Computer Crime

From: Dr. Nelson Kofi <drnelson-----kofi@att.net>
Subject: **{Spam?6} URGENT REPLY**
Date: March 6, 2011 11:03:01 AM PST (CA)
To: undisclosed recipients: ;
Reply-To: koffinelson@gmail.com

Dr.Nelson Koffi
Branch Manager
Eco Bank of Ghana
Kaneshie Branch
Accra,Ghana

Good Day,

This message might meet you in utmost surprise. However, it's just my urgent need for foreign partner that made me contact you for this transaction.

I'm Dr.Nelson Koffi,the branch manager Eco Bank of Ghana,Kaneshie branch.I'm writing to solicit your assistance in the transfer of US$10,750.000.00 (TEN MILLION SEVEN HUNDRED AND FIFTY THOUSAND UNITED STATES DOLLAR) into your account abroad.This fund is what my branch which I'm the manager made as there operational profit in the year 2009 and my Head Office is not aware of it and can never be aware of it because i have already submitted an end of year financial

Topics

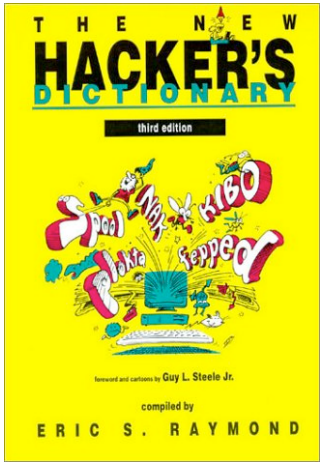
- Hacking
- Online scams
- Fraud, embezzlement, sabotage, information theft, and forgery
- Crime fighting vs. Privacy and Civil Liberties

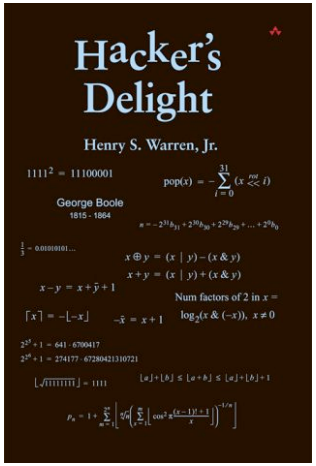
Challenges wrt Computer Crime

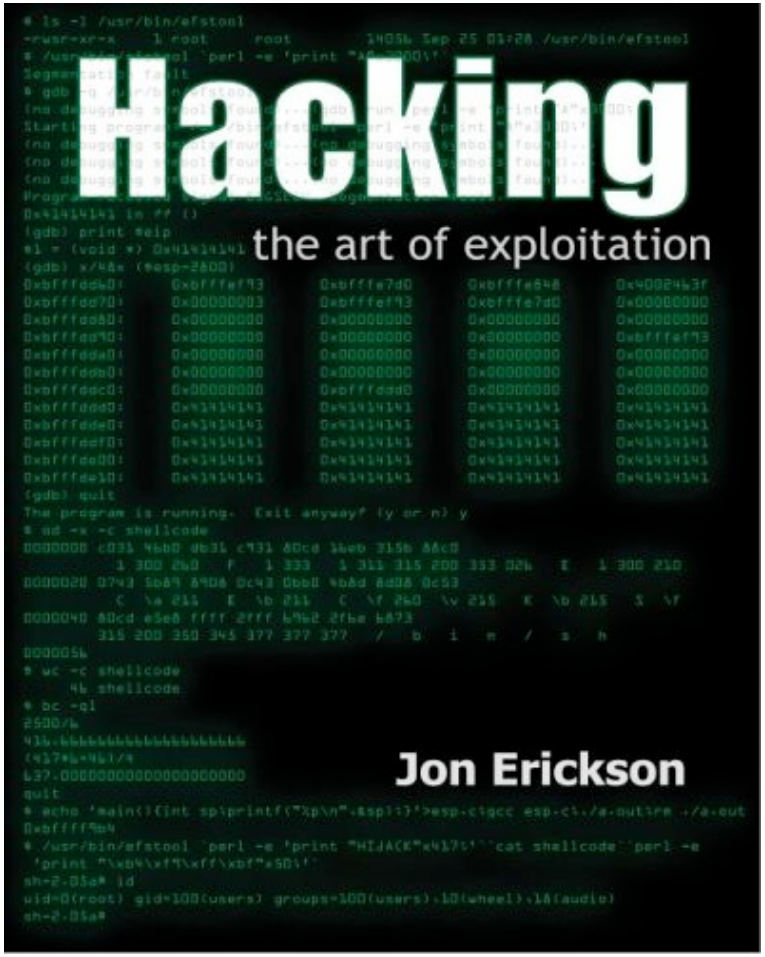
- There are at least three:
  - Prevention
  - Detection
  - Prosecution

Q: What kinds of computer crime have you or someone you know experienced?

