

# **Crimes Online**

by Hui Liu, December 8, 2005

JOMC 223

Professor Deb Aikat

"It shall be the responsibility of every student at The University of North Carolina at Chapel Hill to obey and support the enforcement of the Honor Code, which prohibits lying, cheating, or stealing when these actions involve academic processes or University students or academic personnel acting in an official capacity."

## **Introduction**

This report is a survey of crime online. I will present information about current and potential crimes. In addition, information is presented about the criminals themselves, legal and policing issues, as well as their societal context. Possible solutions are provided near the end of the report.

Hui Liu,

[huialyanakian@yahoo.ca](mailto:huialyanakian@yahoo.ca)

## Thesis

Is crime online a new phenomenon? Before the Internet, there was crime. Was mail fraud a new phenomenon? Before mail service existed, there was crime. Even now, there are increasing numbers and types of crimes using portable telephones. There will always be men and women who commit crimes whatever the venue. What does not seem to change is the response and preparation for these criminal activities.

I feel that public attention is diverted from the underlying reasons for crime. These may be individual differences in the criminal. They may come out of cultural differences. Naturally, most people, even poor ones with criminal parents, have free will and can make choices, but a frank look at statistics is in order. Without laying blame, one can investigate these factors which influence criminal behavior. I find that news outlets hype crimes without investigating the root causes in detail.

I once heard [a speech](#)<sup>1</sup> by former U.S. President Bill Clinton in which he said that offense always wins first before "sooner or later, hopefully sooner, decent people get together and figure out how to defend themselves". Is that so? In the case of Cybercrime, and the likely rise in mobile phone crime, there are many preemptive measures that can be tried.

So, those are my twin topics that develop into one thesis; namely, an understanding of the types of people who commit crimes, especially with technology, can help us learn to defend ourselves.

---

<sup>1</sup> President Bill Clinton, Speech,  
[http://www.georgetown.edu/admin/publicaffairs/protocol\\_events/events/clinton\\_glf110701.htm](http://www.georgetown.edu/admin/publicaffairs/protocol_events/events/clinton_glf110701.htm)  
(Nov. 7. 2001)

# Cybercrime

[Large parts of this section have been taken from my EOTO report of November 8<sup>th</sup>, 2004 (<http://www.unc.edu/~huiliu55/blog/blogger.html>).]

## **SCOPE: MONEY**

One's own money is at risk by people who break into our mail boxes and intercept our Internet communication. Moreover, even if one uses the latest encryption software, the costs of losses may be seen in higher prices for all items. It is just like shoplifting. Everyone pays for it.

According to Swartz, consumers and businesses, such as credit card providers, lost \$14 billion to online crime. That was 10 billion for spam, two billion in losses for online merchants and another two billion from individuals who were victims of [scams](#)<sup>2</sup>. Loss of confidence and future revenue are harder to gauge.

## **SCOPE: TRENDS**

One can see that the scope is very large and increasing, according to [Ferris Research](#). Online fraud is surging according to the [National Fraud Information Center](#). Swartz cites FBI statistics and examples to demonstrate the increase in online extortion.

Here is an easy-to-read table from Carnegie Mellon University cited by Scott Charney, whom Microsoft named as Chief Security Strategist. How clear is the trend?

---

<sup>2</sup> Scott Colvey, "Top 10 Internet Scams" <http://www.vnunet.com/features/1140235> (Apr 16, 2003)

<u>Year</u>	<u>Attacks</u>
<u>1988</u>	<u>6</u>
<u>1989</u>	<u>132</u>
<u>1990</u>	<u>252</u>
<u>1991</u>	<u>406</u>
<u>1992</u>	<u>773</u>
<u>1993</u>	<u>1,334</u>
<u>1994</u>	<u>2,340</u>
<u>1995</u>	<u>2,412</u>
<u>1996</u>	<u>2,573</u>
<u>1997</u>	<u>2,134</u>
<u>1998</u>	<u>3,734</u>
<u>1999</u>	<u>9,859</u>
<u>2000</u>	<u>21,756</u>

On a positive note, legislation and penalties are growing in volume and severity. For example, on October 7, 2004, the U.S. House of Congress passed a law against spyware. International cooperation (e.g., an extradition treaty) is also needed as criminals set up shop in the countries with least legislation.

