Protecting Yourself In Our Digital World

Jodi Ito
Information Security Officer
jodi@hawaii.edu • (808) 956-2400
New Information Security Team!

• Deanna Pasternak
deannacp@hawaii.edu
(808) 956-7975

• Taylor Summers
tsummers@hawaii.edu
(808) 956-5791
Contact Info:

Email:
infosec@hawaii.edu

Website:
www.hawaii.edu/infosec
Today’s Digital Environment
has become a verb!
Young people say online meanness pervasive

By Associated Press

POSTED: 02:55 a.m. HST, Sep 27 2011

3 indicted for ID theft as drivers filled tanks

They allegedly attached devices to gas pumps to "skim" information about bank accounts

By Nelson Daranciang

Prosecutors seek bail

By Associated Press

POSTED: 07:52 p.m. HST

The tourist from Washington state charged with killing his girlfriend during their stay at a Big Island resort was on probation for domestic violence and cyber-stalking before arriving in Hawaii for vacation, according to police and court documents.
National Cyber Security Awareness Month

October is Cyber Security Awareness Month

Learn More
Secretary Janet Napolitano on Cyber Security

http://www.dhs.gov/video/
secretary-napolitanos-cybersecurity-message
Cyber Security is National Concern

- Department of Homeland Security (DHS)
  - “Stop. Think. Connect.” Campaign:
    - http://stopthinkconnect.org/
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
  - http://msisac.cisecurity.org/
- United States Computer Emergency Readiness Team (US-CERT)
  - http://www.us-cert.gov/cas/tips/
www.hawaii.edu/infosec/ncsam.html

• Be Cyber S.M.A.R.T.
  – Week 1: Secure Information Destruction
  – Week 2: Management and Storage of Sensitive Information
  – 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
Technologies and Trends

• INFORMATION AGE!

• **NOW** Generation

• PDAs, laptops, netbooks + (wireless networks/cellular broadband) = Mobile Computing

• Cellphones --> Smartphones

• “Texting”, “Tweeting”, “Friending” --> Social Networking

• **WHOLE NEW WORLD!**
Today’s Conveniences?

iPhone App Deposits Bank Checks

Qualified USAA customers can use the iPhone camera to take pictures of their checks and make deposits into their accounts over the air.

By Marin Perez, InformationWeek
August 10, 2009 01:54 PM

United Services Automobile Association bank customers won't have to worry about finding a branch or ATM, as the bank's iPhone app will soon enable users to deposit checks with the handset's camera.

The company said it planned to update its iPhone app this week to enable customers to take pictures of both sides of checks, and then have the funds deposited over the air. Users don't have to send the check to the bank later, and USAA said the process will be handled entirely electronically.

http://www.informationweek.com/iphone-app-deposits-bank-checks/219100621
Using mobile devices to open hotel doors

Hotel door opening technology moving to mobile devices

Posted by Kevin May on 01 March 2010

Travel technology firm OpenWays is attempting a major push to the world’s hotel chains with a new system which allows customers to open doors with a mobile.

The system works by sending an digitally encrypted audio bleep to the door locking mechanism from any smartphone.

Customers are given a code when they check in to a hotel which then sits within a downloadable app on their iPhone, Android or Blackberry device.

The technology was created so it would work with existing locks that use the Crypto Acoustic Credential system, a standard on many electronic access control and locking devices such as those in hotels.

http://www.youtube.com/watch?v=eHruySdTarE
Keyless systems on cars easily hacked, researchers say

Researchers at Switzerland's ETH Zurich University show how passive keyless entry and start systems can be compromised

By Jaikumar Vijayan, Computerworld
January 19, 2011 11:28 AM ET

The passive keyless entry and start (PKES) systems supported by many modern cars are susceptible to attacks that allow thieves to relatively easily steal the vehicles, say security researchers at Switzerland's ETH Zurich University.

