Think Before You Click

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
  o Provide oversight of IT security issues and concerns
  o Ensure compliance with policies
  o Perform security audits and risk assessments
  o Initiate and monitor the protection of sensitive information
  o Implement mandatory information security training
  o Support the automatic monitoring of network and technology resources
  o Review and revise security policies
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:
  o Raise awareness about cyber security and online safety precautions
  o Protect our national digital infrastructure
  o Help prevent fraud and identity theft
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.

![Smart banner](smart.png)
UH Awareness Campaign for Cyber Security Month

• What’s in it for the UH community?
  o Prevent future breaches
  o Safeguard sensitive information
  o 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

• Criminals are after your personal information to commit fraud or other crimes
• Minimize the amount of personal information you share
• Check your credit report and personal financial accounts regularly
• Other forms of identity theft
  o Child identity theft
  o Medical identity theft
• Refer to resources available on identity theft

Responsible Computing Practices Review

- Physically protect your devices, media, and paper
- Don’t leave electronic devices unattended even for a minute
- Secure access to data with strong but memorable passwords and security questions
- Enable screen saver auto lock with password
- Install and update anti-virus
- Keep all software up to date – set auto updates

What Will We Cover Today?

- Web browsing safety
- Phishing
- Malware
- Digital Millennium Copyright Act (DMCA)
- Steps to protect your data and cyber footprint
### World Internet Usage and Population Statistics

**June 30, 2012**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Africa</strong></td>
<td>1,073,380,925</td>
<td>4,514,400</td>
<td>167,335,676</td>
<td>15.6 %</td>
<td>3,606.7 %</td>
<td>7.0 %</td>
</tr>
<tr>
<td><strong>Asia</strong></td>
<td>3,922,066,987</td>
<td>114,304,000</td>
<td>1,076,681,059</td>
<td>27.5 %</td>
<td>841.9 %</td>
<td>44.8 %</td>
</tr>
<tr>
<td><strong>Europe</strong></td>
<td>816,372,817</td>
<td>105,096,093</td>
<td>518,512,109</td>
<td>63.5 %</td>
<td>393.4 %</td>
<td>21.5 %</td>
</tr>
<tr>
<td><strong>Middle East</strong></td>
<td>223,608,203</td>
<td>3,284,800</td>
<td>90,000,455</td>
<td>40.2 %</td>
<td>2,639.9 %</td>
<td>3.7 %</td>
</tr>
<tr>
<td><strong>North America</strong></td>
<td>348,280,154</td>
<td>108,096,800</td>
<td>273,785,413</td>
<td>78.6 %</td>
<td>153.3 %</td>
<td>11.4 %</td>
</tr>
<tr>
<td><strong>Latin America / Caribbean</strong></td>
<td>592,994,842</td>
<td>18,068,919</td>
<td>254,915,884</td>
<td>43.0 %</td>
<td>1,310.8 %</td>
<td>10.6 %</td>
</tr>
<tr>
<td><strong>Oceania / Australia</strong></td>
<td>35,815,913</td>
<td>7,620,480</td>
<td>24,279,579</td>
<td>67.8 %</td>
<td>218.6 %</td>
<td>1.0 %</td>
</tr>
<tr>
<td><strong>WORLD TOTAL</strong></td>
<td>7,012,519,841</td>
<td>360,985,492</td>
<td>2,405,510,175</td>
<td>34.3 %</td>
<td>566.4 %</td>
<td>100.0 %</td>
</tr>
</tbody>
</table>

# Statistics

<table>
<thead>
<tr>
<th>Computer Virus Statistics</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of US households that experience heavy spam</td>
<td>24 million</td>
</tr>
<tr>
<td>Number of households that have had serious virus problems in the past 2 years</td>
<td>16 million</td>
</tr>
<tr>
<td>Number of households that have had spyware problems in the past 6 months</td>
<td>8 million</td>
</tr>
<tr>
<td>Number of households that lost money or had accounts misused by phishing</td>
<td>1 million</td>
</tr>
<tr>
<td>Estimated cost to US households for viruses, spyware and phishing</td>
<td>$4.55 billion</td>
</tr>
<tr>
<td>Percent of all US households that have been affected by viruses</td>
<td>40 %</td>
</tr>
<tr>
<td>Most widespread virus to date by number of infections – “Conficker Virus”</td>
<td>8,976,038</td>
</tr>
</tbody>
</table>

Web Browsing Safety

- Use anti-virus software on your computer
- Use a firewall on your computer
- Create and use strong passwords
- Update your security software
- Beware of instant message links and e-mail attachments
- Protect yourself on all wireless networks
Web Browsing Safety

• Check the URL of a website to make sure it’s legitimate
• Ensure your web browser software and all plugins are up to date
• Recognize fake antivirus popups
WARNING! 3 threats found!!!

