Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 22
HACKING ETHICS AND LAWS

DRAFT

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Pete Herzog, ISECOM
Marta Barceló, ISECOM
Bob Monroe, ISECOM
Jaume Abella, ISECOM
Francisco de Quinto
Jordi Saldaña
J. Agustín Zaballos
Mario Platt
Sandeep Singh

ISECOM

Introduction

New technologies, while building a new paradigm that invades every human activity, also influence the dark side of these activities: criminal behavior of individuals and of organized groups.

For this reason, we have reserved this lesson of HHS to analyze some aspects related to Legality and Ethics, analyzing several behaviors that could end in crimes and the consequences of these crimes.

For the Internet, the driving force is anonymity. Since there is no positive identification on the Internet, it acts as an amplifier for all human behavior. Everyone believes they can get away with everything because they will never be found or pointed out. This lets criminals cast their nets worldwide. This course is intended to teach you enough to know how not to fall prey to those people. As time passes, more countries are joining in the legal fight against criminals and those who abuse the Internet. It *is* possible to trace online activity back to its source, with various governments' cooperation

A second issue is the different rate of change of technology and the courts. Technology evolves remarkably fast, with generations of technology now lasting less than a year. Courts often take months to years to try a case; governments take years to decades to adapt the body of law. The courts are simply being outpaced by change.

Foreign Crimes Versus Local rights

1. As noted above, the introduction of new technologies can result in the creation of new dark sides of activities: criminal behavior of individuals and organized groups. There are two main characteristics through which **Information Technology and Communications (ITCs)** are related to crime:

2. Technologies renew traditional ways of breaking the law. These are illegal activities which traditionally appear in the penal codes, but are now being executed in new ways. Examples include **confidence scams** ("**con jobs**"), money laundering and illegal types of pornography.

3. In addition, because of their own innovation, ITCs are resulting in the appearance of new types of criminal activities, and because of their nature, these new crimes are in the process of being added to the legislation of several countries. Examples include the distribution of spam and virus attacks. A specific example would be the banking theft malware distributed on the Internet. The victim typically visits a website that is legitimate but has been poisoned by the criminals. The victim unknowningly downloads a piece of malware that installs itself to their computer. The malware "watches and listens" for them to do their banking online. Then it either steals their banking credentials (ID and password) or uses the online banking session to execute unauthorized electronic transfer of funds to foreign bank accounts.

Another characteristic of the ITCs which must be emphasized is their territorial displacement, which affects the general surroundings but without any doubt affects other countries as well. Previously, areas of law always had a clear territory regarding the judicial authority judging (**Competent Jurisdiction**) and regarding the law to be applied in the judging (**Applicable Law**). Both concepts are still noticeably geographic. With the worldwide distribution of the Internet, crime now may involve many countries, all with their own laws.

In summary, we can say that the ITCs are global and international, while the law and the courts are limited to a specific state or territory. The law thinks "geographically," while the ITCs "think worldwide." This disorientation is even more confusing than it initially appears. Although we are not aware of it, a bidirectional online communication between a user in Barcelona, Spain and a Web site hosted in an ISP in California can pass through more than 10 ISPs, hosted in a variety of remote points around the world. Facing this diversity of addresses and nationalities, it becomes necessary to ask *What laws of which country will be applied in case of litigation? Which of the possible countries will be the suitable court to adjudicate the case?*

The relatively recent European Council's agreement on cyber-crime was signed in November 2001 in Budapest by almost 30 countries, including the 15 partners of the European Union, the United States, Canada, Japan and South Africa. This agreement intends to restore the TERRITORIAL PRINCIPLE to define competent jurisdiction. The signing of this agreement is the culmination of four years of work that have resulted in a document containing 48 articles that are organized into four categories:

- Infractions against confidentiality
- Falsification and computer science fraud
- Infractions relative to contents
- Violations of intellectual property

Once the especially complex regulations and sanctions on criminal activity on the Internet have been described, consensus must then be reached on three main areas of concerns or difficulties:

