**Chapter 5 Summary: Crime:**

**5.1 Introduction:**

-Computers and the Internet make many activities easier for us. They also make many illegal activities easier for criminals. They provide a new environment for fraud, stock manipulation, theft, forgery, industrial espionage, and many old and new scams.

-Crimes committed with computers and on the Web are more devastating and harder to detect than similar crimes committed without computers.

-Just as the Web changes the impact of crime, it changes the impact of law.

**5.2 Hacking:**

**5.2.1: What is hacking?**

-The term *hacker* to many people, means an irresponsible, destructive criminal. Hackers break into computer systems.

-They intentionally release computer viruses. They steal sensitive personal, business, and government information. They steal money, crash Web sites, destroy files, and disrupt businesses.

**Phase one: The joy of programming:**

-In the early days of computing, a *hacker* was a creative programmer who wrote very elegant or clever programs. A “good hack” was an especially clever piece of code. Hackers were *computer virtuosos*.

**Phase two: From the 1970s to mid-1990s:**

-The word *hacking* took on its most common meaning today: breaking into computers on which the hacker does not have authorized access. By the 1980s, hacking also included spreading computer viruses, then mostly traded on FLOPPY DISKS! Hacking behavior included pranks, thefts, and *phone phreaking*.

-Hackers obtained passwords by sophisticated techniques by *social engineering*: fooling people into disclosing them.

-Programs called *sniffers*, they read information traveling over the Internet and extracted passwords.

**5.2.2 Hacktivism, or political hacking:**

-Hacktivism is the use of hacking to promote a political cause.

-Just as hacking in general ranges from mild to highly destructive activities, so can political hacking.

-Hackers posted political messages on Web pages they hacked to direct suspicion at others or to divert attention from their true motives, including theft of credit-card numbers or other data.

-Political hacking is that this kind of hacking can be hard to identify.

-In free countries where almost anyone can post his or her words and video on the Web for free, it is hard to justify hacking someone else’s site to promote a political cause.

-Some countries have oppressive governments that control the means of communications and prohibit open political discussion. In such countries, where sponsoring one’s own Web site is impossible or dangerous, there might be good arguments to justify political hacking to get one’s message out to the public. The nations in which Hacktivism is likely to have the most ethical justification are those least likely to respect the acts of civil disobedience.

**5.2.3 The Law: Catching and Punishing Hackers:**

**The Law:**

-State governments passed laws that specifically addressed computer crimes. Congress passed the main federal computer crime law, the Computer Fraud and Abuse Act (CFAA).

-Prosecutors use more than a dozen other federal laws to prosecute people for crimes related to computer and telecommunications systems.

-Access to computers by an unauthorized person is now illegal in most cases.

-Actions are crimes if done while intentionally accessing a computer without authorization or when exceeding one’s authorization.

-State and federal ant hacking laws provide for strong penalties including prison sentences and fines.

-Some hackers hack to demonstrate weaknesses and encourage fixing them.

-Law enforcement agencies now employ people who are well informed about technical aspects of hacking and the hacker culture.

-Agents and security professionals read hacker newsletters and participate in online discussions of hacking, sometimes undercover.

-Law enforcement agents, some undercover, attend hacker conferences.

-Security specialists maintain logs of chat channels used by hackers.

-Security professionals set up *honey pots*: Web sites that look attractive to hackers so that they can record and study everything a hacker does at the site.

-Law enforcement agents use wiretaps to collect evidence and build their cases against hacking suspects.

-Unsophisticated hackers are sometimes easy to trace because they do not hide.

-Computer forensics is used to collect and save information about everything we do on the Internet and to search and match records to build consumer profiles. The same tools that threaten privacy aid in catching criminals.

-Investigators trace viruses and hacking attacks by using Internet service provider (ISP) records and the logs of routers, the machines that route messages through the Internet.

**Penalties for young hackers:**

-We want young hackers to mature.

-We do not want them to turn into resentful, hardened criminals or wreck their chances of getting a good job by putting them in jail. This does not mean that we should not punish young hackers if they trespass or cause damage.

-Kids do not mature and become responsible without good direction, or if we reward irresponsibility.

-The point that we should not overreact and over punish.

-Many exploits of young hackers are more like pranks, trespass, and vandalism. They usually do not include financial gain for the hacker.

-Sentences for hacking, as for other crimes, depend on the person’s intent, the person’s age, and the damage done.

