



WSU IT Security Office

Computer Security Awareness

Objectives

- Provide an overview of policies
- Examples of threats
- Your responsibilities
- Resources

WSU Strategic Goals

- Offer the best undergraduate experience in a research university
- Nurture a world-class environment for research, scholarship, graduate education, the arts, and engagement

WSU Strategic Goals

- Create an environment of trust and respect in all we do
- Develop a culture of shared commitment to quality in all of our activities

Computer Security Issues at WSU

- Inappropriate Use
- Copyright Violations
- Physical PC security
- Weak Passwords
- No Software Updates
- SPAM
- Phishing
- Confidentiality
- Privacy
- Viruses

Federal Laws

- **FERPA** – Family Educational Rights and Privacy Act (1974)
- **DMCA** - The Digital Millennium Copyright Act (1998)
- **GLBA** – Gramm-Leach-Bliley Act (1999)
- **HIPAA** – Health Insurance Portability and Accountability Act (2000)

State Laws

- (RCW) Revised Code of Washington
- (WAC) Washington Administrative Code

State Ethics Law

- RCW 42.52 -ETHICS IN PUBLIC SERVICE
 - RCW 42.52.160 Use of persons, money, or property for private gain
 - RCW 42.52.180 Use of public resources for political campaigns
- WAC 292-110-010 Use of state resources.

Washington State University

- Business Policies and Procedures
- Executive Policy Manual

Computer & Network Policies

- Electronic Publishing Policy – EP4
- University Data Policies – EP8
- Wireless LAN Policy – EP13
- University Antivirus Policy – EP14
- University Network Policies – EP16
- Computer and Network User Identification and Password Policy– EP18
- University Domain Name Policy – EP21
- University Electronic Correspondence Policy – EP23

University Data Policies

-- WSU Executive Policy #8 --

Data are valuable institutional assets of Washington State University:

- Data Administration
 - Management responsibility for University data
- Data Access
 - Inquiry and download access to University data

University Data Policies

-- WSU Executive Policy #8 --

- Data Usage
 - Appropriate use and release of University data
- Data Maintenance
 - Upkeep of University data
- Data Security
 - Physical protection of University data

University Data Policies

-- WSU Executive Policy #8 --

- **Public Data**
 - of interest to the general public and for which there is no University business need or legal reason to limit access
- **Non-Public Data**
 - not appropriate or available for general public use
- **Confidential Data**
 - restricted for legal or other University business reasons

Data Breaches

- ChoicePoint – 145,000 records
- Bank Of America – 1,200,000 records
- Time Warner – 600,000 records
- CitiFinancial – 3,900,000 records
- US Dept of Agriculture – 350,000 records
- US Dept of Veterans Affairs – 28,600,000 records

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Your Responsibilities

As a user of Washington State University Information Technology Resources, it is your responsibility to ***help in the protection and proper use*** of our information and technology assets.

Appropriate Use Policy

-- *WSU Executive Policy #4*

WSU's computer resources, information technologies, and networks may be used in support of *academic instruction, research, public service and administrative functions of the university.*

Inappropriate Use

- Violating federal, state or local laws
- Violating WSU policies
- Tampering with WSU resources
- Compromising privacy
- Unauthorized access
- Obscene material
- Violating copyright or trademarks
- Personal or commercial business activities
- Political activities
- Unsolicited email (SPAM)
- Interfering with others' use

Inappropriate Use - Copyright

- Assume ***everything*** found on the network or web is protected by copyright unless explicitly stated otherwise
- Text, images, music and movies
- Peer-to-peer file sharing almost always involves copyrighted materials

Inappropriate Use - Copyright

- Downloading or distributing copyrighted material is a violation of federal and state laws, and of WSU policies
- Unlicensed software installed on WSU machines also violates copyright law

Consequences of Copyright Infringement

If copyright infringement is detected on a faculty or staff member's computer, the offense will be handled through Human Resource Services in accordance with applicable policies. Some cases may warrant termination of employment, or come under the jurisdiction of outside agencies.