1. **Jurisdiction Conflict:** Election of the most competent court for judging multinational and multi-border crimes. This problem is not definitively solved by any of the known judicial systems.
2. **Conflict of Laws:** Once the court has been chosen, the first obstacle that the court faces is choosing the law applicable to the case. Again we are forced to conclude that traditional legal criteria are not designed for the virtual surroundings.
3. **Execution of Sentence:** Once the competent court has determined a sentence, the sentence must be carried out, possibly by a different country than the country which dictated the sentence. Therefore, it is necessary to have an international commitment to recognize and accept any sentences imposed in other countries. This problematic issue is even more complicated to solve than the two previous ones. Would your country be willing to accept its citizens sentenced by courts in the United States of America? Russia? China? France? Germany?

These complications were clearly demonstrated in the recent case of a hacker in Russia, who had hacked several US systems, and was invited to a phony US company for an interview. During the interview, he demonstrated his skills by hacking into his own network in Russia. It turned out that the interview was actually conducted by the FBI, and he was arrested. The FBI used sniffers placed on the interview computer to raid the hacker's computer in Russia and download evidence that was used to convict him.

But there are many unresolved issues:

1. Was it legal for the FBI to examine the contents of a computer in Russia, without first obtaining permission from the Russian government?
2. By inviting the hacker to the US, the FBI did not have to arrange for his extradition to the US. Was this legal?
3. Could the US convict a person for crimes that were technically committed on Russian soil?

Finally, he was convicted in the US, because he had used a proxy server in the US to conduct some of the attacks. He served just under four years in prison and now lives and works in the US.

Exercises

12.1 Conduct a modified white-hat/black-hat discussion of at least one of these questions (examination of a computer on foreign soil; invitation or entrapment(?) to avoid extradition; conviction for internet crimes committed against a country from foreign soil).

1. First, focus on and list reasons why the chosen topic was probably legal.
2. Then reverse and focus on and list why the chosen topic was probably illegal.
3. After these completely separate discussions, see if the class can reach a decision.
4. If you were to take the knowledge from these courses and execute crimes online, are they willing to face the jurisdiction of a different country?

Note – these questions are interesting for discussion. There are no right answers governments are still working to come to a consensus on these and other issues related to the international nature of these crimes. This exercise is purely for critically

examining and thinking about internet crimes, as well as formulating a logical argument for an opinion related to internet crimes.

Crimes Related to the ITCs

This section discusses legal issues from the view of the Spanish body of law. Similar issues will apply in your country. The particular laws, phrasing, and sentences may be different. A good exercise is investigating which laws apply in your country; which tools may be against the law in your country; and the potential punishments that apply, both to minors and to adults. With that knowledge, you may better decide whether you wish to engage in certain activity. For example: child pornography laws apply to minors in the United States. If you take a sexually explicit picture of yourself or your friend(s) and send it or store it anywhere, and any of those people are under-age, you have committed child pornography. The penalties are severe. In some countries, even the possession of tools for "hacking" is against the law. Do your homework.

The classification of criminal behaviors is one of the essential principles in penal systems. For this reason, several countries must think of changes to their penal codes, such as Spain, where the effective Penal Code was promulgated relatively recently. The well known Belloch Penal Code was approved on November 23rd 1995 (Organic Law from the Penal Code 10/1995) and it recognizes the need to adapt the penal criteria to the present social reality.

Among others, we can classify potential criminal actions into the following six sections.

1. Manipulation of data and information contained in files or on other computer devices.
2. Access to data or use of data without authorization.
3. Insertion of programs/routines in other computers to destroy or modify information, data or applications.
4. Use of other peoples' computers or applications without explicit authorization, with the purpose of obtaining benefits for oneself or harming others.
5. Use of the computer with fraudulent intentions.
6. Attacks on privacy, by using and processing of personal data with a different purpose from the authorized one.

The technological crime is characterized by the difficulties involved in discovering it, proving it and prosecuting it. The victims prefer to undergo the consequences of the crime and try to prevent it in the future rather than initiate a judicial procedure. This situation makes is very difficult to calculate the number of such crimes committed and to plan for preventive legal measures.

