Cyber Secure your Home and Family
Agenda

• Securing your home network
• Password Safety
• Web browsing safety
• Phishing & Spam
• Digital Millennium Copyright Act (DMCA)
• Mobile Security
• Partial credit for this presentation.... University of Hawaii Information Security Team
  – Jodi Ito - Information Security Officer
  – Deanna Pasternak & Darryl Higa Information Security Specialists

• This entire presentation can be found at http://maui.hawaii.edu/cybersecurity
Common Security Problems

- Delayed or no security fixes or patches
- Incorrect preventative measures
- Lack of focus on security
- Absence of training
- Consumed by running your home
- Reliance on outsourcing, cloud storage
- Lack of technology savvy…etc.
Evolution of Security Issues

10 years ago…after the dot-com bust
- Low Internet penetration in homes
- Reliance on paper, fax, phones etc
- OK, if you did the basics
  - Virus Protection and Backups

Today…and the future
- Phishing, social engineering, malware etc.
- Cloud computing, HIPAA, devices etc.
- Cyber breaches can ruin your privacy etc.

10/13/15
Cybersecurity for all of us
Proposed Solutions...

- **Level 1 - Basic Hygiene**
  - Train family members in security principles
  - Provide firewall security for the entire home
  - Make backup copies of important business data
  - Secure your Wi-Fi networks and secure routers
  - Limit access to data and information
Proposed Solutions

• Level II - Active Defense
  • Actively monitor your networks and property
  • Proactive guidance, policies and training
  • Reward vigilance and safe computing practices
  • Watch out for exceptions and abnormal behavior
Proposed Solutions

• Level III - Neighborhood Watch

  • Share common tactics and strategies with others
  • Obtain alerts from the crowd of friends and family
  • Actively report information security issues and concerns to authorities and others
Level I - 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, Customer records, Health information, credit card numbers, dates of birth, job applicant records, etc.

• State, Federal and Regulatory requirements provide standards for protecting sensitive information.
Know What to Protect

• A partial list of data considered sensitive

  • Customer records
  • Health information (HIPAA)
  • Personal financial information
  • Social Security Numbers
  • Dates of birth
  • Access codes, passwords and PINs
  • Answers to "security questions"
  • Confidential salary information
How to Protect Information

• Know where it is stored
• Safeguard it with physical security
• Encrypt it
• Redact it
• Delete it
Level I - Scan Your Computer

- Identity Finder – Hunt for SSNs and other confidential information
  Windows and Macs
  - Download at http://www.identityfinder.com/
Level I - Encryption

• Encrypting a Windows file, folder, and entire disk - BitLocker
  – http://www.hawaii.edu/askus/1285

• Encrypted disk images and full disk encryption for a Mac – Secure Disk Image
  – http://www.hawaii.edu/askus/676
What Does An Encrypted File Look Like?

```
EE042 5C5A4CBA54318DABCEE996A2D244E1FDF26FA4424
FE992FB268CDB4B5AFE33D8FB46576BE647BEAC33C3CE0
3C2A9CD3D057115959DE709C3B839E949F928C30FD7DDE
1D7C410AD7C938FE2463978ACA839E949F928C30FD7DDE
7B8C7ADA158053537191EF3F70839E949F928C30FD7DDE
FB8156535D9E7CDC43903CD613839E949F928C30FD7DDE
4F8031B047A5A7E505DB8E435F839E949F928C30FD7DDE
292F2744236B3160A625BE3725A7D87E8F09FBC7E39B70
B57BA53C31ABEB10B9E257942FA7D87E8F09FBC7E39B70
DA45CD5E898058B89E2A8C0BA5A7D87E8F09FBC7E39B70
F76B75C2A2080DED879F1ECC29A7D87E8F09FBC7E39B70
4DB29618A507685BA27166A152A7D87E8F09FBC7E39B70
```
DO NOT LOSE YOUR ENCRYPTION KEY

• When using encryption be careful to safeguard your encryption key. If lost ITS might not be able to help you recover your data.
Ways To Securely Transfer Sensitive Information
Level I - Secure File Transfer

• Providers such as SendThisFile  
  https://www.sendthisfile.com/solutions/overview.jsp  
  – Secure file transfer up to 100GB  
    – $19.95/mo, 10 day file access

• Security ends at transmission, you will still need to secure information on your computer
Level I – Spot Secure Links

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

- The S or the padlock means:
  - That you have a secure (encrypted) link with this web site
  - That this web site is a valid and legitimate organization or an accountable legal entity
Level I - Do Not Use To Transfer Sensitive Information

- Unencrypted Email
- Third party cloud applications such as Dropbox
- Google Drive
- Unsecured USB drives or other external devices
Level I - Where Should Sensitive Info Be Stored?

- Encrypted folders, partitions, or drives
- Secured servers
- Encrypted external drives
- Secure applications
- Locked file cabinets
Level I - Where Not To Store Sensitive Information

• Your email
• Unsecured paper files
• Your hard drive unencrypted
• Social networking sites
Level I - The Cloud

• The Cloud is not secure
• Do not store information in the cloud unless it is encrypted
Level I - Keep Sensitive Information Secure From Social Engineers

- Verify callers
- Do not respond to email scams, phishing, or suspicious phone calls requesting confidential company information or your own personal information.

- Remember the IRS will NEVER ask for your password over email.
Level I - Back-Up

• Regularly backing up your data is critical in case of a computer failure
  – Store your backup in a secure location
  – Secure your backup, lock it up, encrypt it.
  – Regularly verify you can restore from this backup.
Level I - Securing Your Password

- Password keepers such as KeePass or Last Pass
- Do not store on your monitor or under keyboard
- Use something easy to remember but hard to guess
- Follow password generation guidelines
  - CAPITALS
  - lowercase
  - numb3r5
  - $ymbo1s
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
  
  => BING01965bs!
Securing your home router

• Your home router is usually made by
  • Linksys, Netgear or D-Link

• Router is your key protector from outside cyber intruders
  • Provides a Firewall from outsiders to your inside home network

• Follow instructions to secure router
  • Ensure that your router is password protected
  • Choose Wi-Fi Protected Access - WPA2 security

• Review and Monitor Router Settings
  • Usually found in router manual instructions
  • Can always check by typing http://192.168.0.1 in browser
  • Ensure that router has not been reset by powering off/on
Parental Controls

• **Control/Filter Computer Content**
  • Install software such as WebWatcher

• **Control/Filter Phone Content**
  • Install software such as WebWatcher
  • Use parental controls from telecom provider such as Verizon

• **Control/Filter entire home network**
  • Install filtering software that connects to your router
  • Open DNS and others filter your entire network flow
  • Note that all your network traffic will go through OpenDNS!
Filtering your online content

- **Open DNS and other filtering tools**
  - Filter at the router level – block all computers and devices
  - Filter at the computer level by using various parental controls
  - Check out OpenDNS.com, now owned by Cisco

---

OpenDNS Family Shield
FREE
Preconfigured to block adult content — set it & forget it

OpenDNS Home
FREE
Our classic, free service with customizable filtering and identity theft protection

OpenDNS Home VIP
$19.95/year
OpenDNS Home package plus one year of usage stats & optional white-list mode
Level I - Web Browsing Safety

- Use anti-virus software on your computer
- Create and use strong passwords
- Beware of instant message links and e-mail attachments
- Protect yourself on all wireless networks
- Check the URL of a website to make sure it’s legitimate
- Ensure your web browser software and all plugins are up to date
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
Level I - 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 "mircosof.com" instead of "microsoft.com." These slight differences can be easy to miss, and that's what phishers are counting on.
Level I - 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.
Level I - 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
Level I - 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.

  [source](http://us.norton.com/security_response/spam.jsp)
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

• Report to FTC or ISP:
  – If you get spam that is phishing for information, forward it to spam@uce.gov.
  – 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.
  – 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.
Level I - Phishing

- **Agencies such as the IRS will NEVER ask you for your password over email**

- Social engineers will combine emails with phone calls

- **Subscribe to Phishing Alerts**
Don’t Fall For This

Sample message:

---------- Forwarded message ----------
From: notify admin <notifyhawaii.edu@gmail.com>
Date: Fri, 0ct 5, 2012 at 12:46 PM
Subject: notify Installment payments due
To:

This is an automated message to remind you of upcoming payment dates.

Installment payments are automatically scheduled when you sign up for
the payment plan and will be deducted from your designated account on
the scheduled payment dates. Be sure to have sufficient funds
available in your bank account or on your card.

======== PAYMENT PLAN DETAILS ========
Payment Plan --- [ Fall 2012 UH Payment Plan - Jul, Aug, Sep, Oct ]
Due Date --- [ 10/19/2012 ]
Amount Due --- [ $1,181.75 ]
Payment process---[ Send your payment details and receipt from western
union to notifyhawaii.edu@gmail.com]

==========================================

Please do not reply to this message, as it was sent from a notify-only
address that cannot accept incoming email.

-------------------------------------------
Digital Millennium Copyright Act (DMCA)
Level I - 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
• Downloading and sharing of copyrighted materials via peer-to-peer file sharing software / networks **WITHOUT LEGAL PERMISSION** from the copyright owner or agent

• BitTorrent, LimeWire, and Gnutella are examples of methods used for downloading large amounts of data from the Internet
Safe Social Networking Practices

Cybersecurity for all of us
Level I - Safe Social Networking Practices

• Limit personal information online
• Ensure information you post does not answer security questions (dog’s name, mothers maiden name)
• Check privacy settings to see who has access to online info
• Google yourself to see what people can piece together about you
Social Networking

• Do not post TOO MUCH INFORMATION!

• The Internet is FOREVER!
  – Whatever you post may circulate even AFTER you delete it

• New scams use social networking sites to get background personal information
Facebook Security

- [https://www.facebook.com/security](https://www.facebook.com/security)
Mobile Device Security
Level I - 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 aware when using location-aware services
Mobile Malware

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

• What can mobile malware do?
  – Sends out SMS messages
  – Destroys data on device
  – Can spread to computers to infect them when synced
Geotagging

• Pictures taken w/ a GPS-enabled smartphone “tags” each picture with the longitude & latitude of the location of the picture
Turning off Location Services

- iPhone
- Settings > Location Services

Location Services

Allow the apps below to determine your approximate location.

- Camera
- Compass
- foursquare
- Maps
- Twitterrific

An app that has requested your location within the last 24 hours will show the location services icon next to its name.
“Location-Aware” Services

www.groupon.com
Level I - 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
- Scan your computer for vulnerabilities and PII
- Use accounts and strong passwords
- Encrypt sensitive information
- Don’t install unknown software from unknown sites
- DO NOT SHARE your accounts/passwords
- Use password protected screen savers
Level I - Wireless & Public Computers

• Be cautious when using open wireless networks
  – Others using the network may be “sniffing” the network

• If you must use a public computer, change the password on the account accessed using a secure computer ASAP
Level II and III

• **Level II - Active Defense**
  - Actively monitor your networks and property
  - Proactive guidance, policies and training
  - Reward vigilance and safe computing practices
  - Watch out for exceptions and abnormal behavior

• **Level III - Neighborhood Watch**
  - Share common tactics and strategies with others
  - Obtain alerts from the crowd of small businesses
  - Actively report information security issues and concerns to authorities and other small businesses
Conclusion

• Homes and small businesses have security issues just as large businesses

• Lack of a cybersecurity culture impacts the ability to fight security problems

• Level I precautions can be done today. Level II and III require work!

• For further information email debasisb@hawaii.edu or http://maui.hawaii.edu/cybersecurity