Agenda

• What’s new in CyberSecurity?
• Levels of Cyber Training
  • I – Basic Hygiene
  • II - Active Defense
  • III – Neighborhood Watch
• Securing your Work
• Securing your Home
• Security your Life
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
Proposed Solutions...

Level 1 - Basic Hygiene

• Train family members in security
• Provide firewall security for entire home
• Make backup copies of important data
• Secure your Wi-Fi networks and 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
Secure your life: Medical Data

Cybersecurity for all of us
Medical Data

Medical Data is more prized than credit cards!
US and Canada cyber security agencies issued an alert last week regarding an increasing number of ransomware attacks against healthcare organizations. Five providers, in just the last month alone, have been infected with such computer viruses, and often they are forced to pay Bitcoin ransoms.

“Malicious software” infected the computer system at Alvarado Hospital Medical Center in San Diego last month. Two other hospitals, Chino Valley Medical Center and Desert Valley Hospital in Victorville, were also infected. Each of these infected parties is a Prime Healthcare Hospital.

In Indiana, hackers locked down King’s Daughters Health computer systems after compromising just one employee’s files with a ransomware virus. The hospital claimed in a statement that no patient data had been compromised in the attack.
Two California hospitals – Chino Valley Medical Center in Chino and Desert Valley Hospital in Victorville – have been attacked by hackers demanding a ransom.

The latest hit comes just a month after Hollywood Presbyterian paid hackers a $17,000 ransom to regain control over its computer systems and during the same week on the heels of ransomware attacks against Methodist Hospital in Henderson, Kentucky, and Ottawa Hospital in Ontario, Canada.
Secure your life: Identity Theft

Identity Theft Is On The Rise
What You Need To Know

IDentity Theft
Secure your life:
Identity Theft Protection

IDENTITY THEFT MONITORING

Reclaiming your identity can be costly, time consuming, and stressful. AAA helps safeguard your identity with comprehensive Identity Theft Monitoring.

ProtectMyID® Essential
ProtectMyID® Deluxe
Secure your life:
Identity Theft Protection

LifeLock Advantage™

$19.99/mo
$219.89 annually
(Plus Applicable Sales Tax)

Choose Advantage level monitoring if you:
- Have 2+ bank accounts
- Have savings to protect
- Monitor your finances

This plan helps resolve ID theft with:
- Up to $1 Million for lawyers & experts‡
- **$100,000** Lost Funds Reimbursement‡
  Coverage currently limited for NY and WA

Start Your Membership

LifeLock Ultimate Plus™

$29.99/mo
$329.89 annually
(Plus Applicable Sales Tax)

Choose our best membership plan if you:
- Have retirement and 401(k) investments
- Have higher net worth

This plan helps resolve ID theft with:
- Up to $1 Million for lawyers & experts‡
- **$1 Million** Lost Funds Reimbursement‡
  Coverage currently limited for NY and WA

Start Your Membership
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, letters…even personal visits to your work/home

- Subscribe to Phishing Alerts
Level I - Social Engineering

• 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.
Sample message:

---------- Forwarded message ----------
From: notify admin <notifyhawaii.edu@gmail.com>
Date: Fri, Oct 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.

---------------------------------------
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 – 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 - 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

http://www.lancelhoff.com
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](http://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.
Level 1 - 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 1 - Encryption

- Encrypting a Windows file, folder, and entire disk - BitLocker
  - [http://www.hawaii.edu/askus/1285](http://www.hawaii.edu/askus/1285)

- Encrypt your devices
  - Phone, Tablets, Laptops

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

```
EE0425C5A4CBA54318DABCEE996A2D244E1FDF26FA4424
FE992FB268CDB4B5AFE33D8FB46576BE647BEAC33C3CE0
3C2A9CD3D057115959DE709C3B839E949F928C30FD7DDE
1D7C410AD7C938FE2463978AC839E949F928C30FD7DDE
7B8C7ADA158053537191EF3F70839E949F928C30FD7DDE
FB8156535D9E7CDC43903CD613839E949F928C30FD7DDE
4F8031B047A5A7E505DB8E435F839E949F928C30FD7DDE
292F2744236B3160A625BE3725A7D87E8F09FBC7E39B70
B57BA53C31ABEB10B9E257942FA7D87E8F09FBC7E39B70
DA45CD5E898058B89E2A8C0BA5A7D87E8F09FBC7E39B70
F76B75C2A2080DED879F1EEC29A7D87E8F09FBC7E39B70
4DB29618A507685BA27166A152A7D87E8F09FBC7E39B70
```
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 - The Cloud

• The Cloud is not secure
• Do not store information in the cloud unless it is encrypted
Safe Social Networking
Level I - 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
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
Mobile Device Security

Cybersecurity for all of us
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

An app that has requested your location within the last 24 hours will show the location services icon next to its name.
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

- 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
Level 1: Backup

- 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.

[www.carbonite.com](http://www.carbonite.com)
Automatic, easy, cheap!
Level 1: 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:

Level 1: Password Techniques

- 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
  - scramble vowels – a=@, e=3, i=l, o=0, u=U
  - numb3r5
  - $ymb0l$
Creating a Strong Password

• Incorporate something memorable to you
• Replace letters with numbers or characters
• Example:
  – First dog’s name is Bingo => Bing0
  – You got him in 1965 => 1965
  – Black spots => bs
  – Add special characters => !
  ==> BING01965bs!
Or, scramble with letters/numbers
Debasis ==> 12D3b@$I$34
Maui ==> 12M@UI34
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](http://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

Cybersecurity for all of us
Level I - Wireless & Public Computers

• Be cautious when using open wireless networks – at Starbucks and McDonalds
  – 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 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.
Conclusion

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

• Lack of *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