Most Common Security Mistakes

- Leaving your computer on, unattended
- Poor password management
- Not using anti-virus software
- Out of date software patches
- Opening unexpected email attachments

Physical Security

All computers are common targets for thieves.

- Lock your door
- Use a password protected screen saver
- Lock up your Laptop
- Remember Removable Media

Passwords

Weak Passwords are one of the vulnerabilities most frequently targeted by someone trying to break into a system.

Computer and Network User Identification and Password Policy

-- *WSU Executive Policy #18*

- User IDs shall be assigned to individual users
- Passwords are considered *confidential* and *shall not be shared or transferred to others*
- Passwords should not be written down where anyone else can find them

Executive Policy #18

- Minimum length 8 characters
- Combination of upper- and lower-case letters, numbers and special characters
- Change your password at least once a semester
- Choose a password that cannot be guessed easily
- Do not log in with a stored password

Password Construction

License Plate Technique:

“To be or not to be?” = 2BRnot2B?

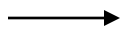
Pass Phrase Technique:

“This May Be One Way To Remember”
becomes:

"TmB1w2R!" or "Tmb1W>r"

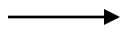
Compromised Passwords

- Network ID\AD
- UNIX Accounts
- AIS Accounts



Call the PhoneDesk
335-3663

Local Machine



- Call System Administrator
- Contact the IT Security Office

University Anti-Virus Policy

-- WSU Executive Policy #14

Anti-Virus software is *required*.

- Keep Anti-virus definitions up-to-date
- Scan ALL incoming files
- Contact your Systems Administrator,
or the
Technical Assistance Center (335-5396)

Spyware

- Spyware, installed on your computer without your consent, monitors or controls your computer use
- Be wary of “free” software
- Use Spyware detection and removal tools periodically
- Install a personal firewall to reduce the risk of security exposures

Spam

Annoying and “clogs” email servers

- 70-85% of email incoming to WSU is Spam
- Often financial offers
- Delete Spam messages and attachments
- Don't respond to “Take me off your list”

WSU Daily Virus Statistics

Viruses caught by the Barracudas, 2/4/2007

Total: 13836

Count	Virus name
4398	Trojan.Downloader.Tibs.Gen
2930	HTML.Phishing.Bank-627
2683	HTML.Phishing.Bank-1019
649	HTML.Phishing.Bank-1075
315	HTML.Phishing.Bank-473
262	HTML.Phishing.Bank-164
260	HTML.Phishing.Auction-226
241	HTML.Phishing.Auction-113
139	HTML.Phishing.Bank-629
121	HTML.Phishing.Bank-520
118	HTML.Phishing.Bank-1087
107	HTML.Phishing.Bank-1104
91	HTML.Phishing.Pay-36
91	HTML.Phishing.Auction-258
89	HTML.Phishing.Bank-362
84	Worm.SomeFool.Gen-2
77	HTML.Phishing.Pay-38

More than 120 items

Phishing

Phishing is an automated way of tricking a person into disclosing information under false pretenses, often through the Web or e-mail.

Phishing Example – Email Redirect

Sent: Wednesday, September 12, 2001 6:17 AM
Subject: Account Alert

Dear Valued Member,

According to our Terms of Service, you are required to confirm your account by the following link, or it will be suspended within 24 hours due to security reasons.

<http://www.wsu.edu/confirm.php?account=connectsupport@wsu.edu>

After following the instructions in the sheet, your account will continue to function as normal.

We apologize for any inconvenience.

Sincerely, Wsu Abuse Department

http://161.246.71.20/Confirmation_sheet.pif = (Ladkrabang, Bangkok)

Your Responsibilities

- **OS** (Linux, Macintosh, Windows)
- **Browser** (Firefox, Internet Explorer, Opera)
- **Applications** (Office, Acrobat, RealPlayer)
- **Anti-Virus** (Symantec, McAfee, AVG)

Contact Information

For questions about security or to report a security incident, contact:

- Your local Systems Administrator
- IT Security Office:
509-335-3900 or email abuse@wsu.edu