This is complicated by the constantly changing technologies. However, laws are changing to increasingly add legal tools of great value to judges, jurists and lawyers to punish crimes related to the ITCs.

Next we will analyze some specific crimes related to the ITCs.

1. Misrepresentation: The anonymity of the internet allows users to pretend to be anyone they want to be. Crimes may be committed when users pretend to be someone else to gain information, or to gain the trust of other individuals.
2. Interception of communications: Interceptions of secrets or private communications, such as emails, or cell phone transmissions, using listening

devices, recording, or reproduction of sounds and or images. (Note: in some countries, even possessing equipment capable of such interception is against the law. For example: Singapore.)

3. Discovery and revelation of secrets: Discovering company secrets by illegally examining data, or electronic documents. In some cases, the legal sentences are extended if the secrets are disclosed to a third party.
4. Unauthorized access to computers you do not own: Illegal access to accounts and information, with the intent of profiting. This includes identify theft. Think of the example of the banking theft malware given above.
5. Damaging computer files: Destroying, altering, making unusable in any other way; damaging electronic data, programs; or documents on computers, networks or systems you do not own.
6. Illegal copying: Illegal copying of copyrighted materials, literary, artistic, or scientific works through any means without the specific authorization of the owners of the intellectual property or its assignees.

It is possible to set up an isolated, closed network, not communicating with computers you do not own, and practicing any and all "hacking," in some countries. As soon as you touch a computer that you do not own, you are probably breaking the law.

Exercises

12.2 Choose one of the topics above, and conduct the following searches:

- Find a legal case which can be classified as the chosen type of crime.
- Was there a legal judgment, and if there was, what sentence was applied?
- Why did the authors commit this crime?

12.3 Regarding intellectual property: Are the following actions a crime?

- Photocopying a book in its totality
- Copying a music CD that you have not bought? Sharing that with others?
- Copying a music CD you have bought? Sharing that with others who have not bought the music?
- Downloading music MP3, or films in DIVX from Internet, with and without paying for the content? Sharing that with others?
- What if it were your music or movie that you created, and you make your living as a musician or videographer and were not getting royalties for? What if it were your artwork, that others were copying and stating that they had created it?

Prevention of Crimes and Technologies of Double Use

The only reliable way to be prepared for criminal aggression in the area of the ITCs is to reasonably apply the safety measures that have been explained throughout the previous HHS lessons. It is extremely important for the application of these measures to be done in a way so that it becomes practically impossible to commit any criminal or doubtful behaviors.

It is important to note that technologies can have multiple uses and the same technique used for security can, simultaneously, result in criminal activity. This is called **Technologies of Double Use**, whose biggest components are cryptography and technologies used to

intercept electronic communications. This section discusses the reality of this phenomenon and its alarming consequences at all levels of the human activity including policy, social, economic and research.

Global Monitoring Systems and the Concept of COMINT

The term **COMINT** was created by integrating the terms **"COMmunications INTelligence**" and refers to the interception of communications. COMINT as a practice has existed since ancient times, with encryption or obfuscation techniques equally ancient. For a simple example, search for information on "Caesar codes." Then search on the background for "steganography." Nowadays, COMINT represents a lucrative economic activity providing clients, both private and public, with intelligence on demand, especially in the areas of diplomacy, economy and research. This resulted in the displacement of the obsolete scheme of military espionage with the more or less open implementation of new technologies for the examination and collection of data.

Two representative examples of COMINT technologies are the systems "ECHELON" and "CARNIVORE" which are discussed next.

ECHELON

The **ECHELON** system has its origins in 1947, just after World War II, in an agreement between the UK and USA with clear military and security purposes. The details of this agreement are still not completely known. Later, countries like Canada, Australia and New Zealand joined the agreement, working as information providers and subordinates.

The system works by indiscriminately intercepting enormous amounts of communications, no matter what means is used for transport and storage, mainly emphasizing the following listening areas:

1. Broadband transmissions (wideband and Internet)
2. Facsimile and telephone communications by cable: interception of submarine cable traffic by means of ships equipped for this
3. Wireless communications, including radio and cell phone communications
4. Voice Recognition Systems
5. Biometric System Recognition such as facial recognition via anonymous filming

Later, the valuable information is selected according to the directives in the Echelon System, with the help of several methods of Artificial Intelligence (AI) to define and apply keywords. Keywords are simply words or phrases of interest to the collector.

