Responsible Computing Practices

UH Information Security Team
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 world wide with a denial of service attack. Infecting 75,000 in the first 10 minutes and disrupted Internet services and some business processes.
Yet Another Variant

Meet the ‘Gauss’ Virus, Stuxnet and Flame’s New Cousin

A new virus capable of spying on bank transactions and stealing sensitive data such as browser passwords, cookies and network information has been discovered infecting computers in Middle East.

Called "Gauss," the virus was designed to siphon data from several major Lebanese banks as well as users of CitiBank and PayPal, sending the stolen information back to its still-unknown creator.

http://mashable.com/2012/08/09/gauss-virus/
STOP | THINK | CONNECT

October

National Cyber Security Awareness Month

staysafeonline.org
Be Cyber Smart

- In conjunction with the **STOP.THINK.CONNECT** campaign

- UH 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

Avoiding Identity Theft Review

- What is identity theft
- Ways to minimize your risk
- Knowing the signs it has happened to you
- Resources available to you
- How to report and recover from identity theft if you are a victim

Rebroadcast available SOON at http://128.171.109.209/ncam/
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?

- Physical computer security
- Password creation and best practices
- Other safe computing practices
- Resources available to you
Why Is Responsible Computing Important?

- As a member of the University of Hawai‘i you could have access to sensitive information that must be protected from unauthorized access.
- Personal responsible computing is important to safeguard you and your families' financial and personal information.
Don’t be the weakest link. Responsible computing starts with 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
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?
Physical Security

• Use physical locks to deter theft
• Take advantage of video camera for monitoring
• Device locating services
• Report physical tampering such as open cases or new devices connected such as USB drives
• Install software that alerts when device moved
• More Information http://hawaii.edu/askus/1425
Don’t leave unsecured devices unattended even for a minute.
Physical Security Is A Problem

[UH Alert] Two offices at Bilger Hall report burglaries

Fri, Oct 19, 2012 at 1:26 PM

According to UH Manoa Campus Security, two offices at Bilger Hall were burglarized and computers were taken during the evening of October 18, 2012.

The discovery that door locks were pried open to gain entry at the Bilger offices was learned at 1 a.m. this morning during a regular Campus Security patrol. Office occupants were interviewed. The Honolulu Police Department is assisting with the investigation.

If you have any information about the suspects or these crimes, call Campus Security at 956-6911 or HPD at 911.

Please take precautions to install tracking programs and to identify your computer equipment. Password-protect your computer access and back up sensitive files for added safety.
Passwords

- Keep account information private
- Don't give your password to anyone
- Avoid writing passwords
- Use different passwords for each online service
- Change passwords often
How To Create A Password for your UH Account

Password requirements:
As you type in your new password, the red X (❌) will change to a green check mark (✅) once that password requirement is fulfilled.

- Must be 8-32 characters long
- Have at least one upper case character
- Have at least one lower case character
- Have at least one numeric character
- Have at least one special character.
  - Note: ( ), " , <, > and : are not allowed
- New password correctly entered twice
- New password cannot be the same as the old password

If you use a regular word, your new password will be rejected.

Re-enter New Password:
Tips For Password Creation

• Choose a password that is hard to guess. Do not use words from a dictionary, birth dates, or names.

• A good way to build a password is to use the first letter of each word in a phrase that you would easily remember, using numbers and symbols if possible. Add something unique to the end for each account.
Example Using Song Lyrics

- Beatles, Hey Jude
- “Take a sad song and make it better”
  Tassamib
- Change letters to numbers and symbol
  T@$@$@m1b
- Add something unique that you can remember for each account
  T@$@$@m1b_uh
  T@$@$@m1b_boh
I MAKE MY PASSWORDS LONG AND STRONG!

Protecting my employer, my colleagues, my customers and myself is my responsibility.

www.stopthinkconnect.org
Don’t use easily guessable answers for security questions. Example: If your dog’s name or city of birth is on Facebook do not use that as a security question.

You don’t have to use the real answers to questions. Consider using random words.

