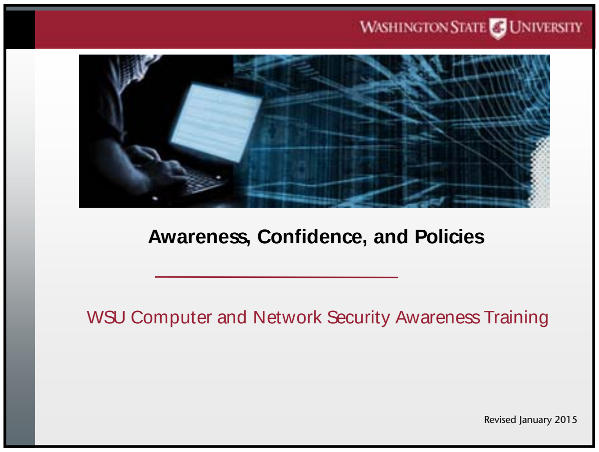
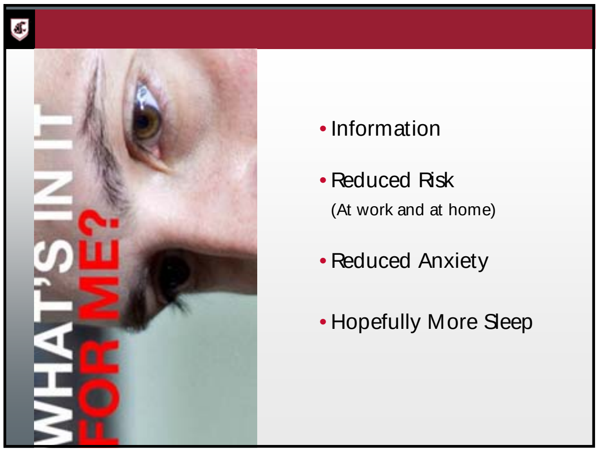


WASHINGTON STATE UNIVERSITY

Awareness, Confidence, and Policies

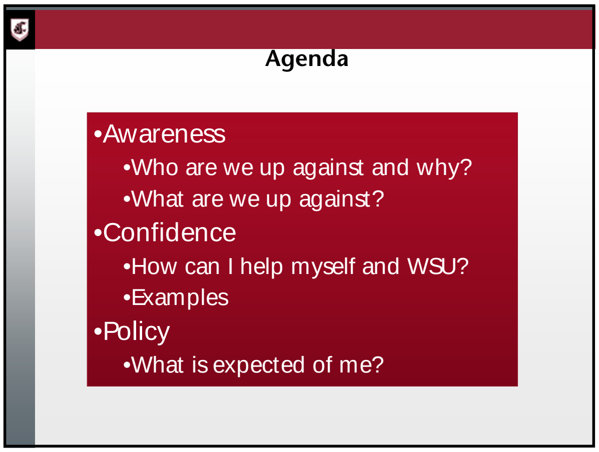
WSU Computer and Network Security Awareness Training

Revised January 2015



WHAT'S IN IT FOR ME?

- Information
- Reduced Risk
  (At work and at home)
- Reduced Anxiety
- Hopefully More Sleep



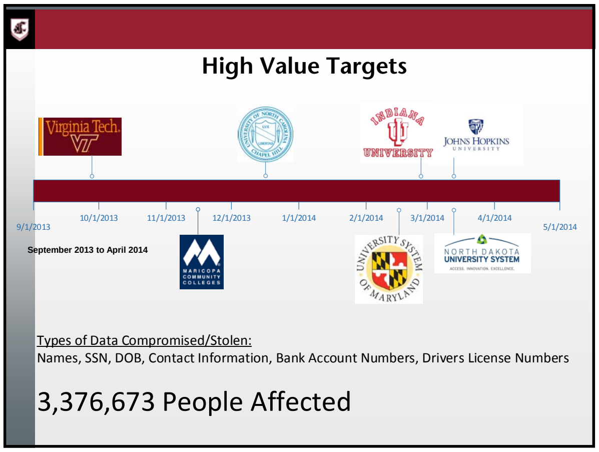
Agenda

- Awareness
  - Who are we up against and why?
  - What are we up against?
- Confidence
  - How can I help myself and WSU?
  - Examples
- Policy
  - What is expected of me?

Awareness

Who are we up against and why?