Unwanted software (malware) or tracking cookies have been found during last scan. It is highly recommended to remove it from your computer.

- Lost Documents and Settings
- Permanent Data Loss
- System not starting up
- System Slowdown and Crashes
- Loss of Internet Connection
- Infecting other computers on your network

Remove all threats now.
URL Safety

- Avoid clicking on links in pop-up ads or links in emails that seem to be phony or suspicious. A good general rule is to type the Web site address in your address bar directly, rather than use a link in an email message.

- You can check the URL in any email or on another Web site by simply holding your mouse above the link. The URL will appear in your browser or status bar (the bar that is usually at the bottom of your screen) and you can see what the name of the site is before you actually click on it.
Common Signs of a Fake URL

• A fairly sure sign that a URL is fake is if the URL contains the "@" sign in the middle of the address. If a URL contains the "@" sign, the browser ignores everything to the left of the link. For example, if you go to a Web site that is www.paypal@150.44.134.189, you are not going to the Paypal site at all.

• A dead giveaway for a fake URL or a fake Web site is basic spelling mistakes in the Web address itself. Some URLs look very much like the name of a well-known company, but there may be letters transposed or left out. An example might be "mircosoft.com" instead of "microsoft.com." These slight differences can be easy to miss, and that's what phishers are counting on.
Fake Paypal URLs

- The popular Paypal site is a common target for phishers and scammers. Even if a URL contains the word "paypal," it may not be the authentic Paypal site. Some common URLs that will NOT lead you to the real Paypal site are: www.paypalsecure.com and www.paypal@accounts.com.
Secure Socket Layer (SSL)

• What is SSL?
  o A protocol that establishes an encrypted link between a web server and a browser ensuring all data passed between the web server and browsers remain private

• In other words:
  o “keeps your data safe”
How do I Know the Link is Secure?

Look for the httpS:// (the S means it is encrypted)

https://myuh.hawaii.edu,cp/home/display/login

And/Or a padlock

Why is it important?

• The S or the padlock means:
  o That you have a secure (encrypted) link with this web site
  o That this web site is a valid and legitimate organization or an accountable legal entity
This Connection is Untrusted

You have asked Firefox to connect securely to [URL], but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▪ Technical Details
▪ I Understand the Risks
Using Public Computers

• Remember to “Logoff” of any password protected webpage instead of just closing your browser

• Clear the browser’s cache and web cookies

• When logging into password protected sites, do not use the “Save my username and password” option

• Do not log into banking or other sensitive sites over public or unsecured wireless hotspots

• Use private browsing
Private Browsing

Private Browsing allows you to browse the Internet without saving any information about which sites and pages you’ve visited.

Warning: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be installed on your computer.
What is Phishing?

• From Wikipedia: Phishing is "the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication."

http://en.wikipedia.org/wiki/Phishing
---------- Forwarded message ----------
From: 2012 Site Upgrade <various email addresses>
Date: Wed, Oct 10, 2012 at 12:44 PM
Subject: Dear HAWAII.EDU Account User
To:

--

Dear HAWAII.EDU Account User

Due to congestion on our email users and removal of all unused accounts, We will be closing all unusual accounts on 17TH October 2012. You must confirm your account as soon as possible so we can update your account before the deadline.

To confirm your account fill out the form to verify the account.
Full name:
Email: 
password:
Tel:

After following the instructions on the sheet, your account will not be interrupted and will continue normally. Thank you for your attention to this request.

We apologize for any inconvenience.
S2012 HAWAII.EDU USER Upgrade Equipment
Remember

• ITS will NEVER ask you for your password over email

• Check the ITS website for current Phishing attempts
  o http://www.hawaii.edu/its/

• How to report a Phishing email targeting UH
  o http://www.hawaii.edu/askus/966
Email

• Don’t click on attachments that you weren’t expecting
• Do not reply to Phishing emails, even to say that you aren’t interested in or to ask them to stop contacting you
• Use spam filters
• Be wary of emails that have misspellings or don’t use your correct name
• Type in the URLs of your bank or other sensitive websites instead of clicking on the URL in emails
Spam

- Email Spam is the electronic version of junk mail. It involves sending unwanted messages, often unsolicited advertising, to a large number of recipients. Spam is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks.