-One of the purposes of criminal penalties is to discourage people from committing crimes. But sometimes the company who gets hacked hires the hacker after catching him.

-With any criminal law, there is a trade-off between having fixed penalties and flexibility. With young people, flexibility is probably more important.

-Penalties can focus on using the hacker’s computer skills in a productive way and on paying victims for damage done.

**5.2.4 Security:**

-Hacking is a problem, so is poor security.

-Security weaknesses come from:

1. The Internet and the Web, from the inherent complexity of computer systems.
2. The speeds at which new applications develop.
3. Economic and business factors.
4. Human nature.

-Security was not a primary design concern. That made it easy for hackers to invade and disable or damage the sites.

-*Firewalls* are software or separate computers that monitor incoming communications and filter out those that are from untrusted sites or fit a profile of suspicious activity.

-Encryption and antivirus software protect systems.

-Insurance companies offer insurance for hacker attacks.

-Some software and security companies hire hackers to attack and find flaws in systems they are developing.

-Software developers are constantly finding and patching security flaws.

**Responsibility for security:**

-No matter how well designed security software and procedures are, the complexity of computer systems means that there will be unexpected security failures.

-Software companies have an ethical obligation to design and implement their products so that they do not expose users to severe security threats.

**Criminalize virus writing and hacker tools?**

-Some law enforcement personnel and security professionals propose making it a crime to write or post computer viruses and other hacking software.

-A law against writing or publishing viruses and hacking software could make security work and research more difficult.

-A federal court ruled that software is a form of speech, so a law against hacking software or virus software might conflict with the First Amendment.

**5.3 Identity Theft and Credit Card Fraud:**

**5.3.1 Stealing Identities:**

*-Identity theft* describes various crimes in which a criminal uses the identity of an unknowing innocent person in various ways for financial gain.

-The individual victim might lose a good credit rating, be prevented from borrowing money or cashing checks, be unable to get a job, or be unable to rent an apartment.

-*Phishing*: Sending millions of e-mails fishing for information to use to impersonate someone and steal money and goods. The e-mail message tells the victim to click on a link to what purports to be the Web site of a well-known bank or online company. The phony site asks for account numbers, passwords, and other identifying information. Phishing is an example of social engineering, a method used by hackers: a thief or hacker directly asks a person for sensitive information with some false pretext. The first defense against *phishing* is to be extremely wary of clicking on a link in unsolicited email, especially if the message is about account information. If you are uncertain whether the message is authentic and want to respond, you should ignore the link in the e-mail, type the company’s URL in your browser, and check your account in the usual way. The e-mail provides a telephone number to call. *Vishing* for voice phishing. *Pharming* is another technique to lure people to fake Web sites where thieves collect personal data. Corrupting a DNS is more difficult than sending a huge number of phishing e-mails, hence, it is much less common.

-Resumes contain a lot of personal information. Identity thieves collect addresses, SSNs, birth dates, work histories, and all the other details that help them convincingly adopt their identity.

-People must adapt and be more cautious. That means omitting sensitive data from a posted resume, not providing sensitive information until you have an actual interview or finding other ways to determine that the potential employer is authentic.

-Hackers and thieves hide malicious software in innocent-appearing programs, these are called *Trojan horses*. Such programs can track keystrokes.

**5.3.2 Responses to identity theft:**

**Authenticating e-mails and Web sites:**

-E-mail programs, Web browsers, search engines, and add-on software can alert users to likely fraud.

-Some mail programs let users check the actual return address.

-Some mail programs will alert the user if the actual URL that link will take you to is different from the one displayed in the text of an e-mail message.

-Fake Web sites are easy to spot because of poor grammar and generally low quality.

-Software can reasonably well determine the geographic location of a site.

-Some browsers will flag Web sites they consider safe or show alerts for sites known to collect and misuse personal information.

**Authenticating customers and preventing use of stolen numbers:**

-Financial institutions have added procedures to authenticate customers.

-Some security firms offer more sophisticated authentication software using artificial intelligence techniques.

-Geographic location tools: If the customer Is not in the country where his or her credit card was issued, or if the customer is in a country with a high fraud rate, the retailer or credit-card company can require extra identification.

**Reducing the damage of identity theft:**

-Congress made it a federal crime to knowingly use another person’s identification with the intent to commit a felony.

-A fraud alert is a flag on your credit report that tells the credit bureau to call you for confirmation when anyone tries to open a new credit account in your name.

