http://www.scmagazineus.com/education-sector-most-affected-by-malware/article/180337/

Education sector most affected by malware

Angela Moscaritolo October 04, 2010

PRINT EMAIL REPRINT PERMISSIONS FONT SIZE: A | A | A

During the first six months of 2010, academia was the sector most impacted by malware, according to a report issued Monday by anti-virus firm Trend Micro.

The report, which covers cybercrime incidents from January to June, states that 44 percent of all malware infections hit schools and universities, which often have "complex, distributed and diverse infrastructures."

Information Security Open Forum

- National Cyber Security Awareness Month
- CSU Information Security Audit Updates:

  When will I be affected?
- Securing your wireless router at home.
- Personal firewall protection:

  Why it's smart to have a barrier between your computer and the Internet.

Wednesday, October 20, 2010
University Union 220

Terry Vahey, Sharon Anderson, Tim Schmidt, Mike Cook , Chris Call

CSU Information Security Audit

- **CSU Audit Fieldwork** — Sept to Dec 2009
- **CSU Audit Review/ Feedback to Campus** — Jan to July 2010
- **Cal Poly Audit Responses Due** — June to Nov 2010
- **Implementation of Cal Poly Standards** — Oct to Apr 2011
- **Self Assessments** — May 2011

CSU Information Security Audit

- CSU policies require the campus to establish Information Security Policies and Standards
- Scope: all campus departments
- Information Security Standards were developed by ITS and LAN Coordinator working groups
- ITS will work with LAN Coordinators and security representatives across campus as new standards, procedures, and guidelines are developed

Information Security Standards

- Information Security standards available now:
  - Computing Devices
  - Web Application Development
  - Network
  - Managing Computer Accounts
  - Cal Poly Passwords
  - Information Classification and Handling

Why Personal Wireless Access Points Aren't Allowed On Campus

- The Campus has implemented the CSU standardized wireless technology with coverage in all campus buildings and some outside common areas (e.g. Kennedy Library Atrium and the University Union Plaza).

- Non-standard wireless access points do not provide the security required by CSU Policy and University Standards.

- Traffic traversing the campus wireless network is not encrypted at this time. ITS is implementing an encrypted wireless solution (WPA-2 targeted for Winter 2011).

Wireless Vulnerability In Public

- What is a hotspot?
- Are you safe at hotspots?
- How do I stay safe at a hotspot??