### **SCOPE: POTENTIAL ISSUES**

Could a cyber-attack close a bank? Could one damage national security? [Amit Yoran](#) quit his post as the American national cyber-security chief because these [questions were not being dealt with](#)<sup>3</sup>. This follows the departures of Richard Clarke, Rand Beers, and Howard Schmidt. I guess it is not an easy job in an environment where [21%](#)<sup>4</sup> of

---

<sup>3</sup> Hannibal, "Cybersecurity Czar Bails" <http://arstechnica.com/news.ars/post/20041001-4264.html> (Oct 1, 2004)

<sup>4</sup> Scott Charney, "Cybercrime" <http://www.pwcglobal.com/extweb/newcolth.nsf/docid/1A47C7356C3D57AC85256AD1005834D1?OpenDocument> (Dec, 2001)

Fortune 500 companies do not even know if they have experienced an attack. In any case, the U.S. is not getting the leadership it deserves.

According to a Mercer Research study: "[without defenses against mobile-borne attacks, by 2005 each incident would cost \\$2 billion, with viruses infecting as much as 30 percent of the population in just three days](#)"<sup>5</sup>. Thankfully, the defenses are being developed but one can see the stakes involved. What is not speculation is that the potential harm is as great as our reliance on digital devices.

## **Cybercriminals – Two Case Studies**

Here are two cases. They illustrate that factors such as egotism, alienation and affiliation are common themes in the hackers' subculture. We need to know who the individuals and groups are before rushing to judgment (After we know who they are, THEN we can rush to judgment— wink!).

### **Kevin Mitnick's story**

Kevin Mitnick is a computer expert and criminal of renown, even in China. He is most famous for monitoring the e-mail of MCI and Digital Equipment Corporation security officials. His forte was so-called social engineering; basically, he was a good liar and made a lot of people look careless and stupid.

People gave him vital information related to computer networks. For example, he illegally entered one company and put a name card in a Rolodex file. Later he called and asked an unsuspecting IT employee for the "lost" password of the fake employee in the Rolodex file. He usually got what he wanted, but he did not become rich directly from hacking.

---

<sup>5</sup> Textually.Org, "Mobile Antivirus Engine In Development"  
<http://www.textually.org/textually/archives/001996.htm> (Oct 17, 2003)

His subsequent books traded on his notoriety and have made him well off. What Kevin Mitnick gained the most was attention, from both fans and enemies. He and his admirers built a larger-than-life persona by publicizing what he had done. Stories circulated on message boards. Mitnick did not have to blow his own horn because he had others to do so.

Mitnick has a legion of fans. There is a revealing resource at [SlashDot.Org](http://SlashDot.Org)<sup>6</sup> that has a question-and-answer session with many of them. Here is a sampling of his responses:

"I was challenged by a friend of mine to get his Sprint Foncard number. He said he would buy me dinner if I could get it. I couldn't pass up a good meal..."

"...The truth of the matter is I never was a hacker out for fame or prestige."

"...I was never accused of abusing a position of trust, profiting from any illegal activity, or intentionally destroying information or computer systems."

"Breaking into systems and networks is much easier today than it was a decade ago."

"Unfortunately, too many organizations are lulled into a false sense of security when they acquire and implement typical security technologies, such as firewalls and antivirus software. Although these technologies are essential in mitigating risk, in my personal experience, I have combined technical attacks with social engineering to compromise my targets. It's a lethal combination. No technology in the world can stop people from being manipulated and deceived. As the site <http://www.sqlsecurity.com> posts, 'there is no patch for stupidity.'"

"I'm the only person in United States history that was held without an initial bail hearing."