- According to Symantec’s latest State of Spam report, spam now accounts for **72% of all email messages**.
I WON AN IPAD!

I BETTER GIVE THEM ALL OF MY PERSONAL INFORMATION!
How Do You Know it’s Spam?

• Messages that do not include your email address in the TO: or CC: fields are common forms of Spam

• Some Spam can contain offensive language or links to Web sites with inappropriate content

• Spam also includes many misspellings or poor sentence structure
Reporting Spam

• If you obtain spam from an @hawaii.edu account, you can report it to abuse@hawaii.edu

• If it's not from an @hawaii.edu account:
  o If you get spam that is phishing for information, forward it to spam@uce.gov.
  o If you believe you've been scammed, file your complaint at http://www.ftc.gov and then visit the FTC's Identity Theft Web site at http://www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft.
  o If you receive a porn spam (pornography), you can report it at http://www.obscenitycrimes.org/. It should also be reported back to the ISP (Internet Service Provider) where the email originated from.
What To Do?

• Install Spam filtering/blocking software

• If you suspect an email is Spam, do not respond, just delete it

• Consider disabling the email client’s preview pane and reading emails in plain text

• Keep software and security patches up to date
Malware vs. Spyware

• Malware is a blanket term that is used to describe a number of malicious types of software, including adware, spyware, viruses, trojans, and more.

• Spyware is a specific type of malware, but is quite different from most other malicious software because of what it is designed to do.
Malware

- Malware is a category of malicious code that includes viruses, worms, and Trojan horses. Destructive malware will utilize popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy.

- Malware works to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user.
What To Do?

• Only open email attachments that come from a trusted source and that are expected

• Have email attachments scanned by antivirus prior to opening

• Delete all unwanted messages without opening

• Do not click on Web links sent by someone you do not know

• Only transfer files from a well known source

• Keep security patches up to date
Spyware

• Spyware can be downloaded from Web sites, email messages, instant messages, and from direct file-sharing connections. Additionally, a user may unknowingly receive spyware by accepting an End User License Agreement from a software program.

• Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user.
How Do I Avoid Spyware?

• Be selective about what you download to your computer

• Read licensing agreements

• Watch out for anti-spyware scams

• Beware of clickable ads

• Keep your Internet browser up to date

• Scan your computer often
Scan Your Computer

• Identity Finder – Windows and Macs
  o Download at www.hawaii.edu/software
  o How to use: www.hawaii.edu/askus/1297

• Find SSN – Linux, Solaris and Legacy OS
  o www.hawaii.edu/askus/1323

• Scan for vulnerabilities
  o Scan a single machine:
    http://openvas.hawaii.edu/cgi-bin/myopenvas
  o Batch scan:
    http://openvas.hawaii.edu/batchopenvas/index.php
Instant Messaging
Instant Messaging Tips

• Create a strong password for your IM account
• Never accept files or click links within messages you weren’t expecting.
• Never trust that your IM conversations are completely secure.
  o Use SSL encryption if possible
• Never give out any personal or sensitive information when using IM
• Choose a screen name that isn’t too close to your real name
• Check your security settings
• Make sure you’re using an updated version of your IM software
• Remember that your IM client is only as secure as your own computer
• Reject all Instant Messages from persons who are not on your Buddy list
Digital Millennium Copyright Act (DMCA)
What is DMCA?

• An act created to protect intellectual property in digital form

• Downloading / Distribution of copyrighted work without authority constitutes an infringement

• Examples of copyrighted materials are songs, movies, TV Shows, software, and games

• Violations are subject to civil and criminal liabilities
UH Responsibility for Copyright Infringements

• The University of Hawaii policy E2.210: Use and Management of Information Technology Resources prohibits illegal downloading or sharing of copyrighted information

• Copyright agents notify UH when copyrighted materials are illegally shared

• Per federal mandate, UH must investigate each incident

• UH must comply with all reported incidents or the University of Hawaii could lose ALL Federal Financial Aid!
UH Requirements for DMCA

• Notify the copyright infringer of the infringement
• Require them to remove the infringing material
• Provide education on Copyright Infringement
DMCA Violation
Consequences

• UH complies with all copyright legal obligations
• When presented with a subpoena UH will provide the violators information
• The individual can be sued
• Penalties include civil and criminal penalties
• Civil penalties may be actual damages at not less than $750 and not more than $30,000 per work infringed
• Criminal penalties include imprisonment of up to five years and fines up to $250,000 per offense
WEB & COMMUNICATION SOFTWARE

Judge Sees Nothing Unreasonable About $675,000 Music Piracy Fine

By Jared Newman, PCWorld

A U.S. District Court judge has upheld a $675,000 fine for Joel Tenenbaum, the former Boston University student who illegally downloaded and shared 31 songs through the long-defunct service Kazaa.