- Recent Headlines
- Humans as Adversaries
- Our Digital Assets



High Value Targets

Types of Data Compromised/Stolen:
Names, SSN, DOB, Contact Information, Bank Account Numbers, Drivers License Numbers

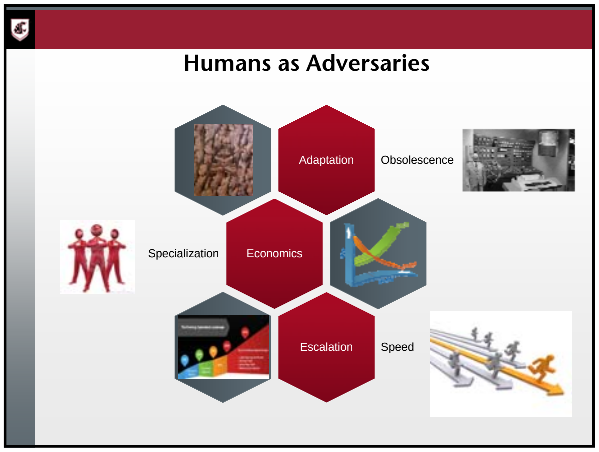
3,376,673 People Affected

WSU's Environment

- 9.4 Trillion Security-Relevant Events per Day

In the Last 6 Months at WSU:

- Server Compromises
- PCI-Related Compromises (Credit/Debit Card)
- Hundreds of Workstation Compromises
- Dozens of Compromised Email Accounts
- Dozens of Compromised VPN Accounts



Humans as Adversaries

Adaptation

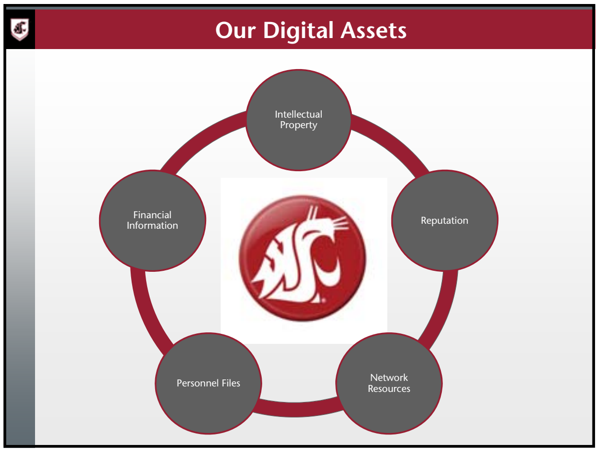
Obsolescence

Specialization

Economics

Escalation

Speed



Our Digital Assets

Intellectual Property

Reputation

Network Resources

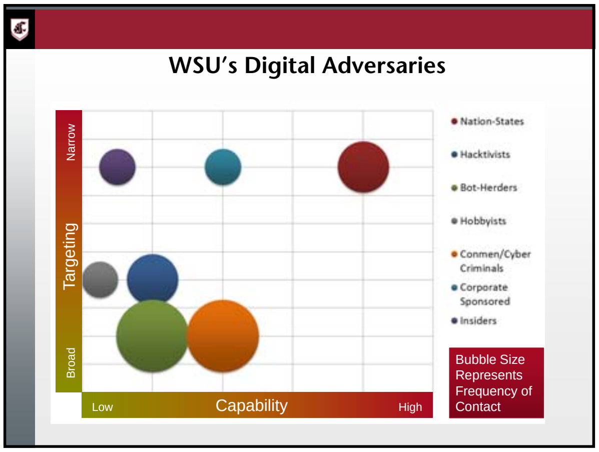
Personnel Files

Financial Information

Awareness

Who are we up against and why?

- WSU's Digital Adversaries



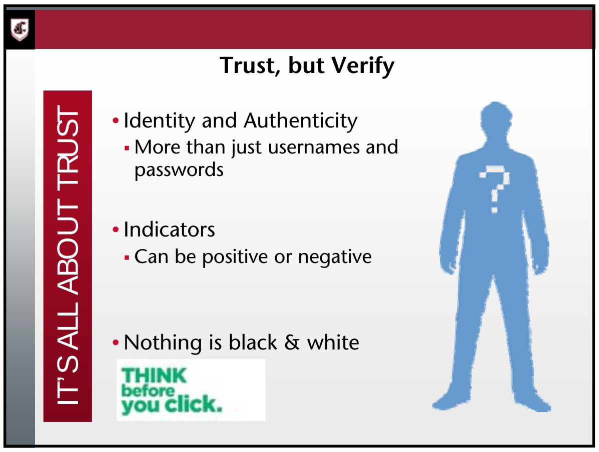
WSU's Digital Adversaries

Bubble Size Represents Frequency of Contact

Confidence

How can I help myself and WSU?

