

Session 46



Information Security – Creating Awareness, Educating Staff, and Protecting Information

Chris Aidan, CISSP

Information Security Manager

Pearson

Topics Covered

- Data Privacy
- Spyware & Adware
- SPAM & SPIM
- Phishing
- Passwords
- Social Engineering
- Email & Chat Services
- Securing Workstations
- Data Backups
- Equipment Disposal
- Data Recovery Demo
- Data Disposal
- Access Rights
- Physical Security
- Emerging Threats
- Incident Response
- Creating Awareness
- Questions
- Useful Links

Why Security?

- Liability
- Privacy Concerns
- Copyright Violations
- Identity Theft
- Resource Violations
- Reputation Protection
- Meet Expectations
- Laws & Regulations

Understanding Threats

- What is valuable?
- What is vulnerable?
- What can we do to safeguard and mitigate threats?
- What can we do to prepare ourselves?
- Most believe they will win lottery before getting hit by malicious code

Keep Sensitive Data Private

Protecting Information like:

- Social Security Number
- Drivers license number
- Insurance numbers
- Passwords and PIN's
- Banking information

Terminology

- Hackers
 - white hat
 - grey hat
 - black hat
- DOS & DDOS
- 1337 (Leet) speak
- Warez
- Script kiddies

Spyware & Adware (Scumware)

- ❑ Spyware-Applications that monitor activity *without* express permission
- ❑ Adware-Applications that monitor activity *with* express permission
 - Read the EULA

- Some of the Web pages viewed
- The amount of time spent at some Web sites
- Response to GAIN Ads
- Standard web log information (excluding IP Addresses) and system settings
- What software is on the personal computer
- First name, country, city, and five digit ZIP code
- Non-personally identifiable information on Web pages and forms
- Software usage characteristics and preferences

Gator® eWallet



- The world's most popular digital wallet. The Gator eWallet automatically remembers login IDs/passwords and fills in online forms with just one click. No more lost passwords, and no more typing information such as address, email, credit card numbers, etc! And the Gator eWallet is completely secure. All your information is encrypted and stored on YOUR computer.

SPAM & SPIM

□ SPAM-

- Junk email

□ SPIM- SPAM has come to Instant Messaging

- Uncontrolled viewing (pop-up windows)
- Bot generated

Phishing

- ❑ **Phishing** is a computer scam that uses SPAM, SPIM & pop-up messages to trick us into disclosing private information (Social Security Number, Credit Cards, banking data, passwords, etc)
 - Often sent from someone that we “trust” or are in some way associated with us
 - Appears to be a legitimate website
 - Embedded in links emails & pop-up message
 - Phishing emails often contain spyware designed to give remote control to our computer or track our online activities

Passwords

- ❑ Select a good one
 - At least 7 characters
 - Mixture of upper and lowercase characters
 - Mixture of alpha and numeric characters
 - Don't use dictionary words
- ❑ Keep passwords safe
- ❑ Change them often
- ❑ Don't share or reuse passwords
- ❑ Two-factor authentication



Social Engineering

Social Engineering is the art of prying information out of someone else to obtain access or gain important details about a particular system through the use of deception

Email & Chat Services

- ❑ Email and chat are sent in clear text over the Internet
- ❑ Data can easily be captured and read by savvy computer users and systems administrators
- ❑ Safeguards should be put into place prior to using these programs for sending/receiving sensitive information like Social Security Numbers

Enhance Our Work Area Security

- ❑ Secure workstations
 - Lock our systems (Ctrl-Alt-Delete)
 - Shut down
 - Run up to date virus scanning software
 - Password protect files
 - Apply software patches
 - Install cable locks
 - Run a desktop firewall

Is Our Data Being Backed Up?

- Test backups
- Securely store backup media (offsite)
- Restrict access to who can perform restoration

Equipment Disposal

- What happens to old computer when they are replaced?
- Do those systems contain sensitive information?
- Several programs to securely remove data from computer systems are commercially available

Data Recovery



DEMO

Dumpster Diving

- We never know who is looking in our trash
- Shred sensitive documents
- Secure shred barrels, and make sure that proper handling procedures are in place

