

The Importance of Protecting Privacy Information

2008 I.T. Summit
NMDP Headquarters
Minneapolis, Minnesota

January 18-19, 2008



Today, numerous threats jeopardize your privacy and personally identifiable information (PII)



"Police: Identity thief cashed \$30,000 in checks,"
WTVJ-TV, November 20, 2007

"Fugitive indicted on ID scam,"
By Shelley Murphy,
Boston Globe, November 3, 2007

"Mortgage office manager charged with identity theft and grand larceny,"
By Thomas J. Lueck and
Bruce Lambert,
New York Times, October 16, 2007

"The littlest victims of ID theft,"
By Michelle Singletary,
Washington Post, October 4, 2007



We are now operating in a new paradigm

COMPUTERWORLD

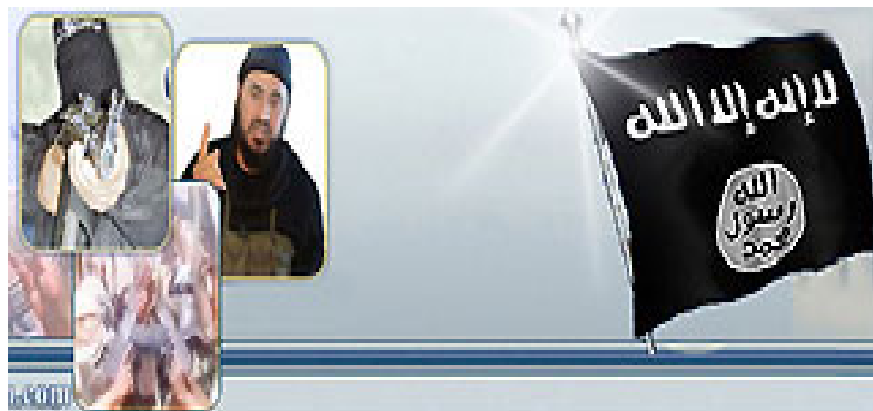
Government-sponsored cyber attacks on the rise, McAfee says

Big Brother -- *someone's* Big Brother -- is actively messing with you

November 30, 2007 ([Network World](#)) -- Governments and allied groups worldwide are using the Internet to spy and launch cyber attacks on their enemies, targeting critical systems including electricity, air traffic control, financial markets and government computer networks, according to McAfee's annual report examining global cyber security.

"Cyber assaults have become more sophisticated in their nature, designed to specifically slip under the radar of government cyber defenses," McAfee states. "Attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic and technical espionage."

We are now operating in a new paradigm



"Since the events of 9/11, terrorist presence online has multiplied tenfold," says Hsinchun Chen, director of the University of Arizona's Artificial Intelligence Lab. "Around the year 2000, there were 70 to 80 core terrorist sites online; now there are at least 7000 to 8000."

FoxNews.com Friday, October 12, 2007

سنة الفرقان للإنتاج الإعلامي
:: تقدم ::

التحيات اخوانكم



We are now operating in a new paradigm

Federal and State Governments Aim To Outlaw Spyware

Report to lawmakers: Pay more attention to cyber security

NIST to develop credentials for FISMA consultants

Government's Attempts To Legislate Infosec

Privacy: To Disclose or Not To Disclose

Encryption: Impact on Law Enforcement

The Legal Issues of Information Warfare



PII is any information that can be used to identify, contact, or locate an individual

What is PII?

Name

Social Security Number (SSN)

Date of Birth

Home Address

Phone Number

Email Address

Account Number

Driver's License Number

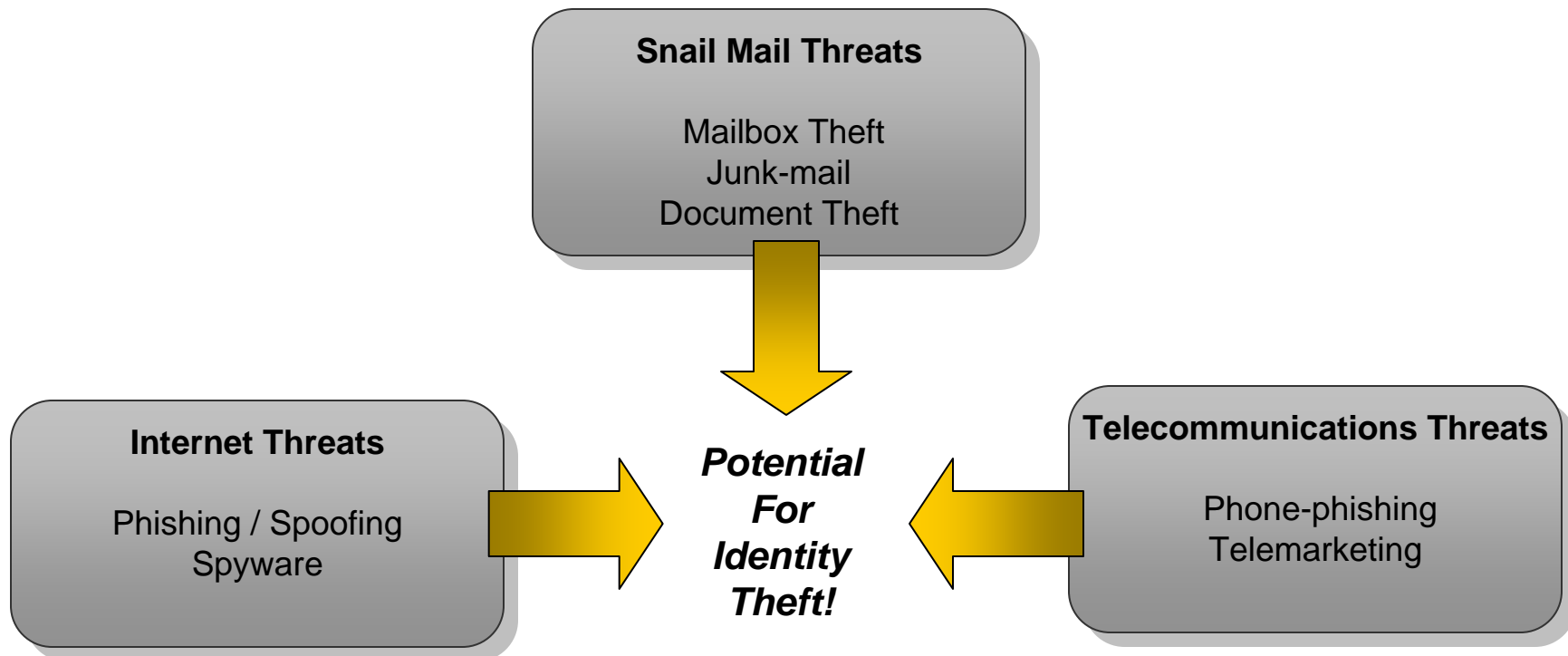
Fingerprint

Photograph

Any information associated with PII should be considered private and be properly protected!



Many emerging dangers put you at risk for identity theft





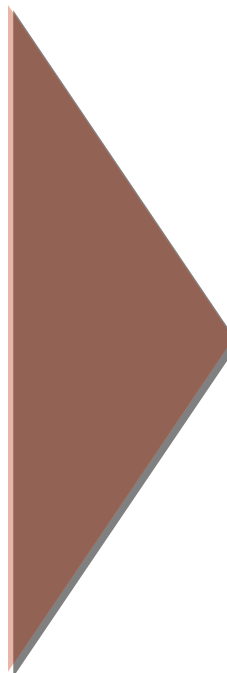
Various locations leave your personal information vulnerable to theft

Storage Location	How to Protect Your Personal Information
Trash	<ul style="list-style-type: none">• Use caution when discarding information in your waste bin; always shred sensitive information
Fax Machines	<ul style="list-style-type: none">• Double check fax numbers before dialing to ensure you have it correct; call the recipient BEFORE and AFTER the transmission for verification that it was received by the right person
Printers	<ul style="list-style-type: none">• Verify printer location PRIOR to sending a document to the printer and promptly pick up all copies of the document
Email	<ul style="list-style-type: none">• Make your default action “reply to sender” rather than “reply to all”• Double check email addresses to make sure that you have selected the correct recipient• Double check your attachment to make sure that you have selected the correct document• Confirm that sensitive data has been received properly• Use a password lock for your machine when you are away from your desk
External Storage Devices	<ul style="list-style-type: none">• Be sure to remove your storage device from public computers• Store your device in a safe place to make sure that it is not lost or stolen
Public Places	<ul style="list-style-type: none">• Do not discuss sensitive information in public places, such as restaurants, elevators, hallways, or bathrooms



There are steps you can take to protect your privacy online

- Learn how filtering and monitoring software can assist in protecting yourself
- Never offer your personal information, such as a credit card or social security number, via email or instant message
- Never provide personal information via a website, without first consulting the website's privacy policy
- Encrypt sensitive information
- Ensure proper controls are in place to limit access to systems that contain sensitive data
- Access sensitive data from secure computer only
- Remove temporary files created when using the internet



**Stay Safe
Online**



Educate your children on internet safety

- ▶ The Children's Online Privacy Protection Act (COPPA) is a United States federal law that:
 - Requires website operators that target children under the age of 13 to post a privacy policy detailing any PII that is collected
 - Restricts website operators from using children's information, unless parental consent is received

Explain to your children that they should:

NEVER give out personal information (name, address, phone, school name)

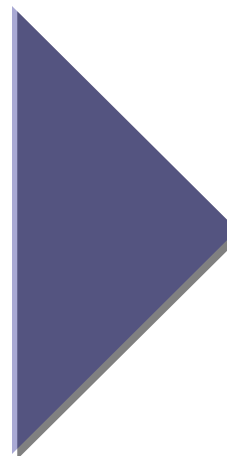
NEVER share their photo with strangers over the internet

NEVER meet anyone from online without your permission



Additionally, there are measures you can take to increase your snail mail privacy

- Drop your mail in a United States Post Office collection box, instead of your home mail box
- Shred old documents, such as mailed credit card and bank statements, before disposing of them
- Ensure that current businesses and companies, such as credit card companies, have your correct mailing address



Keep Your Personal Information Secure



Furthermore, take precautions to protect your telecommunications privacy

Protect Yourself on the Phone

- Never provide sensitive information over the telephone to someone you do not know
- Register your telephone number with the “do-not-call” registry, found on the Federal Trade Commission (FTC) website at <http://www.ftc.gov/>
- Do not answer calls that appear to be restricted or do not provide information regarding the source of the phone call



If you suspect a breach of PII in the workplace, report the incident to the proper authorities

- ▶ Issues can come about from the loss of private information; to mitigate these concerns, make sure you heed these tips when you suspect a security violation or other incident:

How to Report a Security Incident

- Report ANY unauthorized disclosure involving sensitive information to your Chief Information Security Officer (CISO)
- IMMEDIATELY report all incidents, whether suspected or confirmed
- DO NOT move, delete, or tamper with evidence
- Note any unique circumstances



HHS has taken numerable steps in response to federal privacy legislation

Office of Management and Budget (OMB) Memorandum (M)-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

HHS Response Plan:

- Review existing privacy and security requirements
- Evaluate holdings of PII
- Assess and reduce unnecessary use of SSNs
- Evaluate security requirements highlighted in OMB M-06-16, *Protection of Sensitive Agency Information*
- Implement incident management and routine use language guidance
- Develop and employ a breach notification policy to respond to PII incidents
- Create and implement a “rules and consequences” guide for failure to follow rules of behavior

HHS Policies, Memoranda, and Standards:

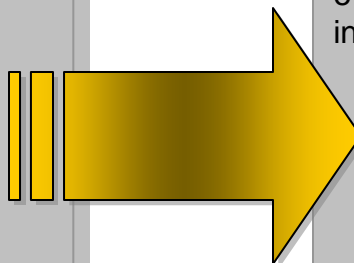
- HHS Encryption Standard for Mobile Devices and Portable Media
- Establishing an Incident Response Capability
- *HHS Incident Notification Process*
- *Information Security Program Privacy Policy*
- Privacy Impact Assessment (PIA) Guide
- Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide



In September 2006, the Department created a PII Breach Response Team (BRT)

Federal Mandate:

- In September of 2006, an OMB memorandum entitled *Recommendations for Identity Theft Related Data Breach Notification* required federal agencies to establish a BRT



HHS Response:

- The Department created a BRT composed of senior management and executive leadership representatives charged with the evaluation of information security incidents involving PII:
 - Ensures that suspected or confirmed breaches are identified, tracked, and responded to in a timely, effective, and consistent manner
 - Reviews and determines the appropriate PII data breach response course of action, including means of individual notification



Breakout Group Discussion Questions

- ▶ **How will the need for privacy/confidentiality impact future data collection and exchange methods?**
 - You will have to protect and secure it, in transit and in storage

- ▶ **How does one identify existing institution-wide strategies which could be adopted?**
 - Ask! Where you are located there should be some procedures in place.
 - Use the Internet. Network with your peers.

- ▶ **How does one share data in compliance with confidentiality/security restrictions?**
 - It must be secure
 - Encrypted in transit. New Federal Laws are going to mandate encryption for “data at rest”

- ▶ **How does one stay abreast of confidentiality/security changes?**
 - Research it!
 - Look on online at NIST.GOV; DHHS.GOV; HRSA.GOV



Topics for Breakout Group Discussion

▶ 21 CFR Part 11

- Defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records
- Challenged as excessive; FDA has stated in guidance that it will exercise enforcement discretion

▶ Health Insurance Portability and Accountability Act (HIPAA)

- Required the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers
- Established regulations for the use and disclosure of Protected Health Information (PHI)
- Established the Privacy and the Security Rules
- **Privacy - What**
 - Individually Identifiable Health Information (IIHI) defined in Part 160 becomes protected health information (PHI) in Part 164
- **Security - How**
 - Protect information from accidental or intentional disclosure and from alteration, destruction or loss



Topics for Breakout Group Discussion Continued

▶ What Does HIPAA Privacy Mean to You Personally?

- You have a right to privacy mandated through federal regulations
- You have a right to knowledge and education on privacy protections
- You have a right to more control over your health information
- You have a right to access your health information
- You have a right to know “who else” is looking at your health information

▶ Data de-identification

- Need to review reports currently used and disclosed
- If reports contain identifying information
 - Determine if report can be changed to be de-identified
 - If de-identification not possible, determine purpose of report and areas that receive report
 - Verify report recipients need all information contained on report
- Best Practice for reports distributed outside of component - de-identification
- Information that is de-identified is no longer considered to be protected health information, and is thus exempt from the other provisions of the regulation.
- Means of De-Identifying:
 - Removing
 - Coding
 - Encrypting
 - Otherwise eliminating or concealing



Topics for Breakout Group Discussion Continued

▶ Auditing of transactions

- A solid HIPAA compliance strategy for transactions and code sets should encompass:
 - *Transaction formats*--support for XML, X12, HL7 variants and version support
 - *Integration*--efficient integration to legacy applications with decreased data latency
 - *Security*--support for secure messaging of Internet-based transactions
 - *Business process automation*--reengineering the business workflow
 - *Monitoring and auditing*--services that monitor the platform operation and audit disclosures of information
 - *Professional services*--assisting the healthcare organization in developing assessment plans and then designing and implementing appropriate solutions

▶ Application/database documentation

- Certify and Accredite the system
 - SSP
 - Risk Assessment
 - Contingency Plans
 - Standard Operating Procedures
 - System Test and Evaluation
 - Network Architecture
 - Change Control
 - Best Security Practices



Further privacy resources and helpful links are available online

▶ General Privacy Links

- <http://www.privacyrights.org/netprivacy.htm>
- <http://www.perfectlyprivate.com/>

▶ Children's Privacy Protection

- <http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>
- <http://www.cybersavvy.org/>

▶ Opt-Out Services

- http://www.networkadvertising.org/consumer/opt_out.asp
- <http://www.the-dma.org/privacy/>

▶ Financial Privacy

- <http://www.consumersunion.org/finance/i-privacy.htm>
- <http://www.naag.org/features/safeguard.cfm>