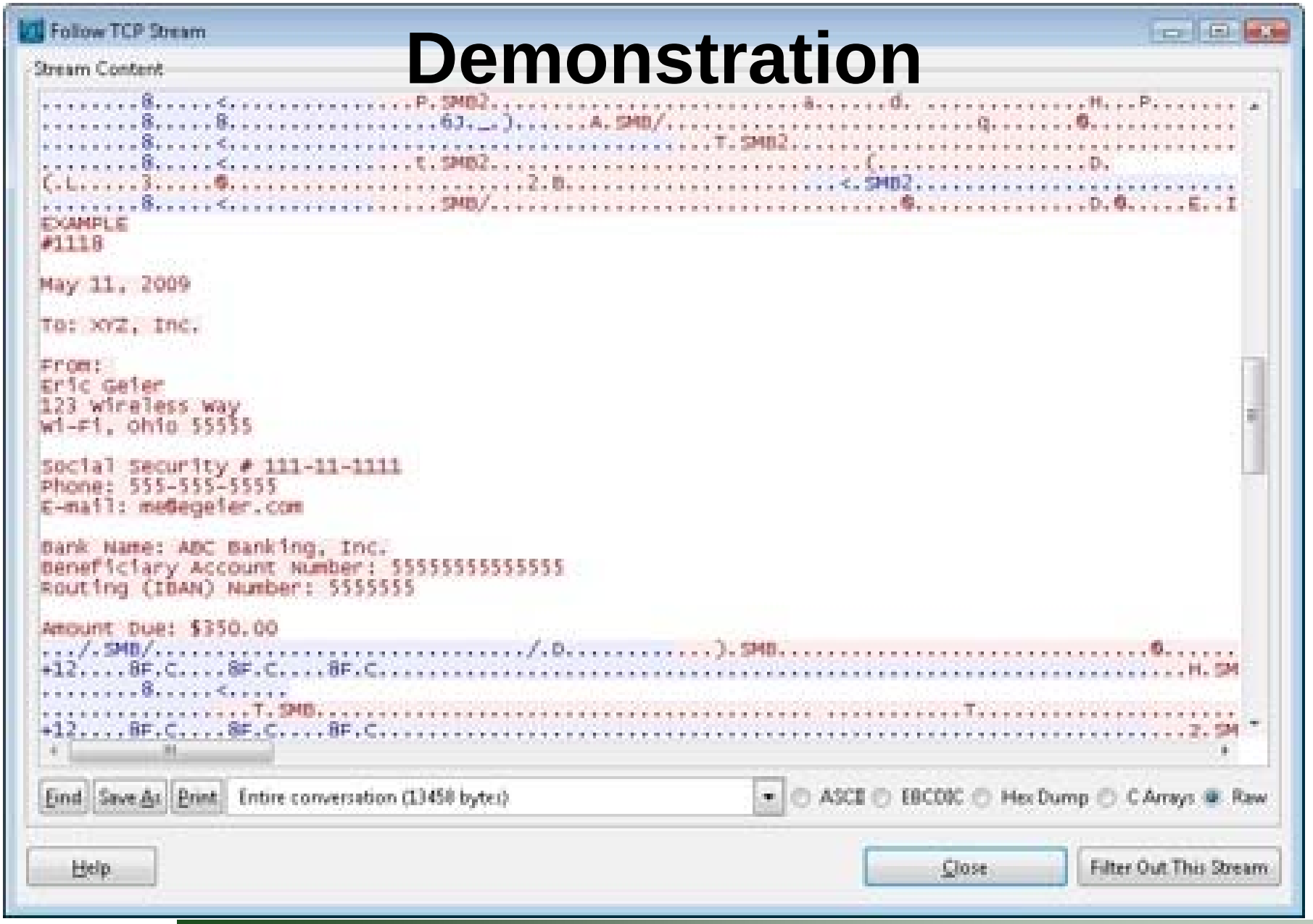
What Is A Hotspot?

- A hotspot is a site that offers Internet access over a wireless network. They can usually be found at locations such as:
  - Barnes & Nobles
  - Starbucks
  - Airports
  - College Campuses
  - Other public facilities

Are You Safe At Hotspots?

- Many hotspots are unsecured.
- In an unsecured hotspot, all the data you access over the network or internet is unencrypted and can easily be captured.
- This means other people can capture the data from your computer and see what you are browsing.
  - It does not matter what type of computer you have.
  - Capturing data out of the air has nothing to do with your operating system.

Demonstration



How Do I Stay Safe At A Hotspot?

- Best practices:
  - Only use encrypted hotspots.
  - Do not access information that you don't want the public to see.
  - Do not use email programs.
  - Do not use any programs that connect to the internet that may have sensitive data.
  - Avoid banking and online shopping.
  - Keep your computing devices patched.
  - Install a software firewall.

Wireless Vulnerability At Home

- I have my own wireless router and don't use a "hotspot"…thank goodness I'm safe!

Are You Safe At Home?

- For most people the answer is no.
  - Unless you have taken specific steps, your data may not be safe.

- Simply not using the wireless does not make you safe.
  - Almost all routers come with wireless access.
  - This means wired computers are still vulnerable unless you secure your router.

Are You Safe Out Of The Box?

- Internet providers do not secure your network when they install your equipment.
- Routers you buy at the store are not secure when you plug them in.
- Many setup wizards that come with your router are not sufficient enough to protect your data.

Demonstration

How Do I Stay Safe At Home?

- Completing the following steps will secure your router.
  - These steps are ordered so you will know what steps to take first.
  - They are also grouped in tiers based on industry recommendations, so you can decide how secure you want to make your router.
  - Please reference your router manufacturer for additional details and full instructions on how to complete these steps for your specific hardware.

