LEB 324H:
Supplemental Study Guide to Cybercrime

Authors:
Pooja Goradia
Catherine Gaither
David Rager
Leah Trilli

Spring Semester 2003
LEB 324H: 
Supplemental Study Guide to Cybercrime

Table of Contents

Purpose of Supplemental Study Guide to Cybercrime 3
Description of UT vs. Phillips 4
Relevant Statutes 9
Relevant Cases 14
US vs. Czubinski 14
US vs. Mitnick 15
US vs. Boudreau 16
Discussion of Ethics and Liability 17
Questions and Answers 23
Resources 26

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Purpose of the Supplemental Study Guide to Cybercrime

The purpose of this study guide is to provide the student with a closer look at cybercrime, specifically nonviolent cybercrimes. This guide contains the following sections:

- University of Texas hacking incident
- Federal Law governing cybercrime—relevant statutes
- Relevant Cybercrime Cases
- Discussion of Ethics and Liability
- Questions and Answers

The University of Texas hacking incident
The guide begins with the discussion of UT vs. Phillips, a hacking incident that occurred at The University of Texas at Austin. A current student hacked into a UT database containing personal information of thousands of current and former UT students and employees. Although the outcome of the case has not yet been determined, by applying other case proceedings and legislative statutes, we will make speculations about the case outcome.

Federal Law governing cybercrime—relevant statutes
This section paraphrases 18 USC 1030, The Computer Fraud and Abuse Act. Included in this legislation are the elements of the CFAA, definitions, and ensuing penalties. The Wire Fraud Act, or 18 USC 1343 is also introduced, as many cybercrime incidents also involve the use of interstate wire communications facilities in attempting to defraud.

Relevant Cybercrime Cases
Cases involving cybercrimes such as hacking, wire fraud, and theft can provide insight into relevant precedents and possible issues that will arise in the UT case. In this section, three cases will be discussed: US vs. Czubinski, US vs. Mitnick, and US vs. Boudreau. After establishing how the courts apply the CFAA and other statutes to these three cybercrime cases, the future ruling in UT vs. Phillips can be more easily speculated.

Discussion of Ethics and Liability
Here we discuss the duties owed by computer users, employers, and employees in using computers and preventing cybercrime. Also included is a discussion of the ethics of UT's actions in securing the private information and then responding to the hacking incident.

Questions and Answers
Finally, there is a section with multiple choice and essay questions testing the student’s knowledge of statutory cybercrime law, case law involving cybercrimes, and the ethical behavior of involved parties. The answers are provided so the student can check his or her mastery of nonviolent cybercrimes.

GOOD LUCK!

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Description of UT vs. Phillips

Overview of Facts

Facts

On Sunday, March 2 at 7:20 p.m., computer systems personnel at UT Austin discovered a computer malfunction. The affected computer system was immediately shut down, and detailed analysis began.

This malfunction was the result of a deliberate query of data from this database server. The design of the system allowed a student to write a program that input millions of social security numbers, fetching the names of people whose social security numbers matched the query list. No student grade or academic records, or personal health or insurance information was disclosed. Computer logs indicate the information was obtained by computers in Austin and Houston over a five-day period.

There is no evidence that the names and social security numbers (data) have been misused or disseminated. To date there is no evidence that the stolen data has been distributed beyond the computer(s) of the perpetrator.

In accordance with public policy, The University of Texas (UT) has involved Federal law enforcement, an occurrence rare in the private sector. On the common public side, UT has notified those affected and is taking measures to implement a system (UT EID) that will not require the use of social security numbers in the future.

Christopher Andrew Phillips

On March 14, Federal prosecutors charged Christopher Andrew Phillips, a Junior Computer Science major, for breaking into a school database and stealing more than 55,000 student, faculty, and staff names and Social Security numbers in one of the nations largest data theft cases involving a university. The formal charges are: unauthorized access to a protected computer and using false identification with intent to commit a federal offense. Under these charges, if convicted, he faces as many as five years in prison and a $500,000 fine.

The University of Texas at Austin

"'We flat out messed up on this one,' said Dan Updegrove, the university's vice president for information technology, in an interview with the Austin American-Statesman. 'Shame on us for leaving the door open, and shame on them for exploiting it. Our No. 1 goal is to get those data back before they get misused.'" (United Press International).