Hacking: Decline of a great term







Defining "Hacking": Phase one

- 1960s and 1970s
- Originally term referred to a creative programmer who wrote clever code.
- First OSes and computer games were written by such hackers.
- Was a positive term (even a compliment)
- Hackers were usually – but not always – high-school and college students.

- E.g. MIT Tech Model Railroad Club (1960s)
- “a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure taken in mere involvement”

http://www.campusactivism.org/html-resource/hackers/section4.html

Q: Describe a modern-day version of “clever” hacks.

Defining "Hacking": Phase two

- Negative overtones appear in 1970s-90s
- Popular authors and media caused this use of term:
  - Described someone who used computers without authorization.
  - Sometimes to commit crimes.
- Early computer crimes were launched against business and government computers.
- Adult criminals began using computers
  - "White collar" crime
  - Organized crime increasingly responsible for computer break-ins

Defining “Hacking”: phase three

- Web era (mid 90s)
  - Increased use of Internet by average people
  - Attractive to criminals with basic computer skills.
- Crimes included the release of malicious code
- Unprotected computers are especially vulnerable
  - Unsuspecting users may have their computers utilized to take part in a DDoS or fraud
- Minimal computer skills needed to create havoc
  - “Script kiddies”
  - Attackers who use tools / code written by others
- 2008 -- 93% of breaches reported by Verizon Business were at financial institutions

Hacktivism

- Use of hacking to promote a political cause.
- Degree can range from mild to destructive
  - Defacing websites
  - Destroying data
  - Denial of service
- Some think hacktivism is modern civil disobedience
- Many do not think so:
  - Denies others their own freedom of speech.
  - Violates property rights.
  - Even some hacktivists reject web-site defacing as legitimate activity.
- An advocacy site: http://www.hacktivist.net/

Q: Do you think hactivism is ethical?

The Law (US)

- Computer Fraud and Abuse Act (CFAA)
  - First passed in 1986
    - Made it a crime to access, alter, damage, or destroy information on a computer without authorization
  - Amended in 1996:
    - Punishes anyone who "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer."
- Computers protected under this legislation:
  - Federal government computers
  - Financial systems (i.e., those under federal regulation)
  - Medical systems
  - Interstate commerce
  - Any computer on the Internet

The Law (US)

- USA Patriot Act (USAPA, 2001)
  - Amended the CFAA
  - Allows for recovery of losses due to:
    - responding to a hacker attack
    - assessing damages
    - restoring systems
  - Higher penalties may now be levied if hacking is into criminal justice system or military computers
  - The US government can monitor online activity of its citizens without a court order.
- Provisions of the Patriot Act are still very controversial

The Law (Canada)

- Existing law has been used and amended to deal with criminal misuse of IT
  - General philosophy – it doesn't matter whether a computer was used to commit a crime, the crime is still the same
- Computer Sabotage - Destruction of hardware, erasure or alteration of data, logic bombs
  - Defined as "mischief".
  - Offence covered by Criminal Code 430(1)
  - If mischief more serious, 430(5.1) deals with acts that may cause actual danger to life.
- Note:
  - Before 1985 the Criminal Code's treatment of "mischief" did not include effect on data.

The Law (Canada)

- "Colour of right"
  - You believed what you did is lawful… possibly based on ignorance or mistake of fact.
  - Also includes ignorance of any matter of law than the actual Criminal Code sections under which one is charged.
- Contrast: "Mens rea" – Latin for "Guilty mind"
  - Notion of "criminal intent" or "moral turptitude"
- Law is quite clear that:
  - No person can be convicted of mischief if he or she "acted with legal justification… excuse or… colour of right".
- Such distinctions will be helpful when thinking about other questions.

The Law (Canada)

- Creating and disseminating computer viruses.
  - No law prohibiting the creation or dissemination of computer viruses.
  - An offence occurs when viruses are used to cause mischief to data under 430(1.1).
  - Distribution of a virus might constitute an offence under 430(5.1)
  - This is so even if the virus has yet to be activated!
- Q: Should the law go further in its treatment of viruses?
  - Huge number of policy issues.
  - Malware in general (i.e., what is a “virus”?)
  - Must tread carefully.