Access Rights

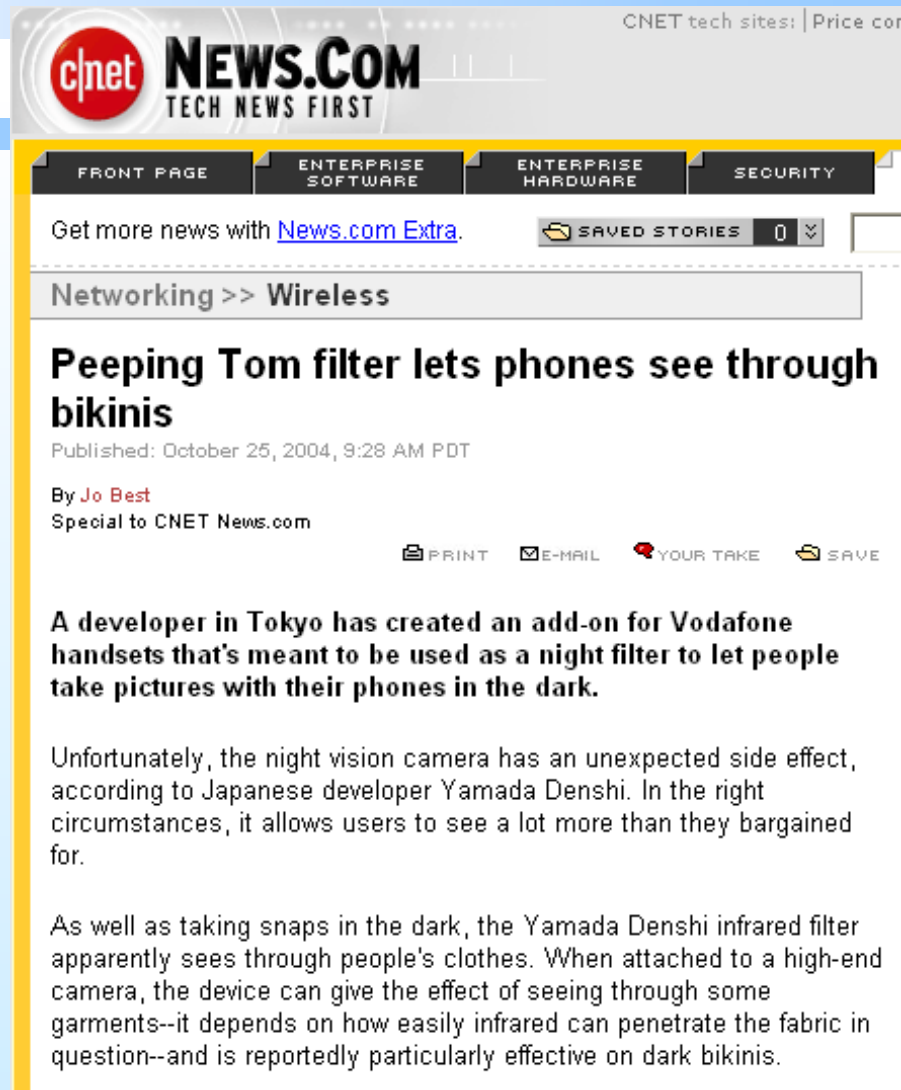
- Only allow access that is absolutely required
- Don't grant accounts based on the fact that access "may" be required
- Use least privilege access policies that state access will only be granted if required, not by default
- Are accounts removed and passwords changed when someone changes jobs or is terminated?
- Perform audits

Physical Security

- Who has access?
- Are sensitive documents secured?

Emerging Threats


- ❑ Wireless Technology
- ❑ Memory Devices-iPod, USB Keys, Coke cans,
- ❑ Camera phones
- ❑ P2P File Sharing



CNET tech sites | Price cor

cnet NEWS.COM
TECH NEWS FIRST

FRONT PAGE ENTERPRISE SOFTWARE ENTERPRISE HARDWARE SECURITY





Get more news with [News.com Extra](#).  **SAVED STORIES** 0

Networking >> Wireless

Peeping Tom filter lets phones see through bikinis

Published: October 25, 2004, 9:28 AM PDT

By [Jo Best](#)
Special to CNET News.com

 PRINT  E-MAIL  YOUR TAKE  SAVE

A developer in Tokyo has created an add-on for Vodafone handsets that's meant to be used as a night filter to let people take pictures with their phones in the dark.

Unfortunately, the night vision camera has an unexpected side effect, according to Japanese developer Yamada Denshi. In the right circumstances, it allows users to see a lot more than they bargained for.

As well as taking snaps in the dark, the Yamada Denshi infrared filter apparently sees through people's clothes. When attached to a high-end camera, the device can give the effect of seeing through some garments--it depends on how easily infrared can penetrate the fabric in question--and is reportedly particularly effective on dark bikinis.

Incident Response

- Do you know what to do and who to contact if a security breach occurs?