Each one of the five member countries provides "KEY WORD DICTIONARIES" which are introduced in the communication interception devices and act as an "automatic filter." Logically, the "words" and the "dictionaries" change over time according to the particular interests of the member countries of the system. At first, ECHELON had clear military and security purposes. Later, it became a dual system officially working for the prevention of international organized crime (terrorism, organized crime, trafficking in arms and drugs, dictatorships, etc.) but with an influence reaching Global Economy and Commercial Policies in companies.

Lately, ECHELON has been operating with a five-point star structure around two main areas. Both are structures of the NSA (National Security Agency): one in the United States, coinciding with their headquarters in Fort Meade (Maryland), and another one in England, to the north of Yorkshire, known as Meanwith Hill.

The points of the star are occupied by the tracking stations of the collaborating partners:

- The USA (2): Sugar Grove and Yakima.
- New Zealand (1): Wai Pai.
- Australia (1): Geraldtown.
- UK (1): Morwenstow (Cornwell).
- There was another one in Hong Kong before the territory was returned to China.

It would be a reasonable assumption that almost any country would have such a system. The more the government wishes to retain power, the more likely such a system will be turned on that government's populace.

Exercises

12.4: Is it appropriate for *your* country to listen in on the communications of other countries? Why or why not? Is it appropriate for *your* country to listen in on the communications of its citizens and populace? Why or why not? Is it appropriate for your country to listen in on the communications of visitors? Why or why not? How do *you* wish to be treated?

CARNIVORE

The second great global system of interception and espionage we will consider is the one sponsored by the US FBI and is known as **CARNIVORE**, with a stated purpose of fighting organized crime and reinforcing the security of the US. Because of its potent technology and its versatility to apply its listening and attention areas, CARNIVORE has caused a head-on collision between a state of the art technical system, political organizations (US Congress) and mass media, not to mention the citizens of the country.

CARNIVORE was developed in 2000, and is an automatic system, intercepting internet communications by taking advantage of one of the fundamental principles of networking technology: the dissemination of information in "packets" or groups of uniform data. CARNIVORE is able to detect and to identify these "packets of information." This is supposedly done in defense of national security and to reinforce the fight against organized and technological crime.

The American civil rights organizations immediately protested this as a new attack on privacy and confidentiality of electronic information transactions. One group, the Electronic Privacy Information Center (EPIC) has requested that a federal judge order the FBI to allow access by ISPs to the monitoring system – to ensure that this system is not going to be used beyond the limits of the law.

In the beginning of August 2000, the Appeals Court of the District of Columbia rejected a law allowing the FBI to intercept telecommunications (specifically cell phones) without the need to ask for previous judicial permission (wiretap warrants), through a Federal Telecommunications Commission project that tried to force mobile telephone companies to install tracking devices in all phones and thus obtain the automatic location of the calls. It would have increased the cost of manufacturing equipment by 45%.

With these two examples, we see the FBI's intention to create a domestic Echelon system, centering on the Internet and cell phones, known as CARNIVORE. The project has been widely rejected by different judicial courts in the US and by Congress, as there is no doubt it means an aggression to American civil rights, at least in this initial version.

The project is being rethought, at least formally, including the previous judicial authorization (such as a search warrant) as a requirement for any data obtained to be accepted as evidence in a trial.

IC3 – Internet Crime and Complaint Center

The Internet Crime and Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C),established May 8, 2000 to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local or international law enforcement or regulatory agencies for any investigation they deem to be appropriate.

The IC3 receives more than 300 000 complaints per year and helps in adjusting heavy dollar loss.

Ninety Percent of the complaints received by IC3 are from the United States of America; the remaining 10 percent comes from countries like Canada, the UK, Australia and India.

Every year IC3 issues an Internet Crime Report both the scope of Online Crime and IC3's battle against it. IC3 also involves itself in conducting awareness activities for the people and several training activities for Law Enforcement bodies from time to time.