The Law (Canada)

- Computer fraud and other economic crimes.
  - Misuse of credit or bank cards
  - Breach of trust or abuse of confidence
  - Forgery and related offences.
- Canadian Courts:
  - Have held that anything that can be considered property can be the object of theft or fraud.
  - This includes credit in a bank account.
- Section 321
  - States that forgery offences also apply to computer documents.
- “Fraud” need not require a form of relationship between fraudster and victim

The Law (Canada)

- Unauthorized entry into or use of computers
- There exists much debate on whether hacking into a system, with an intent just to browse, should be a criminal offence.
- Problems of definition:
  - Breaking and entering?
    - Criminal code: Entry occurs, in part, as soon as “any part of his body or any part of an instrument that he uses is within any thing that is being entered.”
    - These terms do not apply to computer systems.
  - Violations of Privacy? Stealing time?
    - How is this quantified?
    - Theft of electricity!!?

The Law (Canada)

- Unauthorized entry (contd)
- Some established offences apply:
  - Fraud (section 380): Where a personal falsely represents themselves as having the authority to access an account.
  - Personation (section 403): Where a person falsely assumes the identity of a lawful user.
  - Dishonest acquisition of computer services (Paragraph 342.1(1)): If services are acquired fraudulently and without a colour of right, directly or indirectly, then a crime is committed.
- Criminal liability should not be attached to persons who are:
  - acting innocently and
  - honestly believe they have authority to use a computer.

The Law (Canada)

- Trafficking in passwords, digital signatures, encryption keys
  - Some criminals have used websites and BBSes to store this kind of information.
  - RCMP in the past has identified BBSes with complete password and account information, accessible to criminals.
  - Forums promoting this information exchange are often clearly oriented to criminals.
- At present, no law specifically prohibiting online distribution or trafficking in
  - computer accounts, passwords
  - credit card information

The Law (Canada)

- Possession of computer hacking tools
  - No law in Canada prohibits the use, possession or distribution of hacking programs.
- However:
  - If a program is primarily used to obtain unlawful access to a telecommunication facility or service…
  - … then Section 327 prohibits the manufacture, possession, sale or distribution of such software.
- Note: “Telecommunication facilities” are distinct from “computer systems”.

Q: Should this law apply to computer systems?

Definitions

- Definitions of what is Cyber-crime often vary – makes comparison of stats difficult
- In Canada:
  - "Computer crime"
    - if it falls under Section 430 or 342.1 of Canadian Criminal Code (computer or data is object of the crime)
  - Others are "Computer-assisted crime"

Back to Hackers: catching them

- Onerous requirement:
  - Law enforcement must recognize and respond to many different kinds of hacking attacks
- Computer Forensic tools:
  - Undercover agents
  - Honeypots (analogous to bait cars)
  - Archives on online-message boards
  - Tools for recovering deleted or coded information
- Computer Forensics agencies and services:
  - Computer Emergency Response Team (CERT)
  - US National Infrastructure Protection Centre (NIPC)
  - RCMP IT Security Branch (http://www.rcmp-grc.gc.ca/tsb/)

What punishment is appropriate?

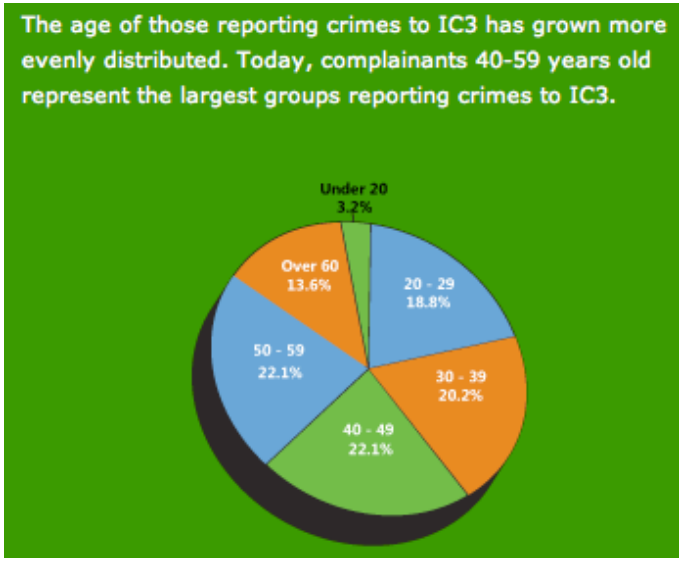
- A 17-year old hacked the LAPD's anti-drug Web page and put pro-drug slogans and images on the site.
- A 30 year-old caused a major denial of service attack, such as the one in 2000.
- A 16-year-old boy broke into 12 Defense Department computers. He did not destroy any files. It appeared he looked around at various directories, then exited.
- A 16-year-old boy hacked into computers that controlled communications for a local airport, rendering the system unusable for six hours. The airport used a backup radio system; flights were delayed but there were no mishaps.