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Technical Description of Attack

Original Setup

Firstly, a database server should be setup with a good password policy. The database server in this case has a poor password equivalent in complexity to “12345” or “monday.” This server was not protected from attacks within, as employees could guess at passwords until finding the answer. For proper security, the database server should have “detailed logging” installed, and the logs should be monitored. The UT server did not have detailed logging installed.

Secondly, any database server is best guarded from these attacks when hidden behind a firewall. In fact, UT originally setup the database server behind the firewall, providing access only to those who needed it. While this server was behind the firewall, the data was moderately protected from “Internet-Hackers.” For proper security, this firewall should be monitored continuously for unexpected requests. The UT firewall was not.

When a double layer of security is used, dubbed total security in the field of IT, it requires two separate exploits. Often times, an intrusion can be detected while the second exploit is being planned and launched. While these advanced “hacking” techniques could eventually be used to intrude and steal data, the effort involved to do so, combined with the attention attacks against a total security setup bring, would deem the setup “well-secured.” Because the original setup had a server with a weak password, the setup was only “moderately-secured,” where the main form of defense was the mere existence of the firewall.

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.

- 5 -
New Setup

When the San Antonio office needed access to the database server, The University of Texas's Information Technology staff physically moved the server from behind the firewall, giving it direct access to the Internet. The server's presence outside the firewall, combined with the weak password policy on the database server, changed the firewall's status from "moderately-protected" to "very-loosely-protected." Additionally, when the data is transmitted across the Internet to San Antonio, the data is vulnerable to packet-sniffing, a form of eavesdropping where you can obtain information traveling through a network, like the Internet.

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Phillips' Setup

Phillips used his computer to guess the password of the "very-loosely-protected" server. Password in hand, he chose approximately one million Social Security Numbers somewhat likely to match people stored in the database. Of these one million numbers, 55,000 were found in the database. After Phillips' program determined a Social Security Number was in the database, it queried the database for the name of the person matching the Social Security Number. Much like the transmission of data between Austin and San Antonio, Phillips' request-answer transmission made the data available to those he could not control, "packet-sniffers."

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Phillips’ Extended Setup

Phillips went home to Houston for the weekend and also used his home computer to query data from the database server, opening another connection for “packet-sniffers” to eavesdrop on.

Current Legal Standing

Christopher Andrew Phillips stands formally charged with unauthorized access to a protected computer and using false identification with intent to commit a federal offense. Under these charges, if convicted, he faces as many as five years in prison and a $500,000 fine.

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Relevant Statutes

The Need for Legislative Reform

A. More than 90% of all US companies have reported breaches in computer security. 74% of these reported theft of proprietary information, financial fraud, system penetration, and data or network sabotage.

B. The Computer Emergency and Response Team at Carnegie-Mellon University reports from 1991-1994, there was a 498% increase in the number of computer intrusions, and 702% rise in the number of sites affected.

C. 61% of consumers said that rising cybercrime made them less likely to conduct business over the internet.

D. Over 4.4 billion was spent in 2001 on purchases including firewalls, intrusion-detection programs, and authentication and authorization software.

E. According to the Computer Security Institute's Computer Crime and Security Survey for 2001, conducted in conjunction with the FBI's Computer Intrusion Squad, 186 responding corporations and government agencies reported total financial losses of over US $3.5 million, due primarily to the theft of proprietary information and financial fraud (see www.gosci.com/press/20020407.html).


Definition and Categorization of Cybercrime

Definition

Cybercrime is a subset of computer crime. Cybercrime is a criminal offense committed utilizing the Internet or other computer network as an element of the crime. Computers and networks can be part of the crimes in a variety of ways. The computer or network can be:

- The tool of the crime (used to commit the crime)
- The target of the crime (the "victim")
- Used for incidental purposes related to crime (i.e. for a drug dealer to keep a record of the illegal drug trafficking).


Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
**Jurisdictional Issues**

A. Usually, criminal behavior is subject to the jurisdiction in which it occurs

B. Cybercrime usually occurs in a virtual place, or cyberspace, so it is complicated to determine where the crime occurred

C. Also, laws vary from one geographical location to another, an act that is illegal in one location may be allowed in another

**Categories of Cybercrime**

A. Violent or Potentially Violent Cybercrime Categories
   - Cyberterrorism
   - Assault by threat
   - Cyberstalking
   - Child Pornography

B. Nonviolent Cybercrime Categories – The focus of this study guide
   - Cybertrespass – the criminal gains access into a computer’s or network’s resources without authorization but does not use, misuse, or damage data
     - i.e. teenage hacker breaks into computer networks “on a whim because he can” to sharpen hacking skills or even prove himself to his peers
     - Cybertrespassers enjoy probing into people’s personal emails, documents, frequently visited websites, but do not do anything with what they find
     - Crime in most jurisdictions

**Federal Law – 18 U.S.C. 1030**

The Computer Fraud and Abuse Act, codified at 18 U.S.C. 1030 criminalizes a wide range of conduct that demoralizes the confidentiality, integrity, and availability of data

*18 U.S.C. 1030 (a) (2) – Unlawful Access to Obtain Information*

A. This section is intended to defend the secrecy and confidentiality of data. It is prohibited to deliberately access a protected computer without authorization or go beyond authorized access and acquire:
   - Information contained in a financial record of a financial institution – or in a credit card issuer, from a consumer reporting agency concerning a consumer, etc.
   - Information from a department or agency that is part of the United States

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
- Information on a secure computer pertaining to the interstate or foreign communication

B. When one violates a subsection, this is classified as a misdemeanor with a punishment range up to one year and jail time and/or a $100,000 fine. NOTICE: If offense was committed for the purpose of:

- Commercial advantage
- Personal financial gain
- To build upon any criminal or tortious act in violation of the Constitution or laws of the US, or
- Value of information is greater than $5,000

C. This offense immediately becomes a felony with a penalty range of up to 5 years jail time and/or a $250,000 fine. (18 U.S.C  1030 (c) (2) (B)).

**18 U.S.C 1030 (a) (4) – Unlawful Access to Obtain Something of Value**

This law is designed to protect accessing valuable information used in excess of authorization in the realm of interstate commerce with the intent to defraud.

**Punishment:** Up to 5 years jail time and/or $250,000 fine (18 USC  1030 (c)(3) (A))

**18 U.S.C 1030 (a)(5) – Unlawful Access Causing Damage**

A. This is one of the most commonly prosecuted sections of the CFAA

B. Hint: This subsection is different because it requires *mens rea* to commit the crime[DR2]. *Mens rea* is the state of mind indicating culpability which is required by statute as an element of crime

C. This subsection states that an offense is committed if a person intentionally causes the transmission of a program, code, or information to a protected computer, deliberately causing damage

D. If damage is reckless, then penalty is up to 5 years in jail and/or $250,000 fine

E. If damage is intentional, USA Patriot Act increased punishment to a maximum of 10 years in jail and and/or a $250,000 fine

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
What are damages?

A. The USA Patriot Act clarifies that a defendant can be held liable if it is clear that the defendant intended to cause damage. Therefore, it is irrelevant whether they caused damage in excess of $5,000.

B. Definition of damages: “any impairment to the integrity or availability of data, a program, a system, or information.

C. Under 18 USC 1030 (e) (8) – The Government must prove one of the pertinent mens rea in accordance with the causation of damages and must show that damage caused was greater than $5,000.

D. “Damage” included losses that are a foreseeable consequence of the criminal action, including the cost to “re-secure” the computer (i.e. salary for repairment or IT consultant, etc.)

Odds and Ends

A. A protected computer is essentially one that accesses the Internet regardless of what kind of security measures it has on it.

B. Password trafficking is a criminal offense if there is an intent to fraud which involves interstate commerce or this is used by the US government (18 U.S.C 1030 (a) (6))

C. Extortion is criminalized through an interstate threat to extort an object of value

Wire Fraud - 18 USC 1343

Definition: Federal crime to utilize interstate wire communications facilities in attempting to defraud.

A. A person is found guilty if these elements are present:

1. The person deliberately devised a scheme to defraud, or for acquiring money or property by means of false pretenses, misrepresentations, or promises
2. The person deliberately transmitted or caused to be transmitted by wire in interstate commerce some sound for the sole reason of carrying out the scheme.

B. The Government does not have to prove that the material transmitted was fraudulent, the specific nature of the incident, or that the use of interstate wire communications facilities was intended as the sole means of committing the fraud.

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
C. Ex: US vs. Mitnick (Cal., 1999) – The defendant was charged with wire fraud for allegedly stealing e-mails and monitoring computer systems of companies without consent. For more information on this case, please see the Relevant Cases section. The brief description on wire fraud here will assist you in the application of the relevant cases to the UT vs. Phillips case.