So, if Kevin Mitnick made people look stupid and careless they could become enemies. Other hackers became jealous. Tsutomu Shimomura was one of Mitnick's victims who later turned the tables on him. Mr. Shimomura co-wrote a book modestly entitled

---

<sup>6</sup> Roblimo, "Kevin Mitnick Answers"  
<http://interviews.slashdot.org/article.pl?sid=03/02/04/2233250&mode=nested&tid=103&tid=123&tid=172>  
(Feb 5, 2003)

[Takedown: the Pursuit and Capture of America's Most Wanted Computer Outlaw by the Man Who Did It](#)<sup>7</sup> (Hyperion, January 1996). Here is how Mitnick was described:

Kevin David Mitnick reached adolescence in suburban Los Angeles in the late 1970s, the same time the personal computer industry was exploding beyond its hobbyist roots. His parents were divorced, and in a lower-middle-class environment that lacked adventure and in which he was largely a loner and an underachiever, he was seduced by the power he could gain over the telephone network.

There are many other hackers in the world. Kevin Mitnick did cause limited monetary damages, for example, by scaring off customers of the target business. He did compromise databases, but security was then tightened up as a result of his exploits. For more details about Kevin Mitnick, consult the Literature & Resources section.

### **Brazilian Hacker culture**

According to a [BBC citation](#)<sup>8</sup> of [mi2g](#), a security firm, Brazilian hackers are the most prolific in the world. Furthermore, in 2002, the world's ten most active groups of Internet vandals and criminals were Brazilian. According to [Crime-Research.Org](#)<sup>9</sup>, Brazil is now home to 80% of the world's hackers. These numbers show Brazil is a unique environment because there are few or [no laws](#)<sup>10</sup> related to hacking.

"It would seem to be about bravado," said mi2g Chief Executive D.K. Matai. "Most of us are hackers, not crackers; good guys just doing it for the challenge, not criminals," Brazilian hacker Flávio Assunção said, making the distinction in an [IHT](#)<sup>11</sup> article. In fact, hacking activity has been attributed to [soccer reasons](#)<sup>8</sup> by Brazilians themselves!

Brazil, like Kevin Mitnick's case, lends itself to analysis and facile explanation. There must be *some* reasons for the clear differences between Brazil and its neighboring

---

<sup>7</sup> Bill Uttenweiler, Reviewer, "Takedown" [http://members.impulse.net/~sate/br\\_take.html](http://members.impulse.net/~sate/br_take.html) (2000)

<sup>8</sup> BBC, "Hackers catch World Cup fever" <http://news.bbc.co.uk/1/hi/technology/2210186.stm> (Aug 23, 2002)

<sup>9</sup> Crime-Research.Org, "Brazil is Hackers Favourite" <http://www.crime-research.org/news/15.09.2004/635/> (Sep 15, 2004)

<sup>10</sup> Capetown Times Newspaper, expired Web page, <http://www.capetimes.co.za/index.php?fArticleId=20908>

<sup>11</sup> Tony Smith, "Brazil, the new hotbed for hackers" <http://www.iht.com/articles/115291.html> (Oct 28, 2003)

countries. Of course, societal attitudes and conditions are different in every country. What is a cause and what is an effect? These are questions to ponder for both individual and societal differences and their relation to computer hacking.

## Cyberprofiling

The first line of defence is prevention. A good firewall may not be able to stop a determined hacker, but may protect a site by making it *relatively* harder to hack. Former hackers, as in Kevin Mitnick's case, are often sought out as consultants. 'It takes a thief to catch a thief' is an old English expression that fits this situation.

The police can only make sure that laws are being enforced. As seen in Brazil, the legal system lags behind what is happening in that country. So, police can only become involved *if* laws have been broken, after hacking activity has been detected.

In fact, one of the reasons a country might have a lot of hackers is a loose legal system to deal with it. It is natural that people find the path of least resistance. Hackers can move to a country with the least legislation. This draws attention to international disparities and the glaring weaknesses created by uncooperative or rogue countries.

There is a great demand for forensic specialists. Police forces must compete with computer consulting firms for the best talent. These detectives must work after the fact to determine if a crime has been committed, and only then try to solve it. Once again, cooperation amongst different government and private organizations is needed. [Here](#)<sup>12</sup> is an all-in-one resource which outlines the current state of these matters.

---

<sup>12</sup> Gabriole Zeviar-Geese, "The State of the Law on Cyberjurisdiction and Cybercrime o the Internet" <http://law.gonzaga.edu/borders/documents/cyberlaw.htm> (year unknown)

I will not detail any government or private institutions here. The main point of this section is to highlight cyberprofiling. It is a growing field that serves as a bridge between crime prevention and law enforcement.