Convention on Cyber Crime – Council of Europe

The Council of Europe Convention on Cybercrime, which entered into force in July 2004, is the only binding international treaty on the subject to have been adopted to date. It lays down guidelines for all governments wishing to develop legislation against cybercrime. Open to signature by non-European states, the convention also provides a framework for international co-operation in this field.

Exercises

12.4 There is a joke about these COMINT systems on the Internet. We include it here for class discussion of the ethical and legal implications:

An old Iraqi Muslim Arab, settled in Chicago for more than 40 years, has been wanting to plant potatoes in his garden, but to plow the ground is very difficult work for him. His only son, Amhed, is studying in France. The old man sends an email to his son explaining the following problem:

"Amhed, I feel bad because I am not going to be able to have potatoes in my garden this year. I am too old to plow the soil. If you were here, all my problems would disappear. I know that you would plow the soil for me. Love you, Papa. "

A few days later, he receives an email from his son:

"Father: For God's sake, do not touch the garden's soil. That is where I hid that . . . Loves you, Amhed. "

The next morning at 4:00, the local police, agents of the FBI, the CIA, S.W.A.T teams, the RANGERS, the MARINES, Steven Seagal, Sylvester Stallone and some more elite representatives of the Pentagon suddenly appear and plow up and turn over all the soil searching for any materials to construct pumps, anthrax, whatever. They do not find anything, and eventually go away.

That same day, the man receives another email from his son:

"Father: Surely, the soil is ready to plant potatoes. It is the best I could do given the circumstances. Love you, Ahmed."

Exercises

Search for information about the ECHELON and CARNIVORE systems on the Internet, as well as their application on networks and ITCs in your country to answer the following questions:

1. What does the term "ECHELON" mean?
2. What elements form the ECHELON system?
3. What elements form the CARNIVORE system?
4. Search for an example of controversy attributed to the ECHELON system and related to famous personalities.
5. Search for an example of the application of the CARNIVORE system related to a TERRORIST known worldwide.
6. What is your opinion about the "legality" of such systems?
7. What is your opinion about the "legality" of such systems in your own country?

12.5 Find the list of countries which are members of the Convention on Cyber Crime – Council of Europe

12.6 Search for the latest IC3 Cyber Crime Report and find out the most frequently reported Internet Crimes last year

Ethical Hacking

Besides talking about criminal behaviors, crimes, and their respective sanctions, we must make it very clear that being a hacker does not mean being a delinquent or breaking the law.

Nowadays, companies are hiring services from "**Ethical Hackers**" to detect vulnerabilities in their computer systems and therefore, improve their defense measures. The term itself is a little unfortunate, because it implies that other hackers are unethical – which simply is not true. "Ethical Hacker" is just a catchy title for certifications.

All hackers, with their knowledge, help to define the parameters of defense. They do "controlled" attacks, previously authorized by the organization, to verify the systems' defenses. They create groups to learn new attack techniques, exploits and vulnerabilities, among others. They work as researchers for the security field.

Kevin Mitnick said " The degree of threat presented by any conduct, whether legal or illegal, depends on the actions and intent of the individual and the harm they cause."

Sun Tzu said in his book **The Art of War**, "Attack is the secret of defense; defense is the planning of an attack."

You must know what the attacks may be like to be able to defend yourself.

Hacking, ethical or not, is divided in several phases:

1. Attack Planning/Information Gathering (Reconnaissance) (See Document Grinding)
2. Scanning & Enumeration

3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Final Reporting

One helpful tool that Ethical Hackers use is the **Open Source Security Testing Methodology Manual (OSSTMM)** method. This method is for the testing of any security system, from guards and doors to mobile and satellite communications and satellites. At the moment it is applied and used by important organizations that include:

- Financial institutions
- The US Treasury Department (for testing financial institutions)
- US Navy and US Air Force

Apart from the freely and widely used OSSTMM methodology, the other standards and methods being developed and used for ethical hacking or Penetration Testing are PTES – Penetration Testing and Execution Standards, the OWASP – Open Web Application Security Project for testing Web Application and many more like NIST, FISMA, etc…

Exercise

12.7 Find information about Ethical Hacking and its role in IT security companies.

12.8 Find out detailed information about the phases involved in Ethical hacking

12.9 Search for information about the OSSTMM and similar methods.

12.10 Search for information about certifications related to Ethical Hacking.

The Most Common and Frequent Internet Frauds

Listed below is a summary from different sources about the most common crimes on the Internet as of 2012.