Penalties: Questions

- Intent:
  - Should hackers who did not intend damage or harm be punished differently than those with criminal intentions?
- Age:
  - Should underage hackers receive a different penalty than adult hackers?
- Damage done
  - Should the penalty correspond to the actual damage done or the potential for damage?

How Severe is the Problem?

- US 2010 Stats, reported by IC3:
  - 303,809 complaints (2nd highest # in 10 years)
  - 121,710 referred to law enforcement



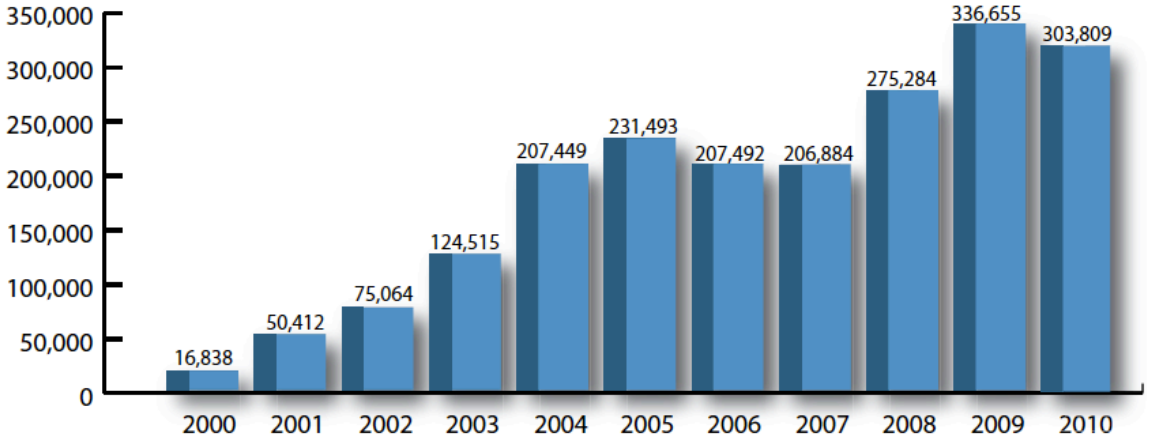
http://ic3report.nw3c.org/national_report.cfm#

Top 5 categories:

Type	Percent
1. Non-delivery Payment/Merchandise	21.1%
2. Identity Theft	16.6%
3. Auction Fraud	10.1%
4. Credit Card Fraud	9.3%
5. Miscellaneous Fraud	7.7%

How Severe is the problem?

- Increase in complaints to I3C over time



- Auction fraud decreasing (71% in 2004, 10% in 2010) -- crimes are diversifying
- Age of those reporting crimes diversifying
  - More and more complaints from older groups

Security weaknesses

- Many hackers say that “searching for weaknesses” is their motivation.
- Causes of security weakness:
  - characteristics of the Internet and the Web
  - human nature
  - inherent complexity of computer systems
  - poorly-understood tradeoffs (security vs. cost)

Improving security

- How to accomplish this?
  - Awareness, awareness, awareness!
  - Ongoing education and training to recognize the risks.
  - Better (i.e., clearer, simpler, more verifiable) system design.
  - Use of security tools and systems.
  - Challenging “others” to find flaws in systems.
  - Writing and enforcing laws that don’t stymie research and advancement

Online Scams: Auctions

- Selling and buying goods has become popular.
- Problems:
  - Sellers do not send goods
  - Sellers send inferior goods
  - Price is driven up by shill bidding (bidding on your own goods)
  - Illegal goods sold.
- Solutions:
  - Educate customers
  - Use an auction system with seller “reviews” (e.g. eBay)
  - Use third-party escrow (holds payment until buyer receives goods)

Tech / Science
Science
Space News
Tech News/Reviews
Security
Wireless
Innovation
Games

News Video
U.S. News
World News
Business
Sports
Entertainment
Health
Tech / Science
Weather
Travel
Blogs Etc.
Local News
Newsweek
Multimedia
Most Popular
NBC NEWS
MSNBC TV

Auction scam hits plasma TV buyers

Con artists insist on Western Union payment, with a twist

By Bob Sullivan
Technology correspondent
MSNBC

June 27, 2002 - A collection of Web auction scam artists are ripping off plasma TV buyers, stealing thousands of dollars per victim, MSNBC.com has learned. The scam works thanks to a bit of wire transfer chicanery. Victims agree to make payment with Western Union, but are instructed to follow procedures that supposedly make the funds untouchable until the TV is delivered — the instructions, of course, are a sham. According the one auction fraud expert, thousands of eBay and uBid users may have already fallen for it.