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Relevant Cases

US vs. Czubinski (US 1st Cir. 1997) – 1030(a)4 and Wire Fraud

Facts

In 1992, Czubinski carried out numerous unauthorized searches of IRS files. He knowingly disregarded IRS rules by looking at confidential information obtained by performing computer searches that were outside of the scope of his duties as a Contact Representative, including information regarding: the tax returns of two individuals involved in the David Duke presidential campaign; the joint tax return of an assistant district attorney (who had been prosecuting Czubinski's father on an unrelated felony offense) and his wife; the tax return of Boston City Counselor Jim Kelly's Campaign Committee (Kelly had defeated Czubinski in the previous election for the Counselor seat for District 2); the tax return of a woman Czubinski had dated a few times, as well as the files of various other social acquaintances and public figures. Nothing in the record indicated that Czubinski did anything more than knowingly disregard IRS rules by observing the confidential information he accessed. No evidence suggested that Czubinski disclosed the confidential information he accessed to any third parties. On December 15, 1995, the district court denied Czubinski's motion for judgment of acquittal on all counts and on that day the jury returned a verdict finding Czubinski guilty. On appeal, Czubinski challenged the denial of his motion to dismiss the indictment.

Holding

The appellate court reversed the conviction

Rationale

The government provided no case in support of its contention that merely accessing confidential information, without doing or clearly intending to do more, is tantamount to a deprivation of IRS property under the wire fraud statute.

The fatal flaw in the government's case was that it did not show beyond a reasonable doubt that Czubinski intended to carry out a scheme to deprive the IRS of its property interest in confidential information. Had there been sufficient proof that Czubinski intended either to create dossiers for the sake of advancing personal causes or to disseminate confidential information to third parties, then his actions in searching files could arguably be said to be a step in furtherance of a scheme to deprive the IRS of its property interest in confidential information. Mere browsing of the records of people about whom one might have a particular interest, although reprehensible, is not enough to sustain a wire fraud conviction on a "deprivation of intangible property" theory or a violation of USC 1030. Curiosity on the part of an IRS officer may lead to dismissal, but curiosity alone will not sustain a finding of participation in a felonious criminal scheme to deprive the IRS of its property.
Application to Texas Case

This case set a standard for wire fraud, in that it established intent as an element of "deprivation of intangible property". This suggests that one key point in the Phillips case will be his intent to use the information. Should it be determined that he did not aim to use the information for his own personal gain or to further his own causes, the final decision might render a lesser punishment or an acquittal on this count. One key point to consider is the fact that the government has already charged Phillips with "using a means of identification with intent to commit a federal offense".

US vs. Mitnick (C.D. California, 1999) – 1030(a)5

Facts

Kevin Mitnick broke into a number of computer systems and stole proprietary software belonging to Motorola, Novell, Fujitsu, Sun Microsystems and other companies, as well as altered computer systems belonging to the University of Southern California and using these computers to store programs that he had misappropriated between 1992 and 1995. He also admitted to stealing E-mails, monitoring computer systems and impersonating employees of victim companies in his attempt to secure software that was being developed by those companies.

Outcome

Mitnick plead guilty to four counts of wire fraud, two counts of computer fraud and one count of illegally intercepting a wire communication and was sentenced to 46 months in federal prison. He was also ordered to pay restitution in the amount of $4125. Additionally, pursuant to the plea agreement with the government, Mitnick agreed that any profits he makes on films or books (which he subsequently wrote) that are based on his criminal activity will be assigned to the victims of his crimes for a period of seven years following his release from prison.

In a statement following the plea agreement, United States Attorney Mayorkas said, "Our vigorous prosecution of Kevin Mitnick sends a message to anyone else that believes that the new technological frontier can be abused for criminal purposes. We will track you down, electronically or by any other means, prosecute you and put you in prison."

Application to Texas case

Mitnick was arguably the most damaging hacker of his time, and his jail sentence was the longest ever ordered for wire fraud. While his crimes were seemingly more destructive than Phillips alleged offenses, the Mitnick case set the standard for the punishment of hackers. Additionally, Phillips was charged with unauthorized access to a protected computer, an offense with similar implications to those named in the Mitnick case. Therefore, a judge or jury might compare the two when and if he/she/they are called upon for sentencing.