1. **Nigerian 419 Scams: 419 scams**, frequently called **Nigerian scams** are summary names for a large number of confidence frauds in which the victim is defrauded for monetary gain. The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud. This scam usually begins with a letter or email purportedly sent to a selected recipient but actually sent to many, making an offer that would result in a large payoff for the victim. The email's subject line often says something like "From the desk of barrister [Name]," "Your assistance is needed," and so on. The details vary, but the usual story is that a person, often a government or bank employee, knows of a large amount of unclaimed money or gold which he cannot access directly, usually because he has no right to it. The scam goes on to request the victim to send an amount of money, or provide bank information, so the "money" may be transferred through the victim's bank account, in exchange for a percentage of the "take." The scammers either collect the "processing fee" or use the bank information to steal all the victim's bank accounts.
2. **Pay Pal Fraud:** Many times with PayPal scams, one is scammed when they have someone respond to an online ad they have placed on Craigslist or some other similar site. The scammers will usually respond to the ad, stating that they are

interested in the product that is being sold and that the product will be sent to a friend or family member within the country. Many times these scammers are people from a foreign country who are promising to pay more money than what the seller asked for in the first place. After shipping the item and after the seller pays, you'll realize that soon enough, PayPal has taken the money from your account, and that you're out of the item you were trying to sell. Many times the "buyer" will contact PayPal saying that they never received the item, or in even worse cases, the scammer will use a fake PayPal address or a stolen account.

3. **Work from Home:** A **Work from Home scheme** is a get-rich-quick scheme in which a victim is lured by an offer to be employed at home, very often doing some simple task in a minimal amount of time with a large amount of income that far exceeds the market rate for the type of work. The true purpose of such an offer is for the perpetrator to extort money from the victim, either by charging a fee to join the scheme, or requiring the victim to invest in products whose resale value is misrepresented. Another version is to have the victim "receive" and "reship" items. The items have been bought fraudulently. The victim pays the postage, ships the item, and then is not reimbursed for the receipt or the shipping. You spend money to send the loot to the criminal, usually overseas.

4. **Fake Auctions/Sales:** The scammer creates an ad or auction on a website like E-bay or Craigslist, stating that he/she has a certain item for sale, usually something that is pretty expensive to begin with, for a very low price. The scammer knows that people will jump all over this "deal," without even stopping to think that it could be fake and just a luring act for money. Plenty of people fall for it, making this particular scam a huge success. They send money; the item is never delivered. If it sounds too good to be true, it probably is.

5. **Online Dating/Romance:** A **romance scam** is a confidence trick involving feigned romantic intentions towards a victim, gaining their affection, and then using that goodwill to commit fraud. Fraudulent acts may involve access to the victims' money, bank accounts, credit cards, passports, e-mail accounts, or national identification numbers or by getting the victims to commit financial fraud on their behalf. A common scheme is to explain that the romantic partner has an immediate, short-term need for money to solve a family problem or for medical reasons. They gradually ask for more and more money for other problems. That "cute young blonde" or "handsome dark-haired guy" may really be a middle-aged sleazy criminal.

6. **Credit Card Fraud:** Surf the Internet and view adult images online for free, just for sharing your credit card number to prove you're over 18. Fraudulent promoters use those credit card numbers to run up charges on the cards.

7. **Investments:** Make an initial investment in a day trading system or service and you'll quickly realize huge returns, or so they claim. But big profits always mean big risk. Consumers have lost money to programs that claim to be able to predict the market with 100 percent accuracy. Think about it: if they were that good, why would they share it with everyone, instead of "owning" the market?

