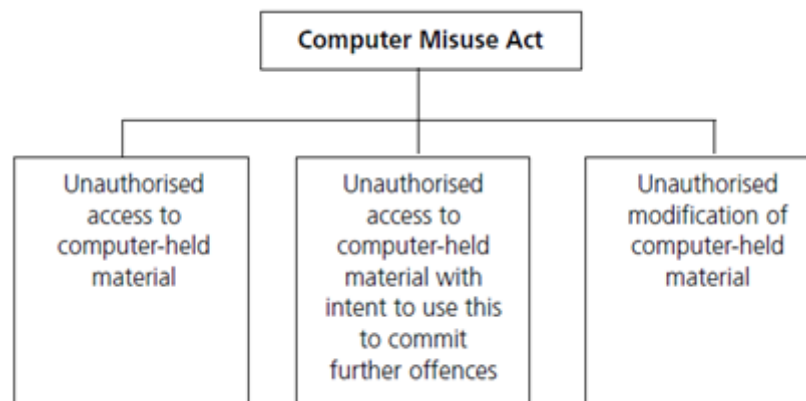
This is described as ‘simple hacking’, that is, using a computer without permission.

- **Unauthorized access to computer material with the intent to commit or facilitate commission of further offences:**

This section of the Act covers actions such as attempting to use the contents of an e-mail message for blackmail, or stealing credit card numbers. This is viewed as a more serious offence; the penalty is up to five years’ imprisonment and an unlimited fine. This offence is tried before a jury.

- **Unauthorized modification of computer material:**

This section of the Act covers distributing a computer virus, or malicious deletion of files, as well as direct actions such as altering an account to obtain fraudulent credit. This offence is also tried before a jury.



**Figure 2.2:** Three criminal offences detailed in the Computer Misuse Act

◀ Preliminary Activity for Week 3

Jump to...



Analysis, Application, and Exploration for Week 3 ▶



**Navigation**



Home

 Dashboard

Site pages

My courses

Capstone Project 1

Multimedia

Ojt/Practicum 1

Social And Professional Issues

Participants

General


01 Law And Government

02 Overview Of Computer Ethics

03 Computer Hacking

 Preliminary Activity for Week 3

 **Lesson Proper for Week 3**

 Analysis, Application, and Exploration for Week 3

 Generalization for Week 3

 Evaluation for Week 3

 Assignment for Week 3

System Integration And Architecture 2

Courses

---

## Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.







## Activities



Assignments



Forums



Quizzes



Resources

---

Bestlink College of the Philippines  
College Department

Powered by [eLearning Commons](#)