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
US vs. Boudreau (Mass. 2003) – 1030 (a)2

Facts

Douglas Boudreau, 22, a former Boston College student, used specialized software to collect personal data on thousands of fellow students, staff, and faculty. After collecting the personal information, Boudreau reconfigured his own campus ID card to make purchases and illegally enter school buildings. He used the newly encoded cards at the bookstore, dining hall, and laundry rooms, stealing about $2,000 in goods and services.

Outcome

Boudreau plead guilty to interception of wire communications, unauthorized access to a computer system, larceny, identity fraud and other charges. He was sentenced to five years probation, ordered to undergo counseling, payback the school, and was subject to computer monitoring.

Application to Texas case

The details of this case are strikingly similar to the facts in the Phillips case, save for the fact that Phillips never used the information that he stole to defraud any of the victims or the University itself. Still, the similarity of the two cases, as well as the closeness in time, could suggest a similar punishment for Phillips, should he plead or be found guilty.
Discussion of Ethics and Liability

Ethics of Computer Users

The costs of hacking corporate victims endure are easy to distinguish. Hacking increases costs leading to higher prices for consumers, decreases efficiency, consumes times in protecting and correcting hacking incidents, creates more work for the company, and makes companies wary of hackers. If these negative implications do not deter hacking, then perhaps the court rulings and statutes established under the Computer Fraud and Abuse Act will discourage hacking.

But even these negative repercussions are insufficient in eliminating the problem. What else might ward off hacking? Besides costs to both the victim and the perpetrator, only the conscience of the hacker can prevent him from hacking. But what might his conscience say?

Cybercrimes, including hacking, are easier to qualify when they are taken from the realm of “cyberspace” and superimposed in a more tangible world. For example, hacking into a network without authorization is comparable to breaking into one’s house uninvited and taking a look around. If the trespasser then were to steal valuables from the house, this would be similar to the cybercriminal stealing important information from the penetrated system, such as private information, trade secrets, and intellectual property.

What if the hacker were to deface the website he penetrated? This is similar to defacing another’s private property. Just as stalkers are not welcome in a tangible world, they are not welcome in cyberspace. We all have a right to enjoy our privacy, and the realm in which we enjoy it is irrelevant.

Thus the ethics that apply to our everyday lives also apply in cyberspace. One should not hack into a secured system not only because of the costs and possible punishments granted when caught, but also because the act is morally wrong. It is reprehensible to invade one’s privacy, regardless of the intent to cause harm. Companies take extreme measures to protect information they view as private or important; hackers should not undermine these efforts just for fun or for their own benefit. As computer users, we all have an obligation not to cause harm, and any sort of hacking certainly inflicts harm either physically or emotionally.

Ethics of Corporations and Employers

Companies currently spend over 4 billion dollars annually in cybercrime prevention and detection mechanisms. They obviously realize the necessity of prevention resulting from a sharp rise in cybercrime in recent years. Then why are so few cases litigated in court under the Computer Fraud and Abuse Act or other cybercrime statutes?

Recent surveys indicate that only 34% of attacked companies report the incident to law enforcement officials. Far more illegal cyber activity and crime occurs to corporations than these corporations report to clients, company stockholders, business partners, and law enforcement agencies. Companies would rather handle the incident quietly and out of court than expose its technology security weakness to the public. Corporations realize that admitting this
vulnerability to the public could decimate consumer confidence and thus business sales and profits.

When a company is a victim of cybercrime, particularly intrusion and data theft, consumers and other affiliated parties expect to be informed of the incident and any impending dangers. Companies requesting information from their employees and consumers have a duty to be loyal and honest to them regarding their information. Because of this duty of loyalty, failure to protect this information invokes a second duty to be honest and to inform the consumer and employee whose information has been exposed.

**Ethics in the UT Hacking Incident**

After The University of Texas realized that its database containing the social security numbers and private information of thousands of current and former UT students and employees, law enforcement officials were immediately notified. Additionally, the University immediately released a report detailing the incident and the necessary steps being taken to remedy the situation. Potential victims whose numbers were exposed were contacted and instructed to remain vigilant of any indication that their identity had been stolen and/or abused. The actions taken by The University of Texas represent how most consumers who entrust their information to another entity expect to be informed when the integrity of that information is compromised. Below is part of the report obtained from the UT website (www.utexas.edu/datatheft):

*Initial Report -- March 5, 2003, 10:00 p.m.*

On Sunday, March 2 at 7:20 p.m., computer systems personnel at UT Austin discovered a computer malfunction. The affected computer system was immediately shut down, and detailed analysis was begun.