- Example “What’s your mother’s maiden name”
- Answer “orange”

If you do this, make sure to develop an easily to remember scheme that you will not forget.
Password hint: Mr.Duck

Actual Password: Mr.Duck
Anti Virus

- Active UH faculty, staff, students, and affiliates may install McAfee anti-virus software **free of charge**
- Make sure you have anti virus installed and that the definitions are up to date.
- [www.hawaii.edu/software](http://www.hawaii.edu/software)

[http://www.hawaii.edu/askus/831](http://www.hawaii.edu/askus/831)
This Includes Macs

Widespread Virus Proves Macs Are No Longer Safe From Hackers

By NICOLE PERLROTH

Finding Sensitive Information

- Install and run Identity Finder on Windows and Mac computers regularly to find and remove sensitive information
  - [http://www.hawaii.edu/askus/1297](http://www.hawaii.edu/askus/1297)
- Use Find_SSN for Linux or legacy machines.
  - [http://www.hawaii.edu/askus/1323](http://www.hawaii.edu/askus/1323)
- Identity Finder free edition for personal use
Vulnerability Scanning

- For vulnerability scanning the links for Open VAS are:
  Scan a single machine:
  http://openvas.hawaii.edu/cgi-bin/myopenvas
  Batch scan:
  http://openvas.hawaii.edu/batchopenvas/index.php
Personal Firewalls

- Properly configured firewalls can help protect from viruses, malware, and hackers into your computer.
- Improper installation can lead to a false sense of security.
- More information
  - [http://hawaii.edu/askus/658](http://hawaii.edu/askus/658)
Patches

- Run Windows and Mac system updates regularly and set to auto update when possible
- Don’t forget to patch other applications regularly
  - Microsoft Office
  - Adobe Products
  - Update web browser software regularly
Social Engineering

- Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.
- Always verify people calling and asking for information.
- When in doubt call company back at a known legitimate number.
Social engineering attacks

Hackers understand that employees are often the weakest link in a security system. A single victim can provide enough information to trigger an attack that will affect an entire organization. While there is no way to stop social engineering attacks entirely, technology experts say the best way to minimize risks is for company leaders to create security-aware cultures.

Channels used in successful security system breaches

- Phone: 46%
- In-person: 37%
- E-mail: 17%
- Texting: 3%
- Social networking site: 2%
- Unknown: 2%

Employees targeted by hackers

- Regular employee/end-user: 43%
- Cashier/teller/waiter: 33%
- Call center staff: 8%
- Finance/accounting staff: 6%
- System/network administrator: 5%
- Executive/upper management: 3%
- Help desk staff: 3%
- Customer: 2%
- Human resources staff: 2%
- Unknown: 6%


http://www.cleveland.com/business/index.ssf/2012/10/social_engineering_is_a_growin.html
Mobile Device Security

- Always use a pin code to secure computer
- Beware of malicious apps and software
- Enable tracking information and ability to remotely wipe devices
Wireless Security Best Practices

- Do not connect to unsecured wireless access points.
- Do not access sensitive information or password protected accounts if you are not sure if the access point is secure.
- For personal access points
  - Change default SSID
  - Enable WPA encryption
Social Networking Best Practices

- Don’t provide too much information online. Social engineers can gain your trust by using information freely available that YOU posted
- Don’t post things that could be used to guess answers to security questions
- Check your privacy settings for each account
Sign Up For The Last Presentation

- Wednesday, October 31 11:30-12:30
- [www.hawaii.edu/training](http://www.hawaii.edu/training)
- Securing your online browsing habits
  - Phishing
  - Malware
  - Safe web browsing
  - Ecommerce
  - Safe Email Usage
Key Points To Remember

- Physically secure devices
- Don’t leave devices unattended
- Use a strong password
- Use and update antivirus software
- Patch all of your applications regularly
- Be aware of social networking tactics
- Don’t use unsecured wireless hotspots for sensitive computing
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 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 after each presentation)*
  - Presentation Rebroadcasts
  - 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
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.

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
Securing Deletions Electronic Information
How to Securely Delete Electronic Information in Windows
Securing Your Desktop Computer
Windows Phishing
Securing Your Computer & Protecting Your Information
Web Transaction Security
Setting Up Windows Encryption
Setting Up Encryption on Mac
Exchanging Files Securely at UH - UH File

Information Security Policies

UH Executive Policies
- E2.210: Use and Management of Information Technology Resources policy
- E7.208: Student Conduct Code [pdf]

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

State of Hawaii Revised Statutes
- HRS 535: Uniform Information Protection Act (UIPA)
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