In demonstrations using 10 cars from eight makers, the researchers showed how they were able to unlock, start and drive away the cars in each case, by outsmarting the smart key system.

The break-ins were carried out using commercial, off-the-shelf electronic equipment available for as little as $100, the researchers said in a paper describing their exploits.
Cybercrime migrating to mobile and Apple, Cisco report

Greg Masters  January 21, 2011

The tide in cybercrime is shifting away from attacks on Windows machines and migrating to the mobile marketplace, according to a just released yearly report from Cisco.

The report cited as one of its chief findings that computer users the world over are falling victim to exploits that prey on their inherent trust through a variety of social engineering scams — whether via email, social networking chat or phone calls. For example, scammers will try to dupe users into action by pretending to be an attractive man or woman, particularly on social networking sites. "People should assume that a flirtatious advance from someone they don't know has a less-romantic purpose behind it," the report warned.

Cybercriminals have also become skilled at convincing users that their infected links and URLs are safe to click on, and that they are someone the user knows and trusts, the report stated. And once stolen security credentials are acquired, the perpetrators can gain access to legitimate software and systems.
Peer-to-Peer (P2P) File Sharing

- Gnutella, Kazaa, BitTorrent
- Largely used to share copyrighted materials illegally
- www.hawaii.edu/its/filesharing
- Other unexpected problems include inadvertently sharing sensitive information…
“P2P Snoopers Know What's In Your Wallet”

Being security researchers and all, Larry Pesce and Mick Douglas thought it would be a hoot to take a look at some of the information people send out over peer-to-peer (P2P) networks. They were taken aback by what they found.

At the 2010 ShmooCon security conference Friday, the duo showed off the extremely sensitive information they’ve been able to intercept, including driver’s licenses and passports, tax return forms with Social Security numbers; someone’s last will and testament and information on one man’s secret activities that could potentially be exploited by terrorists.

Also from ShmooCon: The Bigger the Security Arsenal, the Harder the Fall (podcast)

Douglas and Pesce were inspired to look at P2P networks after highly-publicized incidents where
details on a U.S. Secret Service safe house for the First Family leaked out on a LimeWire file-sharing network. In another incident, classified data on the communications, navigation and management systems on Marine One were found in a publicly available shared folder on a computer in Tehran, Iran, after apparently being leaked over a P2P network.
File Sharers, Beware!
Opening Up Your Computer To Outsiders Can Lead To Snooping
By Jaime Holguin

(CBS) It was among the most frightening phone calls Don Bodiker ever received. A stranger calling from California was reading Bodiker's tax return.

"We had not even sent our taxes in yet," he says. "They had not even been mailed."

And worse, the stranger got the tax return online straight out of his computer, "where he could read every single line of everything that I had on my taxes," says Bodiker.

It was, he says, "a very scary moment for us."

found the mystery caller CBS News, who wants to be known only as "Jeff from Sacramento." So far, Jeff has called 120 people to warn them their financial documents are available because of file sharing.

It's all there, he says – tax files, checking account and routing number.

As CBS News Correspondent Wyatt Andrews reports, file sharing today is the rage on the Internet, mostly because of users who want to share songs. But because file sharing literally opens your computer to outsiders it can also lead to snooping. All Jeff does is search for the word "tax."

http://www.cbsnews.com/stories/2005/05/03/eveningnews/main692765.shtml
Common Digital Threats

• Viruses, Spyware, Trojans & Other Malicious Software such as KEYSTROKE LOGGERS
• Botnets
• Phishing & Spam
• Identity Theft
• Cyber Stalking, Cyber Bullying, Online Predators
• Etc., etc., etc…. 
Facebook stalking of sorority pledges rattles students

Authorities say man claimed to be a sorority alum to extort students in a case that shows the need for online privacy

From staff and wire reports
Category: Higher Ed, Litigation, Safety & Security, Top News
Tags: facebook stalking, online privacy, sorority pledges

A Florida man accused of using Facebook to harass Louisiana State University (LSU) sorority pledges and pressure them into sending him nude pictures also is a suspect in other states, authorities said this month.