Cyberprofiling has a long and ignominious history dating back to witch hunts. [\*The Malleus Maleficarum\*](#) ("The Witches' Hammer")<sup>13</sup> was published in 1486 as a how-to book for witch hunters. The people who used it, for example the Spanish inquisitors, all had problems with logic and the scientific method. [Cesare Lombroso](#) published *The Criminal Man* in 1876, in which a criminal anthropology was suggested as a means of identifying criminals. This was based on a person's outward physical appearance. It was just bad science based on anecdotal evidence.

Still, there are examples of reliable correlations between body shape and behavior, for example, [relative finger length and sexuality](#)<sup>14</sup>. I mention this only as a way to redeem profiling. A good text is *Criminal Profiling: an Introduction to Behavioral Evidence Analysis* by Brent Turvey (ISBN: 0127050418). [Forensic Psychology - the Future of Criminal Profiling](#) is another pertinent text which explains the application of psychology and statistical analyses to criminal investigations. It is the way forward.

## **Analysis & Conclusion**

First of all, I do not want to analyze Kevin Mitnick! He has been analyzed enough by others and in a better way.

I would like to return to President Clinton's speech. Basically, he said that first there is trouble, and then there is a solution or defence to that trouble. Respectfully, I do not agree. I see the advances in the profiling discipline helping prevent trouble in the first place. This is the direction we can move as the social sciences are becoming more empirical.

---

<sup>13</sup> Heinrich Kramer and James Sprenger, editors, "The Malleus Maleficarum" <http://www.malleusmaleficarum.org/> (1928)

<sup>14</sup> BBC, "A finger on sexuality" <http://news.bbc.co.uk/1/hi/sci/tech/695142.stm> (Mar 29, 2000)

In a broad sense, I see increased social justice and economic parity lessening tensions worldwide. When the world stops seeing an 'us' and a 'them', one benefit will be less crime in general. This seems like a pie-in-the-sky statement. OK. It is still true.

On a more negative note, I see a continuation of an oversimplification of crimes online. 'Cybercrime', 'cyberprofiling', 'cyber-this' and 'cyber-that' are examples of a nomenclature that is part of the problem. There is little new in young people acting out. There is little new in people cheating to get ahead. Crime is crime. The new vocabulary engenders a hype which is a distraction to reality. [Yes, I used these words for their attention value but, while I still have your attention, am quick to add that they add little and may very well make the situation worse.]

So Kevin Mitnick was caught. Did he have accomplices? He was never asked! Since the arch-cybercriminal was caught why should the public care if there are thousands more every bit as capable? He was demonized and, as if to show how tough they were on crime, officials threw the book at Kevin Mitnick in a frightening, fascistic way. I do not feel safer. World standards are needed but, as in the Kyoto Accord, hard to achieve without will.

Brazilian hackers? I think it is better just to say 'hackers' because any node on the Internet can reach any other node. To vilify Brazil is to give some malicious person in Montevideo more freedom. On the other hand, one's society must be considered. The sociological and psychological make-up of people is what profiling is all about. Understanding these topics is the first step to using the knowledge.

Not only do we need prevention and penalties, but rehabilitation. There is an addictive aspect to hacking. Any intervention ought to take into account the heavy emotional attachments involved in attention-seeking and affiliation.

The story of Kevin Mitnick may show this, despite his claim that he did not care for fame, yet he did hacking just to win a bet. There is also a mob-rule aspect to hacking.

If activities in Brazil show anything, they confirm an all too human trait to seek affiliation. For whatever reasons hackers initially flourished in Brazil, one must recognize the sustaining effect of wanting to fit in. Brazil has achieved a critical mass so that many people have a cousin or friend or passing acquaintance that is a hacker.

Better international cooperation, especially technical (i.e., ISP management), harmonization of laws and further research seem hard to achieve. I predict that there will either be some catastrophic effect from hacking that will shock us into these measures. Alternatively, people may become sick of government using the threat of "cyber"-terrorism to push through some narrow-minded agenda. Either way, we need to take stock and use straight talk. America is in an actuarial crisis, it seems to me. In any case, less hype will bring more hope for this issue.