8. **Multilevel Marketing Plans/ Pyramids:** Make money through the products and services you sell as well as those sold by the people you recruit into the program. Consumers say that they've bought into plans and programs, but their customers are other distributors, not the general public. There are several "reputable" companies that work this way.

9. **Travel and Vacation:** Get a luxurious trip with lots of "extras" at a bargain-basement price. Companies deliver lower-quality accommodations and services than they've advertised or no trip at all. Others impose hidden charges or additional requirements after consumers have paid.

10. **Lottery Scams:** A **lottery scam** is a type of advance-fee fraud which begins with an unexpected email notification that "You have won!" a large sum of money in a lottery. The recipient of the message — the target of the scam — is usually told to keep the notice secret, "due to a mix-up in some of the names and numbers," and to contact a "claims agent." After contacting the agent, the target of the scam will be asked to pay "processing fees" or "transfer charges" so that the winnings can be distributed; the victim will never receive any lottery payment.

Exercise

Think about the following questions and discuss them with the rest of the class:

12.11 Do you think that you could have been a victim of some of the crimes mentioned throughout the lesson?

12.12 Here is a quote from an ISECOM board member: "In order to have the proper background to evaluate the security readiness of a computer system, or even an entire organization, one must possess a fundamental understanding of security mechanisms, and know how to measure the level of assurance to be placed in those security mechanisms." Discuss what is meant by this and how you could prepare to "evaluate the security readiness of a computer system." Have these lessons given you enough materials to get started?

12.13 [optional exercise for personal consideration (not general discussion)]: After analyzing the comments in this lesson, you may find that there are technological activities that you have heard about, or that you may have even done, that you never considered to be illegal, but now you are not sure. Some research on the Internet may help clear up any questions or confusion that you have.

World Wide Laws And Penalties Related To Internet Crime

Internet Crime is becoming the biggest threat to the current world as almost any type of crime or fraud can happen with the help of the Internet and as discussed earlier in this lesson, dealing with international boundaries is the biggest challenge any country has to face while creating any law or penalty against those types of crimes. Fighting Internet Crime involves great amounts of sophisticated legal and other measures.

The Computer Fraud and Abuse Act: The Computer Fraud and Abuse Act passed in 1986 is one of the broadest statutes in the US used to combat cyber-crime. It has been amended a number of times, most recently by the US Patriot Act of 2002 and the Identity Theft Enforcement and Restitution Act of 2008. Within it is the definition of a "protected computer" used throughout the US legal system to further define computer espionage, computer trespassing, and taking of government, financial, or commerce information, trespassing in a government computer, committing fraud with a protected computer, damaging a protected computer, trafficking in passwords, threatening to damage a protected computer, conspiracy to commit a cyber-crime, and the penalties for violation. The 2002 update on the Computer Fraud and Abuse Act expands the act to include the protection of "information from any protected computer if the conduct involved an interstate or foreign communication.

Internet Spyware Prevention Act: The Internet Spyware Prevention Act (I-SPY) prohibits the implementation and use of spyware and adware. I-SPY also includes a sentence for "intentionally accessing a computer with the intent to install unwanted software.

12.7.3. CAN-SPAM Act: The CAN-SPAM Act of 2003 establishes the United States' first national standards for the sending of commercial e-mail and requires the Federal Trade Commission (FTC) to enforce its provisions

In addition to the above there are many laws around the world which cover some or all parts of internet crime. There are many statutory law enforcement bodies around the world which are working towards fighting internet crime. There are many Cyber Police Cells which are established specifically to fight cybercrime and convicting cyber criminals.

Exercise

12.14 Search for and discuss three recent internet crime cases convicted in court.

12.15 Find out in detail about at least two such laws that cover all areas of computer security and offenses.

Recommended Reading

http://www.ftc.gov/bcp/menu-internet.htm

http://www.ic3.gov/

http://www.coe.int/cybercrime

http://www.ccmostwanted.com/

http://www.scambusters.org/

http://compnetworking.about.com/od/networksecurityprivacy/l/aa071900a.htm

http://www.echelonwatch.org/

http://www.isecom.org/

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM