Avoid Identity Theft

UH Information Security Team (InfoSec)
Who Are We?

• UH Information Security Team
  – Jodi Ito - Information Security Officer
  – Deanna Pasternak & Taylor Summers Information Security Specialists

INFOSEC@HAWAII.EDU
What Do We Do?

• Support the system-wide information security program
  – Provide oversight of IT security issues and concerns
  – Ensure compliance with policies
  – Perform security audits and risk assessments
  – Initiate and monitor the protection of sensitive information
  – Review and revise Security Policies
  – Implement mandatory Information Security Training
  – Support the automatic monitoring of network and technology resources
National Cyber Security Awareness Month (NCSAM) History

• Started in 2004

• Sponsored by the National Cyber Security Division (NCSD) within the Department of Homeland Security and the National Cyber Security Alliance (NCSA)
Cyber Security Awareness Month

• The National Cyber Security Alliance (NCSA) Initiated Cyber Security Month To:
  – Raise awareness about cyber security and online safety precautions
  – Protect our national digital infrastructure
  – Help prevent fraud and identity theft
Examples of Cyber Attacks

- **Flame** – Kaspersky dubbed it the most powerful computer virus in history. Primary target was Iran. Has the ability to steal audio, screen capture, transmit visual data, data behind input boxes (passwords), scan local Bluetooth devices.

- **Stuxnet** – A computer worm that destroyed centrifuges at the heart of Iran’s nuclear program.

- **Slammer/Sapphire** – Worm infected 200,000+ Microsoft SQL servers worldwide with a denial of service attack. Infected 75,000 in the first 10 minutes and disrupting Internet services and some business processes.
STOP | THINK | CONNECT

October

National Cyber Security Awareness Month

staysafeonline.org
Be Cyber Smart

• In conjunction with the STOP.THINK.CONNECT campaign

• InfoSec brings you

R U Cyber S.M.A.R.T.
UH Awareness Campaign for Cyber Security Month

• What’s in it for the UH community?
  – Prevent future breaches
  – Safeguard sensitive information
  – Educate the UH community on safe personal computing practices

Be Cyber S.M.A.R.T
R U - S.M.A.R.T.

- Identified five topics for the five weeks in October
  - Secure Information Destruction
  - Management and Storage of Sensitive Information
  - Avoid Identity Theft
  - Responsible Computing Practices
  - Think Before You Click
Secure Information Destruction Review

- Keep paper locked up until you shred it
- Shred sensitive information on paper, DVD’s
- Physically destroy media
- Securely delete both internal and external hard drives

Management and Storage of Sensitive Information Review

- Know the laws related to sensitive information
- Be aware of where sensitive information is stored – scan your computer
- Protect it – encryption, storage location
- Securely transfer it – Filedrop, SSL, SSH
- Treat passwords and secret questions as sensitive information

UH is sponsoring another 
eWaste Disposal Days in October
Check the website for days and times

Education & Government 
eWaste Disposal Days
October 25-27, 2012 
www.hawaii.edu/ewaste
What Will We Cover Today?

• What is identity theft
• Ways to minimize your risk
• Knowing the signs
• Resources available to you
• How to report and deal with identity theft if it happens to you
What is Sensitive Information?

• Information is considered sensitive if it can be used to cause an adverse effect on the organization or individual if disclosed to unauthorized individuals.

• Some examples are:
  – Social Security Numbers, Student records, Health information, Drivers license numbers, credit card numbers, dates of birth, job applicant records, etc.

• State, Federal and Regulatory requirements provide standards for protecting sensitive information.

• UH Policy E2.214 has a detailed description of Sensitive information: [http://www.hawaii.edu/apis/ep/e2/e2214.pdf](http://www.hawaii.edu/apis/ep/e2/e2214.pdf)
Know What to Protect

- A partial list of data considered sensitive as outlined in UH Policy E2.214
  
  - Student records (FERPA)
  - Health information (HIPAA)
  - Personal financial information
  - Social Security Numbers
  - Dates of birth
  - Access codes, passwords and PINs
  - Answers to "security questions"
  - Confidential salary information
Where is Data Stored?
What is Identity Theft?

- Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.
YES MA'AM, I'M CALLING FROM YOUR LOCAL UTILITY TO CONFIRM SOME INFORMATION... COULD I HAVE YOUR DATE OF BIRTH, SOCIAL SECURITY NUMBER AND ANY CREDIT CARDS OR BANK ACCOUNTS PLEASE?
According to a survey by the National Cyber Security Alliance (NCSA) and McAfee.

Nearly One in Five Americans Report Being Victimized Online

Of Those Surveyed

• 17% say they have been a victim of crime such as identity theft, data theft, bullying or auction fraud.
• 29% know someone who was a victim of crimes
• 1 in 5 Americans had contact with someone on the internet who made them feel uncomfortable through email or online stalking

Examples

40 Defendants Charged in Florida Identity Theft Tax Fraud Cases

MIAMI (OCTOBER 12, 2012)
BY MICHAEL COHN

Federal charges have been filed against 40 defendants in 20 separate cases in Florida dealing with thousands of stolen identities and millions of dollars of fraudulent identity theft tax filings.

Like what you see? Click here to sign up for Accounting Today's daily newsletter to get the latest news and behind the scenes commentary you won't find anywhere else.

A special strike force including federal prosecutors, the IRS's Criminal Investigation division, the FBI, the Secret Service, the Social Security Administration and local police departments in Miami and nearby towns in South Florida announced the crackdown Wednesday.

According to the Federal Trade Commission, Florida had the highest rate of identity theft in the United States in 2011, they noted. While identity theft in Florida ranks highest in the United States, the identity theft rate in Miami has reached near epidemic proportions. Florida's rate of 178 complaints per 100,000 residents is dwarfed by the Miami rate of 324.1 complaints per 100,000 residents. The City of Miami's per capita number of false returns based on identity theft was 46 times the national average, and its per capita SITR fraud dollar value was more than 70 times the national average. Worse still, the problem is projected to grow.
Grand jury indicts five-man identity theft ring

HONOLULU (HawaiiNewsNow) - An Oahu grand jury Tuesday indicted the alleged leader of a five-man ring on 78 counts of identity-theft-related charges, City Prosecuting Attorney Keith M. Kaneshiro said.

Investigators say Pyong Pak produced high-quality fake IDs, credit cards and checks using information gleaned by ring members through methods such as burglaries and auto thefts.

Pak’s co-conspirators were previously indicted on similar charges. The five men face 304 identity-theft-related charges.

Today’s indictment alleges the men used personal information of 145 Oahu residents to obtain $195,000 from May 1, 2010, to Oct. 27, 2010.

Randy Garcia was indicted on 102 counts and Jefferson Ganado on 41 counts. Al Alvarez, who was indicted on 25 counts, and Arnold Agtang, who was indicted on 47 counts, have agreed to plead guilty and serve 10-year sentences.

All five men are in custody.

The indictment was brought by Senior Deputy Prosecuting Attorney Christopher Van Marter, head of the white-collar crime unit in the prosecutor’s office.

Van Marter said the indictments resulted from a months-long investigation involving the Honolulu Police Department, U.S. Secret Service, U.S. Postal Service inspectors, the state Sheriff’s Office and Immigration, Customs and Enforcement.
How do thieves steal an identity?

- **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
- **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
- **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
- **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
- **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.
What do thieves do with a stolen identity?

• Credit card fraud:
  – They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
  – They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

• Phone or utilities fraud:
  – They may open a new phone or wireless account in your name, or run up charges on your existing account.
  – They may use your name to get utility services like electricity, heating, or cable TV.
What do thieves do with a stolen identity?

• Bank/finance fraud:
  – They may create counterfeit checks using your name or account number.
  – They may open a bank account in your name and write bad checks.
  – They may clone your ATM or debit card and make electronic withdrawals in your name, draining your accounts.
  – They may take out a loan in your name.

• Government documents fraud:
  – They may get a driver's license or official ID card issued in your name but with their picture.
  – They may use your name and Social Security number to get government benefits.
  – They may file a fraudulent tax return using your information.

• Other fraud:
  – They may get a job using your Social Security number.
  – They may rent a house or get medical services using your name.
  – They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.
How can you find out if your identity was stolen?

• The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis.
Finding Out The Hard Way

• You may find out when bill collection agencies contact you for overdue debts you never incurred.

• You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.

• You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.
Medical Identity Theft

• You get a bill for medical services you didn’t receive
• A debt collector contacts you about medical debt you don’t owe
• You order a copy of your credit report and see medical collection notices you don’t recognize;
• You try to make a legitimate insurance claim and your health plan says you’ve reached your limit on benefits; or
• You are denied insurance because your medical records show a condition you don’t have.

http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.shtm
How To Detect Medical Identity Theft

- Read the Explanation of Benefits (EOB) statement
- Order a copy of your credit reports
- Ask for a copy of your medical records
Reporting Identity Theft

• **File a complaint with the Federal Trade Commission** online at [https://www.ftccomplaintassistant.gov](https://www.ftccomplaintassistant.gov) or by phone at 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

• **File a report with your local police**, and send copies of the report to your health plan’s fraud department, your health care provider(s), and the three nationwide credit reporting companies. Information on how to file a police report is at [www.ftc.gov/idtheft/consumers/defend.html](http://www.ftc.gov/idtheft/consumers/defend.html).

• **For Medical Identity Theft - Exercise your right under HIPAA** to correct errors in your medical and billing records.
Reporting Identity Theft

• Contact only one of the three companies to place an alert. The one you call is required to contact the others that, in turn, place an alert on their versions of your report, too.

• TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

• Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241

• Experian: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9554, Allen, TX 75013
ID Theft and Children

- Target group because of lack of credit history and length of time before someone figures it out
- Child identity theft happens when someone uses a minor’s personal information to commit fraud. A thief may steal and use a child’s information to get a job, government benefits, medical care, utilities, car loans, or a mortgage. Avoiding, discovering, and undoing the damage resulting from the theft of a child’s identity can be a challenge.
Protecting Children’s Identity

• Keep all documents that show a child’s personal information safely locked up.

• Share your child’s Social Security number only when you know and trust the other party.

• Before you share personal information on the internet, make sure you have a secure connection.

• Use a computer with updated antivirus and firewall protection. If you use a password to sign into a website, log out of the site when you’re done on that site.
Protecting Children’s Identity

• Limit the chances that your child’s information will be stolen or misused at school. Find out who has access to your child’s personal information, and read the notices that schools are required to send explaining your rights under the Family Educational Rights and Privacy Act (FERPA). That law protects the privacy of student education records, and gives you the right to opt out of the release of directory information to third parties, including other families.
Warning Signs of Child Identity Theft

• You get calls from collection agencies, bills from credit card companies or medical providers, or offers for credit cards or bank account checks in your child’s name, even if your child has never applied for or used these services.

• Your child, or your family, is denied government benefits because benefits are being paid to another account that is using your child’s Social Security number.

• The Social Security Administration, Internal Revenue Service (IRS), or some other government agency asks you to confirm that your child is employed, even though your child has never had a job.

• After you file a tax return listing your dependent child’s name and Social Security number, you get notice from the IRS that the same information is listed on another tax return.

• Your child gets a notice from the IRS saying he or she failed to pay taxes on income, even though your child has no income.
Minimize Your Risk

• Protect your Social Security number
• Treat your trash and mail carefully
• Be on guard when using the Internet
• Select secure passwords
• Verify a source before sharing information
• Safeguard your purse and wallet
• Store information in secure locations
Services to Minimize Risk

- Fraud alerts
- Credit Freezes
- Free Credit reports
- Identity Theft Protection Products and Services for Sale
AAA Members

• Free identity theft monitoring
  – Once you enroll, your Experian credit report will be monitored daily and you'll receive email or mobile text alerts if key changes are detected. If you become a victim of identity theft, you’ll have access to fraud resolution support.
Photocopy Your Wallet

• Photocopy the front and back of the contents of your wallet and store in a safe location.
Credit Freeze?

• What is a credit freeze?
  – Restrict access to his or her credit report.
  – State laws determine who can initiate
  – Possible fee

• Can I temporarily lift my credit freeze if I need to let someone check my credit report?
  – You can grant exceptions
  – Possible fee

• What does a credit freeze not protect from?
  – Existing identity theft
  – Services that don’t require credit check

http://www.ftc.gov/bcp/edu/microsites/idtheft/credit-freeze.html
Credit Freeze vs Fraud Alert

• A fraud alert is another tool for people who’ve had their ID stolen – or who suspect it may have been stolen. With a fraud alert in place, businesses may still check your credit report.

• A credit freeze, on the other hand, will prevent potential creditors and other third parties from accessing your credit report at all, unless you lift the freeze or already have a relationship with the company.
My Responsibility?

- Using credit vs. debit cards
- Must report within 48 hours
- Responsible for $50-$100
Identity Theft Insurance

• Although identity theft insurance won't deter identity thieves, it can, in certain circumstances, minimize losses if an identity theft occurs.
• Be aware that one of the major "costs" of identity theft is the time you will spend to clear your name.
• Also be aware that many companies and law enforcement officers will only deal with you (as opposed to an insurance company representative)
• You may also consider checking out the insurer with your local Better Business Bureau, consumer protection agency and state Attorney General.
Things to Consider

• The amount of coverage the policy provides
• Whether it covers any lost wages
• The amount of the deductible
• What might be excluded
• If the policy provides a personal counselor to help you resolve problems
• Whether your existing homeowner's policy already contains some coverage
Prevention

• Verify a source before sharing information.
• Safeguard your medical and health insurance information.
• Treat your trash carefully.
Do Not Call Registry

- www.donotcall.gov
- Not only can telemarketers be annoying, but they can also put you at risk for identity theft.
- The less information that is circulating about you, the less likely you are to become a victim of identity theft.
Opt Out Prescreen

- https://www.optoutprescreen.com
- While you are signing up for the Do-Not-Call Registry, you might want to stop receiving marketing materials from the credit reporting agencies.
- By doing this, you will receive fewer preapproved credit card offers.
- Less trash to dig through
Fighting Back

• http://www.ftc.gov/bcp/idtheft/

• DETER. DETECT. DEFEND
Credit Reports

- Visit www.AnnualCreditReport.com
- Check 3 times a year instead of all at once
Safe Social Networking Practices
Safe Social Networking Practices

- Limit personal information online
- Ensure information you post does not answer security questions (dog’s name, mother’s maiden name)
- Check privacy settings to see who has access to online info
- Google yourself to see what people can piece together about you
I can't believe there are so many privacy risks involved in broadcasting my entire life on Facebook.
Hawai‘i Resources

• Identity Theft Resource Center –

• Hawai‘i Identity theft portal

• Secure your ID Day – Sponsored by the BBB
  – http://hawaii.bbb.org/secure-your-id/
UH Resources

• Tips on Protecting Yourself from Identity Theft
  – http://www.hawaii.edu/idalert/

• UH Policies for computing and protecting sensitive information
  – http://www.hawaii.edu/infosec/policies.html
UH Commitment To Protecting Against Identity Theft

- UH Financial Literacy Program
  - Currently Mānoa only

S.T.A.R.T.
Saving Towards A Rewarding Tomorrow
HTTP://MANOA.HAWAII.EDU/FINLIT
I OWN MY ONLINE PRESENCE!

By controlling my internet security and privacy settings, I can share only what I’m comfortable sharing.

www.stopthinkconnect.org
IDENTITY THEFT

Yes, it could happen to you.
How Do I Get iTunes?

• To be eligible for the weekly $15 iTunes cards drawing you must:
  – Attend or watch a rebroadcast of this presentation
  – Have a Facebook Account
  – Like our page at www.facebook.com/uhinfosec
  – Answer the Security Question of the Week for October correctly (will be posted after this session ends)
  – You will then be added to the drawing for an iTunes card
    • I will contact you directly if you are the winner for delivery

• To be entered to win the $25 gift card at the end of October, you must sign up for a session at www.hawaii.edu/training
  (no Facebook account required)
More Prizes

Register or sign in on-line ([www.hawaii.edu/training](http://www.hawaii.edu/training)) to be eligible for a drawing each week for a UH Mānoa Bookstore donated prize. Prizes will be mailed to outer island winners.
For More Information

• Visit the Cyber Security Month (NSCAM) website
  – Link to all presentations *(posted soon)*
  – Link to FTC materials
  – Posters
  – Cyber security brochure
  – Think. Stop. Connect. brochures
2012 National Cyber Security Awareness Month

October 2012 marks the ninth annual National Cyber Security Awareness Month (NSCAM) sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance (NCSA) and the Multi State Information Sharing and Analysis Center (MS-ISAC).

The purpose of NSCAM is to raise awareness to the issues facing us about cyber security not only at UH, but also in our daily lives.

Working with the NCSA theme of STOP. THINK. CONNECT, the Information Security Team at the University of Hawaii System will be recognizing NSCAM with the theme of "Are you Cyber S.M.A.R.T."

There will be five presentations, one given each week, over the month of October.

Each week you will have a chance to win an iTunes giftcard!

Attend or view a rebroadcast of a weekly presentation, then visit and Like the InfoSec Facebook page to answer that week's security question correctly and enter a drawing for a $15 iTunes card. In addition to the five weekly drawings there will be a sixth drawing at the end of October for a $25 iTunes card.

- **Week 1 - Secure Information Destruction** - Thursday October 4 10:30am - 11:30am
- **Week 2 - Management and Storage of Sensitive Information** - Monday October 8 11:30am - 12:30pm
- **Week 3 - Avoid Identity Theft** - Friday October 19 12:00pm - 1:00pm
- **Week 4 - Responsible Computing Practices** - Monday October 22 11:30am - 12:30pm
- **Week 5 - Think Before You Click** - Wednesday October 31 11:30am - 12:30pm

Presentation Resources

- Weekly Powerpoint presentations (Coming Soon)
- Order free FTC ID Theft Materials
- Download the Information Security Team Brochure [pdf](http://www.hawaii.edu/infosec/ncsam.html)
- STOP.THINK.CONNECT resources Website Tip Sheet and Mobile Tip Sheet
- Losing Your Mobile Device Tip Sheet
- Cyber Security Month Merne's New Password, Ceiling Cat, Secure Password
- Watch a presentation rebroadcast [here](http://www.hawaii.edu/infosec/ncsam.html)
Information Security at UH

Welcome to the University of Hawaii Information Security (InfoSec) home page. The Information Security site and team are here to provide guidance and assistance to the University community to keep its resources safe and secure from both cyber and physical threats. The InfoSec Team is also responsible for development and implementation of the University of Hawaii Information Security Program.

Click here to register and be entered into a drawing for an iTunes card!

October is National Cyber Security Awareness Month

Education & Government
eWaste Disposal Days
October 25-27, 2012
www.hawaii.edu/ewaste

To contact the Information Security Team, send email to: infosec@hawaii.edu

Protecting Sensitive Data

- Password Guidelines
- Security Deleting Electronic Information
- How to Securely Delete Electronic Information in Windows
- Securing Your Desktop Computer
- Anti-Spam/Phishing
- Securing Your Computer & Protecting Your Information
- Web Transaction Security
- Setting Up Windows Encryption
- Setting Up Encryption on Mac
- Exchanging File Security at UH - UH File Doc

Information Security Policies

- UH Executive Policies
  - E2.210: Use and Management of Information Technology Resources policy
  - E2.216: UH Information Security Policy [pdf]
  - E7.200: Student Conduct Code [pdf]

- UH Administrative Procedures
  - E5.710: Credit Card Program [pdf]
  - AR 711: Electronic Payments via University Websites [pdf]

- State of Hawaii Revised Statutes
  - HRS 92F: Uniform Information Practices Act (UIPA)
  - HRS 92F-1: UIPA - Thereneon
Email us at: infosec@hawaii.edu
Visit us at: www.hawaii.edu/infosec
Like us on Facebook: www.facebook.com/uhinfosec
Follow us on Twitter: www.twitter.com/ITSecurityUH