Campus police officers at LSU and Florida Department of Law Enforcement (FDLE) agents on Dec. 16 arrested 27-year-old Mitchell Hill at a home in Key West, Fla., where he works as a chef at a Cuban restaurant.

He's facing only Louisiana charges so far, but FDLE spokesman Keith Kameg said Hill is suspected in Facebook stalking investigations by police at the University of Florida, Florida State University, and possibly other Florida schools.

Similar cases also have been reported at Auburn University, the University of Alabama, and the University of Tennessee, but investigators said there probably are others in a case that serves as a stark reminder of the need to safeguard online privacy.
Tyler Clementi Suicide Result of Cyber Bullying? Video

By Kaitlyn Piccoli on September 30th, 2010

Phishing

• University of Hawaii Phishing Attacks
• Generally: email asking for UH username/password
• Usually threatens closing of account due to: Quota, Congestion, Upgrade, Update, etc…

• DO NOT RESPOND!
• UH will NEVER ask for your password in an email!
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
Excellent UH Phish!

• “Security” email directed recipients to web site to “protect” their accounts
• Email contained a link that APPEARED to be: mail.hawaii.edu
• Phishers used UH graphics to replicate phishing web page
Inspect the web link CAREFULLY!!

(XXX.hawaii.edu should be after http://)
Targeting CFOs

Cyber Thieves Steal Nearly $1,000,000 from University of Virginia College

Cyber crooks stole just shy of $1 million from a satellite campus of The University of Virginia last week, KrebsOnSecurity.com has learned.

According to several sources familiar with the case, thieves stole the funds after compromising a computer belonging to the university’s comptroller. The attackers used a computer virus to steal the online banking credentials for the University’s accounts at BB&T Bank, and initiated a single fraudulent wire transfer in the amount of $996,000 to the Agricultural Bank of China. BB&T declined to comment for this story.

The attack on UVA Wise is the latest in a string of online bank heists targeting businesses, schools, towns and nonprofits. Last week, cyber thieves stole more than $600,000 from the Catholic Diocese of Des Moines, Iowa.

Cyber Crime Industry

“The most optimistic estimate will come in at about US$600 billion per year, the most pessimistic at $920 billion per year, giving a growth of between 15 per cent to 25 per cent year-on-year; that is the value of cybercrime to the global economy,” Doherty said. “To give you some scale, mid-$500 billion is the global narcotics trade.”

- Reported 2/2011
Data breaches earn UH an 'F'

Personal information in nearly 260,000 records has been exposed since 2005, a report says

By Gordon Y.K. Pang

POSTED: 01:30 a.m. HST, Nov 18, 2010

A national organization has given the University of Hawaii a grade of "F" for online security breaches that exposed Social Security numbers and other sensitive information in nearly 260,000 records.

The Liberty Coalition, a nonprofit civil liberties watchdog group, yesterday said more than half of the estimated 479,000 Hawaii records breached since 2005 were those mishandled by UH.

Class-action suit filed against UH over data breaches

By Gene Park

POSTED: 01:35 p.m. HST, Nov 18, 2010

The University of Hawaii is now the target of a class-action lawsuit filed today, as a result of recent data breaches.

The main plaintiff in the case, Philippe Gross, was a student at the Manoa campus from 1990 through 1998. He said four other names have been attached to his social security number, and that his credit card has been used in Georgia.

Data Breaches

- Privacy Rights Clearinghouse
- [http://www.privacyrights.org](http://www.privacyrights.org)

- As of Oct. 10, 2012:

  563,656,459 RECORDS BREACHED
  (Please see explanation about this total.)
  from 3,418 DATA BREACHES made public since 2005
Impact of Social Media
The above cartoon by Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20) only for academic discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.
Social Networking

• Do not post TOO MUCH INFORMATION!
• Internet is FOREVER!
  – Whatever you post may circulate even AFTER you delete it
• New scams use social networking sites to get background personal information
• Watch what your children do on the computer
Online Reputation Management

- Understand service’s privacy policy
- Know how information is being tracked & stored…
- **Know what is online about YOU!**
TTMI...