Recent News

CNN.com Internation

MEMBER SERVICES

SEARCH The Web CNN.com

- Home Page
- World
- U.S.
- Weather
- Business at cnnmoney
- Sports at 5l.com
- Politics
- Law
- Technology**
- Science & Space
- Health
- Entertainment
- Travel
- Education
- Special Reports

TECHNOLOGY

Hackers crack Purdue's computer system

Friday, October 22, 2004 Posted: 4:29 PM EDT (2029 GMT)

WEST LAFAYETTE, Indiana (AP) -- Someone gained unauthorized access to Purdue University's computer network, prompting school officials to urge all students, staff and faculty to change their passwords.

Purdue officials said that after the initial breach was detected, an investigation found that computers in several locations on the 38,000-student campus here had been accessed.

"The full extent of the problem is still being analyzed, but we think it is important to exercise caution, and the best action to take is for all users to change their passwords at this time," said Scott Ksander of Purdue's information technology office.

The police department was notified of the hacking Wednesday.

SERVICES

- Video
- E-mail Newsletters
- Your E-mail Alerts
- CNNtoGO
- Contact Us

SEARCH

Web CNN.com

Powered by **YAHOO!** search

CNET tech sites: | Price co

cnet NEWS.COM
TECH NEWS FIRST

FRONT PAGE | ENTERPRISE SOFTWARE | ENTERPRISE HARDWARE | SECURITY

Get more news with [News.com Extra](#) 0

Security >> Attacks

Hacker strikes university computer system

Published: October 19, 2004, 6:55 PM PDT

By Reuters

A computer hacker accessed names and Social Security numbers of about 1.4 million Californians after breaking into a University of California, Berkeley, computer system in perhaps over suffered by the school, officials

Students suspended for hacking Oxford network

Published: November 1, 2004, 6:06 AM PST

By Graeme Wearden
Special to CNET News.com

Two Oxford students have been suspended after admitting to gaining unauthorized access to the university's IT network.

Patrick Foster, 20, and Roger Waite, 21, claimed they had carried out the hack to expose security flaws. But on Friday a disciplinary hearing ruled that both should be "rusticated," or suspended--Foster until May 2005 and Waite until January 2005.

The pair's actions came to light in May when they wrote an article for The Oxford Student, a university newspaper, detailing their activities. They warned that using tools found through Google they had managed to view live CCTV footage, access information about the computer use of individual students and see their e-mail passwords.

but we have no idea if the (personal) ised," said Carlos Ramos, assistant lth and Human Services Agency.

e FBI were investigating, but the hacker

acker were being used by a UC Berkeley data on elderly people and individuals eniors to study the impact of wages on

Creating Awareness

- ❑ Educate staff
 - Train staff
 - Document processes and outline expectations
- ❑ Research potential candidates
 - Perform background & credit checks
- ❑ Track system changes
 - Audit system access
 - Audit system changes
- ❑ Create & communicate policies:
 - Define document and system disposal processes
 - Define backup procedures
 - Define clean work area policies
 - Define computer usage policies

Be Aware

- Report anything “strange”
- Don't give private information out
- Properly dispose of sensitive information
- Run up to date virus protection & software
- Ask questions

Useful Links

National Cyber Security Alliance

<http://www.staysafeonline.info/>

National Institute of Standards and Technology:

<http://csrc.nist.gov/sec-cert/>

Recent News

[High Profile Computer Compromise](#)

[High Profile Computer Compromise](#)

A lot of Schools have great security resource pages, for example UC Davis and the University of Iowa websites:

<http://security.ucdavis.edu/security101.cfm>

<http://cio.uiowa.edu/itsecurity/>

Example Software References

Some various applications mentioned in the presentation*

- ❑ Email Security
 - PGP <http://www.pgp.com>
 - Instant Messaging Security
 - Simp <http://www.secway.fr/products/all.php?PARAM=us,text>
 - Adware & Spyware Removal Applications
 - Ad-aware <http://www.lavasoftusa.com/software/adaware/>
 - Spybot <http://www.safer-networking.org/en/download/>
- ❑ Secure File Deletion
 - Secure Delete
<http://www.sysinternals.com/ntw2k/source/sdelete.shtml>
- ❑ System Disposal
 - Secure Hard Drive cleaning
http://www.accessdata.com/Product07_Overview.htm

Sample Policies

❑ Developing Security Policy

- <http://www.sans.org/rr/papers/50/919.pdf>

❑ Acceptable Use

- http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

Questions?

Please fill out the session evaluations & thank you for attending this session