**5.3.3 BIOMETRICS: ☺**

*-Biometrics* are biological characteristics that are unique to an individual.

-They include fingerprints, voice prints, face structure, hand geometry, eye (iris or retina) patterns, and DNA.

-DNA matching has freed numerous innocent people mistakenly convicted of such serious crimes as rape and murder.

-Along with fingerprints, DNA has been extremely effective for identifying or eliminating suspects in crimes.

-Researchers fooled fingerprint readers with cadaver fingers and fingers they made from gelatin and Play-Doh. Criminals can wear contact lenses that fool eye scanners.

-Identity theft might become easier to prevent, but much worse for a victim when it occurs.

-Some scanners flash a light at the eye and check that the pupil contracts, as a real one would. Some fingerprint-matching systems distinguish live tissue from fake fingers.

**5.4.1 Auctions:**

**Problems:**

-*Shill bidding*,that is, bidding on one’s own goods to drive up the price.

-Frist solutions was for customers to learn to be cautious.

-Users can consider the reputation of the seller or buyer by reviewing comments other users post on the site.

-User agreements prohibit shill bidding and offering illegal items for sale.

-Auction companies suspended users who break their rules.

-eBay requires a credit card number from sellers. This discourages fraud by making it easier to identify and trace a seller in case of complaints. Requiring a credit card number from bidders as well would help reduce various scams, such as hill bidding by the same person under different names.

-Some users complain, however rival sellers make false accusations.

**5.4.2 Click Fraud:**

-On the Web, an advertiser can pay per click. That is, the advertiser pays only for each click on their ad bringing someone to their Web site. People who host an ad receive a small fee for each from their site.

-Click fraud is an entirely new kind of fraud, based on these complex ways of selling advertising on the web. In one type of click fraud, a competitor repeatedly clicks on its rival’s as, using up the rival’s advertising budget. In another type, people who host ads on their sites click on the repeatedly to increase their fee.

**5.4.3 Stock Fraud:**

-Old forms of stock fraud included posing as investment experts and luring victims to invest in worthless companies with promises of quick and easy big profits.

**5.4.4 Digital Forgery:**

-Desktop publishing systems, color printers and copiers, and image scanners enable crooks to make fakes with relative ease, fake checks, currency, passports, visas, stock, and bond certificates, purchase orders, birth certificates, identification cards, and corporate stationary.

**Defenses:**

-Make copying more difficult.

-Older antifraud techniques include micro printing, the use of paper with watermarks, and many others including the use of holograms and heat-sensitive materials in bills.

-Embedded fibers in paper and special inks that glow under ultraviolet light increase the security of checks, money orders, and identification documents. Some copiers contain a chip that recognizes currency and prevents the copier from making a copy.

**5.5.1 Search and seizure of computers:**

The Fourth Amendment to the U.S. Constitution requires that search warrants be specific about what is to be searched or seized. Courts traditionally take the view that if an officer with a warrant sees evidence of another crime in plain view, the officer may seize it, and prosecutors may use it. Nut the amount of information or evidence that might be in plain view in a house or office is small compared to what is on a computer. Law enforcement agents may search with a search warrant for another reason.

**5.5.2 The Issue of Venue:**

Prosecutors file criminal charges and a trial takes place near the location of the crime.

**5.5.3 The Cybercrime Treaty:**

-The purpose of the cybercrime treaty is to foster international cooperation among law enforcement agencies of different countries in fighting copyright violations, distribution of child pornography, fraud, hacking, and other crime online. It requires countries that sign the treaty to adopt laws to implement its provisions, standardizing cybercrime laws among those countries.

-Law enforcement agencies and the Cyber Security Industry Alliance strongly supported the treaty. Civil liberties organizations, ISPs, and online businesses strongly oppose some provisions. They believe that the treaty reduces protections for privacy and civil liberties.

-A *dual-criminality* provision. It is a provision that one country’s government cannot require assistance from another unless the suspect’s activity is a crime in both countries.

**5.6.3 Libel, Speech, and Commercial Law:**

-Under defamation law, we can sue a person, business, or organization for saying something false and damaging to our reputation in print or in other media such as television or the Web. Libel is written defamation, slander is verbal.

-Even if the laws of two countries are identical the location of the trial is very important. A trial in a foreign country means high travel and legal expenses, time away from work and family, a foreign attorney and jury, unfamiliar forms and procedures, and a cultural disadvantage. But libel laws are not identical.

-The burden of proof differs in different countries.