- Tweeting Too Much Information:
  http://pleaserobme.com/

Raising awareness about over-sharing
Check out our guest blog post on the CDT website.
Geotagging

• Pictures taken w/ a GPS-enable smartphone “tags” each picture with the longitude & latitude of the location of the picture
Introduction

• In August of 2010, Adam Savage, of “MythBusters,” took a photo of his vehicle using his smartphone. He then posted the photo to his Twitter account including the phrase “off to work.”

• Since the photo was taken by his smartphone, the image contained metadata revealing the exact geographical location the photo was taken.

• So by simply taking and posting a photo, Savage revealed the exact location of his home, the vehicle he drives and the time he leaves for work.

Read the full story here: http://nyti.ms/917hRh
Virtual Earth
Street, Anaheim, CA 92802

Google
1500-1640 S West St, Anaheim, CA 92802, USA
Downtown Disney
S West St, Anaheim, CA 92802
Directions Search nearby Save to... more▼

Explore this area »

Photos
Turning off Location Services

- iPhone
- Settings > Location Services
Tapping Your Cell Phone

• http://www.wthr.com/Global/story.asp?s=9346833
Hawaii Stalking Laws

- Click on “Hawaii Revised Statutes”
- Search for “stalking”

§711-1106.4 Aggravated harassment by stalking. (1) A person commits the offense of aggravated harassment by stalking if that person commits the offense of harassment by stalking as provided in section 711-1106.5 and has been convicted previously of harassment by stalking under section 711-1106.5 within five years of the instant offense.

(2) Aggravated harassment by stalking is a class C felony. [L 1995, c 159, §1; am L 2003, c 68, §1]
§711-1106.5 Harassment by stalking. (1) A person commits the offense of harassment by stalking if, with intent to harass, annoy, or alarm another person, or in reckless disregard of the risk thereof, that person engages in a course of conduct involving pursuit, surveillance, or nonconsensual contact upon the other person on more than one occasion without legitimate purpose.

(2) A person convicted under this section may be required to undergo a counseling program as ordered by the court.

(3) For purposes of this section, "nonconsensual contact" means any contact that occurs without that individual's consent or in disregard of that person's express desire that the contact be avoided or discontinued. Nonconsensual contact includes direct personal visual or oral contact and contact via telephone, facsimile, or any form of electronic communication, as defined in section 711-1111(2), including electronic mail transmission.

(4) Harassment by stalking is a misdemeanor. [L 1992, c 292, §2; am L 2003, c 68, §2; am L 2009, c 90, §2]
“Checking in”

- Facebook Places
- Mobile Twitter
- Gowalla
- Foursquare
CHECK-IN
FIND YOUR FRIENDS
UNLOCK YOUR CITY

Foursquare on your phone gives you & your friends new ways of exploring your city. Earn points & unlock badges for discovering new things.

RECENT ACTIVITY

Ong G. in Singapore:
 wrote a tip @ SingTel Business Solution Centre (BSC):
SingTel Business Solution centre is where we showcase our innovations. Come spark off new ideas with us.

Yvin H. in Amsterdam, The Netherlands:
 wrote a tip @ MacHouse Amsterdam: Koffie, thee en warme choocolop op de eerste verdieping!

Wadi M. in Tempe, AZ:
 unlocked the 'Bookworm Bender' badge.