Apparently, scammers now know many consumers have misgivings about sending money to strangers over wire transfers. So they have come up with a fast-talking method to reassure the skeptical and overcome resistance to using Western Union.

MSN TECH & GADGETS

Working wirelessly: What you need to know

Related Links
- R.I.P. for your VCR
- Origami: Ultra-mobile PC introduced
- Geekcorps: A Peace Corps for techies

MOST POPULAR

Most Viewed • Top Rated • Most E-mailed

- Child porn ring busted, 27 face charges
- Bush to reaffirm U.S. anti-terrorism strategy
- Jessica Simpson snubs President Bush
- Bush ratings continue to drop to new lows
- Forget about it, Melissa
- **Most viewed on MSNBC.com**

RSS FEEDS ON MSNBC.COM

Fraud: Examples

- Credit Card
  - Stolen receipts, mailed notices, and cards
  - Interception or weak e-commerce security
- ATM – stolen cards, fake ATMs
- Click Fraud – clicking ads to increase cost to advertiser
  - Competitors
  - Site hosting the ad
- Stock Fraud
  - Hoax rumors
  - Encouraging others to buy so you can sell
  - Hacking to purchase stock for others -> increases price

Embezzlement & Sabotage

- Some causes:
  - Insider information
  - Poor security
  - Complex financial transactions
  - Anonymity of computer users
  - Faulty culture
- Some defenses
  - Rotate employee responsibility
  - Require use of employee ID and password
  - Implement audit trails
  - Careful screening and background checks of employees

Identity Theft

- Some causes of Identity Theft
  - Insecure and inappropriate use of Social Security, Social Insurance numbers
  - Careless handling of personally identifiable information.
  - Weak security of stored records.
  - Insufficient assistance to identity theft victims (or its equivalent: insufficient funding of law-enforcement devoted to identity theft)
- Some defenses for Identity Theft
  - Limit use of personally identifiable information
  - Increase security of information stored by businesses and government agencies.
  - Improve methods to accurately identify a person.
  - Educate consumers.
  - Check credit-report on a regular basis.

Forgery

- Some causes:
  - Powerful computers and digital manipulation software.
  - High-quality printers, copiers and scanners.
- Some defenses:
  - Education consumers and employees.
  - Use anti-counterfeiting techniques during production.
  - Use counterfeit detection methods.
  - Create legal and procedural incentives to improve security.

Crime Fighting vs. Civil Liberties

- There is often tension between them
- Q: Can you think of some examples?

Crime Fighting vs. Civil Liberties

- Scams:
  - Crime Fighting approach → Automated surveillance software to look for suspicious Web activity
  - Privacy and Civil Liberties → No search warrant without proof of probable cause
- Biometrics
  - Crime Fighting approach → Exact match of biological characteristics to a unique person.
  - Privacy and Civil Liberties → Easy to build complete dossier on people.

Crime Fighting vs. Civil Liberties

- Search and Seizure of Computers:
  - Crime Fighting approach → Needs to obtain evidence of a crime.
  - Privacy and Civil Liberties → Day-to-day business ceases; non-criminal contact with others ends
- The Cybercrime Treaty
  - Canada, US, and Europe are signatories
  - Crime Fighting approach → These countries agree to cooperate with each other's investigations.
  - Privacy and Civil Liberties → Possible privacy invasion for countries with less restrictive laws.

Whose Laws Rule the Web?

When Digital Actions Cross Borders:

- Laws vary from country to country
- Corporations that do business in multiple countries must comply with the laws of all the countries involved
- Someone whose actions are legal in their own country may face prosecution in another country where their actions are illegal

Whose Laws Rule the Web?

Arresting Foreign Visitors:

- A Russian citizen was arrested for violating the DMCA when he visited the U.S. to present a paper at a conference; his software was not illegal in Russia
- An executive of a British online gambling site was arrested as he transferred planes in Dallas (online sports betting is not illegal in Britain)

Whose Laws Rule the Web?

- Q: What suggestions do you have for resolving the issues created by differences in laws between different countries?