*What happened?*

The malfunction was assessed to be the result of a deliberate attack from the Internet. Subsequent analysis revealed that a security weakness in an administrative data reporting system was exploited by writing a program to input millions of Social Security numbers. Those SSNs that matched selected individuals in a UT database were captured, together with e-mail address, title, department name, department address, department phone number, and names/dates of employee training programs attended. It is important to note that no student grade or academic records, or personal health or insurance information was disclosed.

*Is there evidence that the stolen data have been misused or disseminated?*

UT, in conjunction with the U.S. Attorney’s Office, the U.S. Secret Service, and other law enforcement agencies, has focused its efforts since Sunday evening on identifying the perpetrator(s) of the break-in and recapturing the stolen data. To date there is no evidence that the stolen data have been distributed beyond the computer(s) of the perpetrator(s).
What is UT doing about this?
UT's highest priority has been to identify the source of the attack and to cooperate with law enforcement authorities to capture the perpetrator(s), and any associated computers and data. Our second priority will be to assess the extent of further data exposure – if any – and to establish a proactive communication program with affected individuals and the UT community.

How many individual records were exposed?
Approximately 55,200 individuals had some of the above data exposed. This group includes current and former students, current and former faculty and staff, and job applicants.

How will affected individuals be notified?
The University is currently developing a communication plan and will contact affected individuals as soon as possible. At this juncture, there is no evidence that the data have been further exposed or misused.

To send a comment or question to the UT Incident Response Team, please e-mail datatheft@its.utexas.edu (do not send your Social Security number in any e-mail message).
UT regrets this incident and commits to do whatever is required to ensure the integrity of the data of all our past and present colleagues.

Daniel A. Updegrove
Vice President for Information Technology
The University of Texas at Austin

When a company or employer requests private information from its employees, these employees expect that their information is secured and remains accessible to only those requiring access. Companies must take necessary measures to comply with employees' expectations. Further, companies should act as The University of Texas acted to alert employees whose private information is exposed due to a poorly secured system.

Ethics of Employees and Former Employees

Employees have a duty to their employers to be loyal to and not to cause harm to their employers or company. Even still, 70% of computer hacks come from a company’s employees or ex-employees. Thus the most expensive fire walls and security systems may prevent the intrusion of outsiders, but few systems can prevent the intrusion of an employee who has a legitimate password into a secured system. Further, little action can be taken to prevent this employee from allowing others to use his password to obtain unauthorized access. Below, Kevin Mitnick discusses how hackers now use social engineering to gain access to a secured system.
Social Engineering

Kevin Mitnick has arguably been identified as the most notorious hacker over the past decade. He has spent two terms in jail and is still currently on probation, which strictly limits his access to computers.

After being released from his second term, he published a book on social engineering. He also now provides consulting services and offers social engineering training to companies who demonstrate a need to prevent insider hacking. Below is a portion of Kevin Mitnick’s responses with interviewer Ian Thompson.

*Firstly, to set the record straight, are you a hacker or a cracker?*

Definitely a hacker. Crackers go into systems for financial gain or to deliberately cause damage. My motivations were those of the prankster and explorer. When I went into systems I was usually just looking around or on the search for specific software for personal use. I’ve served my time and those days are now over.

*So now you’ve published a book on social engineering. What is it and why is it so important?*

Social engineering is the side of hacking that seldom gets mentioned. It’s using people to subvert technology. You can have the best computer set-up in the world but, if someone can convince a member of staff to let them in, all that is useless. The weakest link in any security chain is always human. The skills of social engineering are used by hackers to replace genuine technical knowledge. Today’s script kiddies may not be able to code but, if they can convince instead, they don’t need to.

*Surely it can’t be as simple as just asking for a password?*

Sometimes that’s all it takes. In practice it usually takes several calls using different personae before you can get all the keys you need for access. People like to help each other and, by establishing rapport and building trust, the determined individual can get what they want. Other techniques include setting up a situation so that the mark, or target, comes to you for help. You can even use intimidation, although it’s use is very limited. If someone calls needing to get a report to your boss and verbally bullies a staff member by threatening to make them lose their job they might let something slip that could give access.