GET IT NOW

iPhone →
BlackBerry →
Android →
palm →
“Location-Aware” Services

www.groupon.com
Safe Web Browsing

• Browsers keep information in “cookies” and “temporary files”
• Information in these files are retained unless you explicitly delete them
• Enable “private browsing”
• http://www.hawaii.edu/askus/922
• Google’s new privacy policy (3/1/2012):
  • http://www.networkworld.com/news/2012/022712-google-privacy-policy-256399.html
Facebook Privacy

- http://www.facebook.com/about/privacy

Data Use Policy

Information we receive and how it is used
Learn about the types of information we receive, and how that information is used.

Sharing and finding you on Facebook
Get to know the privacy settings that help you control your information on facebook.com.

Other websites and applications
Learn about things like social plugins and how information is shared with the games, applications and websites you and your friends use off Facebook.

How advertising and Sponsored Stories work
See how ads are served without sharing your information with advertisers, and understand how we

More resources
- Interactive Tools
- Minors and Safety
- View the complete Data Use Policy

If you have questions or complaints regarding our Data Use Policy or practices, please contact us by mail. If you are located in the U.S. or Canada, our mailing address is Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025. If you are located outside the U.S. or Canada, our mailing address is Facebook Ireland Ltd., Hanover Reach, 5–7 Hanover Quay, Dublin 2 Ireland. You may also contact us through this help page.
Sharing and finding you on Facebook

Control each time you post
Whenever you post content (like a status update, photo or check-in), you can select a specific audience, or even customize your audience.

To do this, simply click on the sharing icon and choose who can see it.

Choose this icon if you want to make something Public. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it. Learn more about public information.

http://www.facebook.com/about/privacy/your-info-on-fb
Facebook Security

- https://www.facebook.com/security
Information About YOU!

Facebook: www.facebook.com
Twitter: www.twitter.com
LinkedIn: www.linkedin.com
Spokeo: www.spokeo.com
Pipl: www.pipl.com

SEARCH FOR YOURSELF!
Searching Continued:

Honolulu Property Tax Info
http://www.honolulupropertytax.com/Main/ Home.aspx

Search Public Records:
http://www.publicrecordfinder.com
http://maps.google.com (with street view)
On target and in-depth, Kim’s Columns provide you with what you need to know to buy smart, keep safe and stay informed.

3/13/2010

Databases track your every move and more

Ever wonder just how much information about you is contained in databases and on the Internet? Here’s a hint. It’s much more than you think.

If your telephone number is published, a simple Google search can turn up your home address, phone number, and a map to your front door. Everyone knows that. But there are other databases and sites that contain intimate details of your life.

More Information About Yourself

• Credit Reports:  
  www.annualcreditreport.com

• Personal Information Reports:  
  – LexisNexis  
    Full File Disclosure & FACT Act:  
    https://personalreports.lexisnexis.com/  
  – Acxiom:  
Information About Others

• Hawaii State Court records: [http://www.courts.state.hi.us/legal_references/records/search_court_records.html](http://www.courts.state.hi.us/legal_references/records/search_court_records.html)
  - eCourt Kokua (traffic, appeals, supreme court)
  - Ho’oike (criminal & civil cases in circuit court)

• State of HI Dept. of the Attorney General:
  - [https://ecrim.ehawaii.gov/ahewa/](https://ecrim.ehawaii.gov/ahewa/)
  - Need to register (and verify identity w/ $1.00 one time charge to a valid US credit card)
  - $15 per record
This Cyber “stuff”…

• **Affects us all!**
  • Each unprotected/unpatched computer is a threat:
    – Infected worm/virus/bot
    – Could be used in a concerted attack against a critical infrastructure
  • Computers, servers, mobile storage devices with any sensitive information represent a vulnerability
What Do We Do?