Tenenbaum, who first started fighting the case in 2007, was found guilty two years later, and faced a fine of $22,500 per song. Although U.S. District Court Judge Nancy Gertner found the jury's original verdict to be "unconstitutionally excessive," an appeals court overturned her decision last November.

In May, the U.S. Supreme Court refused to hear Tenenbaum's appeal on constitutional grounds, so the case went back to the U.S. District Court again, with a new judge who was not allowed to rule based on constitutionality.

That brings us to this week's ruling by Judge Rya Zobel. In her decision to uphold the original $675,000 fine, Zobel notes that Tenenbaum "received multiple warnings" about file sharing, and continued to download and share songs even after receiving a cease-and-desist letter from Sony in 2005. She also points out that Tenenbaum had his laptop's operating system reinstalled, and his hard drive wiped, despite being told in 2005 to preserve evidence of his activities.

http://www.pcworld.com/article/261388/judge_sees_nothing_unreasonable_about_675_000_music_piracy_fine.html
Legal Alternatives

- **Movies**
  - Google Play
  - Hulu
  - YouTube Movies
  - IMDB

- **Music**
  - Grooveshark
  - Pandora
  - Last.fm

- **Books**
  - Hawai‘i State Public Library System
    - hawaii.lib.overdrive.com
Mobile Malware

• How does a mobile device get infected?
  o Crafted malicious URL
  o Malicious Apps

• What can mobile malware do?
  o Sends out SMS messages
  o Destroys data on device
  o Can spread to computers to infect them when synced
Malicious websites are a popular method for getting malware out there. An average of 2.7 million malicious URLs were detected each month, pointing to approximately 300,000 bad domains. That works out to about 10,000 new malicious domains being created every day with the express purpose of hosting malware and hijacking unprotected mobile devices.
Steps To Protect Your Digital Footprint

• Think before you add pictures or content to the internet
  o Even if you delete it, it might be there forever
• Check social networking security settings
• Google yourself
• Be careful about what applications you install in Facebook and what information that application has access to on your profile
• Verify friend requests and wall posts that seems suspicious or you weren’t expecting before clicking on them
Cyber Security Month Lives On

• Practice Safe Computing Every Day
  o Verify before you click
  o Limit the information you post on-line
  o Create long and strong passwords
  o Set software to auto update
  o Use and update anti virus software
  o Shred confidential documents
  o Securely erase data from devices before disposal
  o Use a locking feature for all devices
  o Physically secure devices and paper documents
  o Comply with the Digital Millennium Copyright Act
  o Be aware of social networking tactics
UH Resources

• Report phishing
  o http://www.hawaii.edu/askus/966

• Download antivirus
  o http://www.hawaii.edu/software

• ITS security, phishing and virus alerts
  o http://www.hawaii.edu/its/

• Opt-in ITS virus alert listserv
  o http://www.hawaii.edu/askus/967

• Opt-in ITS phishing notification listserv
  o http://www.hawaii.edu/its/notices/index.php
Things To Remember

• Make sure you are going to a valid URL, don’t be fooled just because the site looks valid

• Watch out for spam and phishing emails

• Remember that instant messaging is not safe

• Do not download illegal material

• Remember that malware can affect mobile devices

• Be careful what you post online
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 neighbor 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
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

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

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
Securely Deleting Electronic Information
How to Securely Delete Electronic Information in Windows
Securing Your Desktop Computer
UH Spam/Phishing
Securing Your Computer & Protecting Your Information
Web Transaction Security

Information Security Policies

UH Executive Policies
- E2.210: Use and Management of Information Technology Resources policy
- E2.214: UH Information Security Policy
- E7.208: Student Conduct Code

UH Administrative Procedures
- E8.710: Credit Card Program
- A8.741 Electronic Transactions & University Website

UH Info Sec ITSecurityUH
I am the first event for NCSAM. Learn why.

ITSecurityUH Presidential Proclamation -- National Cybersecurity Awareness Month, 2012

Join the conversation
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