*Is it ever possible to achieve total security in business without losing custom?*

While no system is ever going to be totally secure, companies need to establish a balance between maintaining proper security and giving good customer service. You can’t shut yourself away and stay in business but, with the right tools, you can get an acceptable level of security. It’s really a process of education. Think about how much money

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
companies spend on IT hardware and software protection and compare that to the training budget for teaching staff how to deal with social engineers. It’s pounds to pennies. Teach all the staff, not just the IT department, and you’ll get a much better return on investment than by buying another firewall.

*What's the single most important rule for anyone with access to company secrets who wants to avoid being the victim of social engineering?*

To paraphrase Jefferson, the price of computer security is eternal vigilance. Always ask yourself what proof you have that the person at the other end of the phone is who they say they are. If they’re legitimate they won’t mind you checking. If they’re not, you’ve just saved your company large amounts of time and money.

Thus, even though employees may ethically have a duty to be loyal to the company, or not to cause harm to the company when leaving, the company must implement measures to enforce these duties, such as providing codes of conduct or training against social engineering. Additionally, implemented policies must be enforceable; a policy that cannot be monitored and policed is no better than having no policy at all.

**Education and Prevention**

**Systems**

There are two components to “Total Security.” Firstly, any computer on a network must have its own security measures. These include a good password policy, the latest patches for known security vulnerabilities, and detailed logging of server applications’ transactions for monitoring access. Secondly, networks should be behind a “Firewall.” Put simply, a firewall is something that separates one network from another, and only allows people with valid requests to communicate through it. The firewall should also be monitored for unauthorized network access attempts.

Neither of these alone creates “Total Security,” and even when “Total Security” is implemented, since no system is completely impenetrable, logs must be regularly examined.

**Training**

As Mitnick answered in his interview, the dollar amount that companies spend on firewalls and IT security measures compared to the budget allotted for training staff to handle social engineers is “pounds to pennies.” Few IT systems can prevent an employee from simply handing his access and password information over to another unauthorized person.

Companies have two ways to combat social engineering. The first is to set explicit rules and codes of conduct governing the use of access codes and passwords. History has proved that rules and codes are little more than words on paper. A company must therefore actively monitor and enforce the rules and persecute those who violate these rules. The expected ethical conduct of employees must be ‘built into the system’—into the environment in which they work and the

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
values that the company establishes. A company cannot expect employees to behave ethically when no measures are taken to encourage and monitor ethical conduct.

Secondly, a company can invest to train employees to detect and handle social engineering. According to Mitnick, companies currently spend far less on training programs than they do for IT systems and staff to monitor intrusions. Technology alone cannot prevent cyber attacks. Often a company’s greatest vulnerability to cyber attacks results internally. If the majority of computer hacks come from within the company, why not focus prevention techniques in that direction?

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Questions and Answers

Questions

True/False

1. True/False. The most important part of a password is that it is there. No additional policy is necessary to show proper steps have been taken to secure a server.

2. True/False. Stealing data without intent to misuse involves trespassing.

3. True/False. Law enforcement is often the first called when a company has a security problem.

4. True/False. A majority of hacking incidents come from unknown sources.

5. True/False. Under 18 USC 1030 – Unlawful access to obtain something of value has a penalty of up to 10 years in jail and/or $250,000 fine if damage is reckless.

6. True/False. Under the Wire Fraud Act, Government has to prove intent to defraud.

Short Answer

1. Name and describe two examples of non-violent cybercrime.

Essays

1. Analyze each of the charges in UT vs. Phillips and discuss their validity

2. Discuss whether UT’s protection of the data is moral. Make reference to Dan Updegrove’s “honey pot” statement.

3. What are some of the precedents set in previous cases that are relevant to the Phillips case?
Answers

True/False

1. False – It is absolutely necessary to have a strong password policy in effect. A password equivalent to “12345” can hardly be called due diligence.

2. True – Even just looking at someone else’s network involves trespass, but if there are no damages, there is no civil case, and if there is no motive, there is no criminal case.

3. False – Law enforcement is rarely called when a security breach is discovered. This is why the UT case is so important. Remember that only 3.5 million dollars in loss were reported?

4. False – Most incidents involve insiders who left the company for one reason or another.

5. False - If damage is reckless, then penalty is up to 5 years in jail and/or $250,000 fine. Penalty is 10 years if damage is intentional.