Locking Down Your Network

- Tier 1 – “Locking the doors and windows”
  1. Keep your computing devices patched.
  2. Install software firewalls on all computers.
  3. Change the access password on your router.
     - This is the password used to change settings on your router.
  4. Turn off wireless access if you do not have wireless devices.
  5. Turn on wireless encryption.
     - This means you will need a password to access your wireless, and the data in the air will be encrypted.

Software Firewalls

- A firewall, like a home security system, only allows certain traffic through specified doors or ports.
- A personal firewall product will alert you or take one of many predetermined actions when someone tries to tamper with your computer.
- Personal firewalls are offered individually, or as part of an Internet Security Suite package.

What Is An Internet Security Suite?

- An Internet Security Suite is the next step up from standard Anti-Virus software.
- It includes additional protection such as:
  - Antivirus
  - Antispyware
  - Antimalware
  - Antiphishing
  - Antispam
  - Identity protection
  - Parental Controls
  - Software firewall
  - Bot protection
  - Network monitoring
  - Antirootkit

Internet Security Suites

PCWorld.com Recommended Internet Security Suites:

1. Symantec Norton Internet Security 2010
2. Kaspersky Lab Internet Security 2010
3. AVG Internet Security 9.0
4. PC Tools Internet Security 2010
5. BitDefender Internet Security 2010
6. Alwil Avast! Internet Security 5.0
7. McAfee Internet Security 2010
8. Panda Internet Security 2010
9. Webroot Internet Security Essentials 2010
10. Trend Micro Internet Security Pro 2010

Wireless Encryption

- What encryption should I choose?
  - This depends on your wireless devices.
  - You will need to identify all of your wireless devices and look in the documentation for each to determine what encryption types they support.
  - Choose the highest security you can based on the devices you have.
  - If you have older devices with low security options, it is preferable to replace the device rather than make your network more vulnerable to accommodate it.

Wireless Encryption

- Wireless Security Options:
  1. Wi-Fi Protected Access 2 (WPA2 Personal)
     - The latest in security technology.
     - The most secure and private Wi-Fi network.
  2. Wi-Fi Protected Access (WPA)
     - Improved authentication and encryption features from WEP.
  3. Wired Equivalent Privacy (WEP 128-bit or 64-bit)
     - Least secure and very easily cracked.
     - Significantly better than no encryption.
     - The 128-bit variant is preferable.

Locking Down Your Network

- Tier 2 – “Putting in a home security system”
  1. Complete all items in Tier 1.
  2. Enable MAC Address filtering.
     - A MAC Address is a unique identifier assigned to network cards.
     - MAC filtering lets you specifically choose which computers can access your wireless.
  3. Turn off remote access to the routers administration page.
     - This means you can only access the router administration page when physically connected to the router.
  4. Change your SSID.
     - This is the name or your wireless network.
     - Kind of like putting a home security sign on your lawn.

Locking Down Your Network

- Tier 3 – “Adding cameras and motion sensors”
  1. Complete all items in Tiers 1 & 2.
  2. Change the IP Address for your router & the range of IP Addresses it assigns.
  3. Limit the number of IP Addresses your router can assign to match the number of devices you have.
  4. Assign each device a specific IP Address.
  5. Disable SSID broadcasting.
     - This stops your router from broadcasting it’s name for people to connect to.

Locking Down Your Network

- Tier 4 – “How can I rival the Pentagon?”
  1. Complete all items in Tiers 1, 2 & 3.
  2. Turn off the ‘automatic’ feature on your software firewall and manually create all firewall rules.
  3. Turn off the wireless entirely when not in use.
  4. Position the router in a physically secure area.
  5. Think about purchasing a hardware firewall.

Questions?

Thank you for your participation!

Slides posted at http://security.calpoly.edu

Terry Vahey, tvahey@calpoly.edu, 756-7667
Sharon Anderson, sander17@calpoly.edu, 756-7745
Tim Schmidt, tschmidt@calpoly.edu, 756-2848
Mike Cook, macook@calpoly.edu, 756-7372
Chris Call, ccall@calpoly.edu, 756-7622