



# Financial Crimes

## July 27, 2006

Terry Gudaitis, PhD

## Discussion Topics

- Aspects of financial crimes – electronic
- Vulnerabilities
- Trends
- Tips and Recommendations



# What is Vulnerable?

## **US IT infrastructure not adequately prepared for cyber attacks - IEEE-USA**

Washington (14 July 2006) -- Because our nation's information technology infrastructure is highly vulnerable to hackers, terrorists, organized crime syndicates and natural disasters, increased funding for cyber security research and development is needed, according to a recent position adopted by IEEE-USA.

"Because of society's complete reliance on information technology and cyber networks, all the critical infrastructures and networks are interdependent and interconnected," IEEE-USA stated. "A cyber attack on one sector's infrastructure may have devastating consequences to another sector. U.S. infrastructure is not adequately prepared to defend against such risks."

Nearly every aspect of life in the United States is tied to computers. Air traffic control systems, power grids, financial systems, public health records and military and intelligence cyber networks, among others, all depend on computer networks. According to IEEE-USA, core Internet protocols such as Internet routing, e-mail and end-user authentication are at risk of cyber attack.

Sources - [http://www.eurekalert.org/pub\\_releases/2006-07/i-iii071406.php](http://www.eurekalert.org/pub_releases/2006-07/i-iii071406.php) and <http://www.ieeeusa.org/policy/positions/cybersecurity.asp>

## Recent Crimes and Trends

- Home Targets
- Viruses
- Outsourcing
- Hardware and Devices
- Phishing, ID Theft, and 419
- Internet Disclosure
- Event Based Scams



# Home Machines

## Shifting Target to Home Machines

Source:

<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2006/07/14/BUGGQJUNMB1.DTL&type=business>

*San Francisco Chronicle*

### **Computer crime not as lucrative Hackers suspected of shifting attention to home machines**

Benjamin Pimentel, Chronicle Staff Writer

Friday, July 14, 2006

Companies and organizations continue to lose money because of virus attacks and other computer network breaches, but the losses have declined due to improved security, according to a report released Thursday.

Virus attacks remain the leading cause of network security financial losses, followed by unauthorized access to networks and lost or stolen laptops, according to a survey by the Computer Security Institute together with the FBI's Computer Intrusion Squad.

# Viruses

**Financial losses? Blame viruses!**

**Friday, 14 July 2006**

**The Computer Security Institute with the participation of the San Francisco FBI's Computer Intrusion Squad today released its 2006 report citing that virus attacks are the leading cause of financial losses.**

Source: FBI/CSI Report 2006



# Theft of Hardware and Devices

- Recent Reports of Laptop Theft
- Other Devices Lost and Not Reported

Loss of:

Customer Data

Employee Data

Personal Data

Trade Secrets

IP - Private, Confidential, Sensitive Text

Graphics, Video, Slides



# Outsourcing

## Breaches, Theft, and Crime:

- **Lack of Loyalty**
- **Hiring/Vetting Issues**
- **Impact of Other Employees**
- **Customer Perception**
- **Recent Incidents**

## Sources:

[http://www.infoworld.com/article/06/01/17/73856\\_04OPrecord\\_1.htm](http://www.infoworld.com/article/06/01/17/73856_04OPrecord_1.htm)

1

<http://www.itbusinessedge.com/item/?ci=10521>

[http://www.wasteage.com/mag/waste\\_dangers\\_outsourcing/](http://www.wasteage.com/mag/waste_dangers_outsourcing/)

# Phishing, 419, and Identity Theft

## Falling Victim to Scams:

- **Receipt of Email**
- **Website – Webpage**
  - **Incorrect Domain Name**
  - **IP Address, no domain**
- **Forms**
- **Surveys**
- **No encryption**
- **“Man-in-the-Middle” Attack**
- **Blog Spam**



## Internet Disclosure

- Websites
- Blogs (static postings)
  - EX: LiveJournal
- Social Networking Sites (auto-linking and cross-linking)
  - EX: MySpace
- Chat (IRC)
- Message Boards
- Forums
- Text Messaging
- Gaming Sites

# Event-based Scams

## Perpetrators:

- **Move Fast, Timely Scams**
- **Adaptation to Current Events**
- **Ability to “move on” to another target**
- **Take advantage of panic, anxiety, and necessity**
- **Lower level of scrutiny and security in crisis**

Hurricane Katrina

Pakistan Earthquake

Indonesian Tsunami

**DONOR BEWARE!**

**RECIPIENT FRAUD!**

## 10 Recommendations

- **Use services that are compatible with knowledge**
- **Beware of the return of “junk snail mail”**
- **Protect children’s SS#’s**
- **Be aware of “no-\$ theft” identity theft**
- **Understand where customer service representatives are located**
- **Be aware of self-disclosure on the Internet and personal information on the Internet**
- **Protect/Destroy hard copies of financial, personal, and identification documentation**
- **Account for an protect devices and access to devices**
- **Be careful providing verbal information in stores, banks, over the phone**
- **Beware of ordering forms or surveys on cards or non-sealed packaging**

## Contact Information

Questions? Comments?

**Terry Gudaitis, PhD**  
**Director, Open Source Intelligence**  
**SAIC**

[gudaitist@saic.com](mailto:gudaitist@saic.com)