6. False - The Government does not have to prove that the material transmitted was fraudulent, the specific nature of the incident, or that the use of interstate wire communications facilities was intended as the sole means of committing the fraud under the provisions of the Wire Fraud Act.

Short Answer

1. Some examples:
   A. Embezzlement: Misappropriating money or property for your own use that has been entrusted to you by someone else.
      • Ex: An employee who uses his/her legitimate access to the company’s computerized payroll system to change the data so he is paid extra, or moves funds out of company’s accounts into his/her personal account.

   B. Unlawful Appropriation: Differs from embezzlement in that the criminal was never entrusted with valuables but gains access from outside the organization and transfers funds, modifies documents, giving him title to property he does not own.
      • Ex: UT vs. Phillips case illustrates unlawful appropriation

   C. Piracy: The unauthorized copying of copyrighted works, such as software, music, movies, arts, and books, resulting in the loss of revenue to the legitimate owner of the copyright.
      • Ex: Recording Industry of America v. Napster where Napster held to not have taken the sufficient steps to keep repeat offenders from using the site.

   D. Identity Theft: Internet is used to obtain a victim’s personal information such as Social Security and driver’s license numbers, in order to assume the person’s identity to commit criminal acts,
Ex: Individual steals credit card information through non-secure transaction over the Internet and used number for personal benefit to obtain property or money.

Essay

1. The database server was not in security terms “protected.” As 1030(a)2 defines protected, the server is protected under the law. Given that SSNs are information from a United States agency, Phillips is prosecutable under the first charge “unauthorized access to a protected computer.” However, Phillips has no motive in this crime, and the SSNs are not really property of UT, so in accordance with US v. Czubinski, the second charges might be dismissed.

The second charge of “using false identification with intent to commit a federal offense” implies Phillips was going to commit a federal offense, probably fraud with the SSNs and names he obtained. He has no such intent, and people will testify to his character. As a result, this second charge will probably be dropped.

2. Ethically, employers such as The University of Texas owe a duty of loyalty and honesty to their employers. Although Updegrove truthfully admitted, “We flat out messed up on this one,” his statement does not excuse the initial duty to 1.) protect the information in the first place, and 2.) report honestly to employees when their information in not being protected. Thus, UT should have informed employees when it first realized the information was not secure.

When accounting for Updegrove’s admittance to his mistake and the ensuing actions, UT did act ethically. Secondly, UT later fulfilled its duty to loyalty by exercising every measure possible to rectify its mistake.

The University (and prosecution) must also realize that a jury will clearly agree the recovery of data is important, but they will be reluctant to throw a junior Computer Science major just playing around with no real intent into jail.

3. US v. Czubinski established that there must be intent to use the stolen information in order to convict. Merely accessing information does not suggest guilt. US v. Mitnick was the first high-profile hacking case in 1999, and it set a precedent for punishment of virtual abuse. Mitnick was sentenced to 46 months in prison, a relatively long sentence for crimes of this nature. US v. Boudreau is the case that is most similar to the Phillips case, and could suggest an upper limit for potential punishment. Unlike Phillips, Boudreau used the information that he stole to access buildings and buy sundries on the Boston University campus. His 5 year probation and order to pay restitution could suggest a similar punishment for Phillips, given the similar circumstances.

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
Resources


Liebrock, Dr. Larry. (2003 April 14). Interviewed by David Rager.


Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
SIGNS YOUR CO-WORKER IS A COMPUTER HACKER

10. You ticked him off once and your next phone bill was $20,000.

9. He's won the Publisher's Clearing House sweepstakes three years running.

8. When asked for his phone number, he gives it in hex.

7. Seems strangely calm whenever the office LAN goes down.

6. Somehow he/she gets HBO on his PC at work.

5. Mumbled, "Oh, puh-leezz" 95 times during the movie "The Net"

4. Massive RRSP contribution made in half-cent increments.

3. Video dating profile lists "public-key encryption" among turn-ons

2. When his computer starts up, you hear, "Good Morning, Mr. President."

1. You hear him murmur, "Let's see you use that Visa card now, jerk."

Disclaimer: all of the information in this document is alleged and in no way reflects actual evidence or the outcome of the case.
"This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin colour, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like.

"My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike."

The Mentor, "The Conscience of a Hacker"