*Practice safe computing!*
Keep Your Computers Safe

• Update the software on your computer weekly (or more frequently)
• Install anti-virus and anti-spyware software and keep it up-to-date (UH faculty/staff/students can download for free: http://www.hawaii.edu/askus/1254)
• Use accounts and strong passwords
• Encrypt sensitive information
  – http://www.hawaii.edu/askus/729
• Don’t install unknown software from unknown sites
• DO NOT SHARE your accounts/passwords
• Use password protected screen savers
Use STRONG Passwords

- Not easily guessable
- Do not use dictionary words
- Use a combination of upper and lowercase letters, numbers, and special characters
- No less than 8 characters
- Check your password strength:
  
Creating a Strong Password

• Incorporate something memorable to you
• Replace letters with numbers or characters
• Example:
  – First dog’s name is Bingo
  – You got him in 1965
  – Black spots
  – Add special characters
  ==> B1NG01965bs!
More on Passwords

• Don’t use the same password for all accounts
• Change passwords frequently
• Use more difficult passwords on more sensitive accounts
• Use a password safe (but don’t lose the master password!)
• http://passwordsafe.sourceforge.net/
• http://www.hawaii.edu/askus/705
Protect Yourself and Information

• Don’t open unknown emails & attachments
• Visit only reputable web sites
  –  http://safeweb.norton.com/
• Do not reply to SPAM or Phishing emails
• Don’t let others use your computer irresponsibly
• Use a credit card for online shopping
• http://www.hawaii.edu/infosec
• Don’t save your information in web browsers
• Use https: for sensitive web transactions (ensure lock icon is “locked”)
Basic Security Practices

• Update your operating system and applications regularly
• Do NOT give out personal/sensitive information in responding to an UNSOLICITED inquiry
• Trust your instincts – if it seems suspicious, check it out
• Use complex passwords for sensitive accounts
Mobile Best Practices

• Secure your mobile devices
  – Use accounts and complex passwords
  – Don’t leave your devices unattended
  – Enable “auto-wipe”
  – Encrypt sensitive information

• Be careful when using public wireless networks

• Be aware when using location-aware services

• www.hawaii.edu/infosec
Wireless & Public Computers

• Be cautious when using open wireless networks
  – Others using the network maybe be “sniffing” the network
• If you *must* use a public computer, change the password on the account accessed using a secure computer ASAP
Firesheep In Wolves’ Clothing: Extension Lets You Hack Into Twitter, Facebook Accounts Easily

Evelyn Rusli
Oct 24, 2010

It seems like every time Facebook amends its privacy policy, the web is up in arms. The truth is, Facebook’s well publicized privacy fight is nothing compared to the vulnerability of all unsecured HTTP sites — that includes Facebook, Twitter and many of the web’s most popular destinations.

Developer Eric Butler has exposed the soft underbelly of the web with his new Firefox extension, Firesheep, which will let you essentially eavesdrop on any open Wi-Fi network and capture users’ cookies.

As Butler explains in his post, “As soon as anyone on the network visits an insecure website known to Firesheep, their name and photo will be displayed” in the window. All you have to do is double click on their name and open sesame, you will be able to log into that user’s site with their credentials.

One word: wow.

Wi-Fi Dangers…

- Security Expert Claims Thieves Can Detect Wi-Fi In Sleeping Computers
DO NOT EVER...

• …Give out your personal information in response to an UNSOLICITED email, phone call, voice mail

• If in doubt, CHECK IT OUT!
  – Call the company using another legitimate phone number (not the one provided in the email or phone call)

• New scams use social networking sites to get background personal information
Protect Yourself!

• **BE SUSPICIOUS! & BE CAUTIOUS!**

  You can’t take back information you’ve already given out or posted

• Ask “Why?” when someone asks for your SSN
• Check your credit report:
  www.annualcreditreport.com
BE AWARE!

Know what’s out there

(Google yourself)
Resources

www.hawaii.edu/infosec
Federal Trade Commission
http://www.onguardonline.gov/
Department of Homeland Security
http://www.staysafeonline.org
Privacy Rights Clearinghouse
http://www.privacyrights.org/
Questions?

Jodi Ito
jodi@hawaii.edu
(808) 956-2400