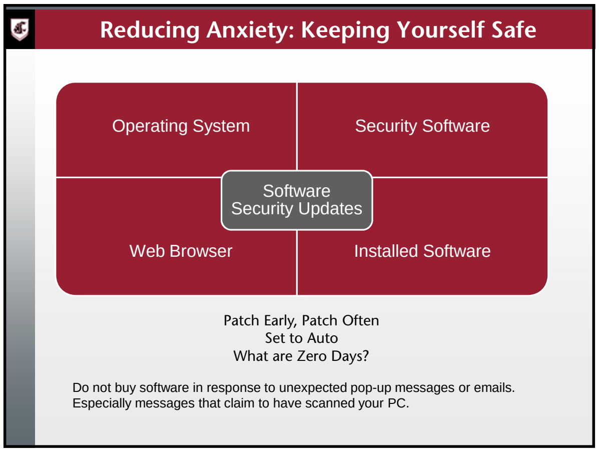
- Trust, but Verify
- Reducing Anxiety: Keeping Yourself Safe
- Reducing Risk: Keeping WSU Safe
- What About the Cloud?



Trust, but Verify

IT'S ALL ABOUT TRUST

- Identity and Authenticity
  - More than just usernames and passwords
- Indicators
  - Can be positive or negative
- Nothing is black & white



Reducing Anxiety: Keeping Yourself Safe

Operating System

Security Software

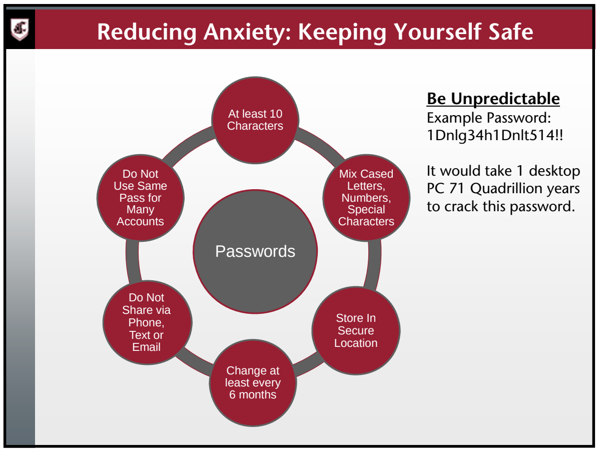
Software Security Updates

Web Browser

Installed Software

Patch Early, Patch Often
Set to Auto
What are Zero Days?

Do not buy software in response to unexpected pop-up messages or emails. Especially messages that claim to have scanned your PC.



Reducing Anxiety: Keeping Yourself Safe

Passwords

At least 10 Characters

Mix Cased Letters, Numbers, Special Characters

Store In Secure Location

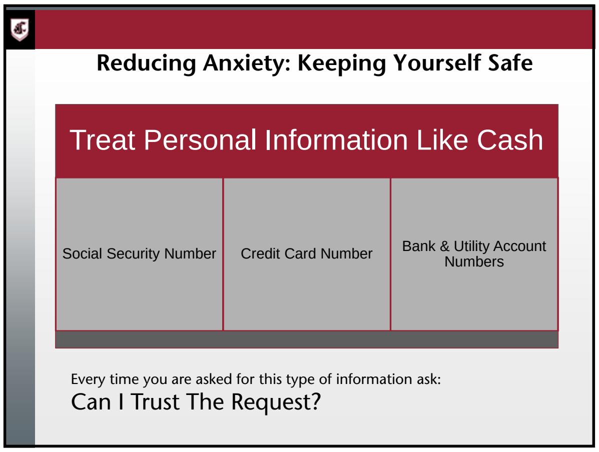
Change at least every 6 months

Do Not Share via Phone, Text or Email

Do Not Use Same Pass for Many Accounts

Be Unpredictable
Example Password:
1Dnlg34h1Dnlt514!!

It would take 1 desktop PC 71 Quadrillion years to crack this password.



Reducing Anxiety: Keeping Yourself Safe

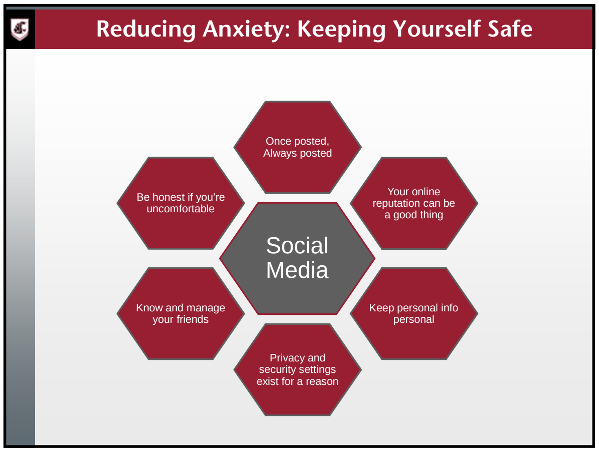
Treat Personal Information Like Cash

Social Security Number

Credit Card Number

Bank & Utility Account Numbers

Every time you are asked for this type of information ask:
Can I Trust The Request?



Reducing Anxiety: Keeping Yourself Safe

Social Media

Once posted, Always posted

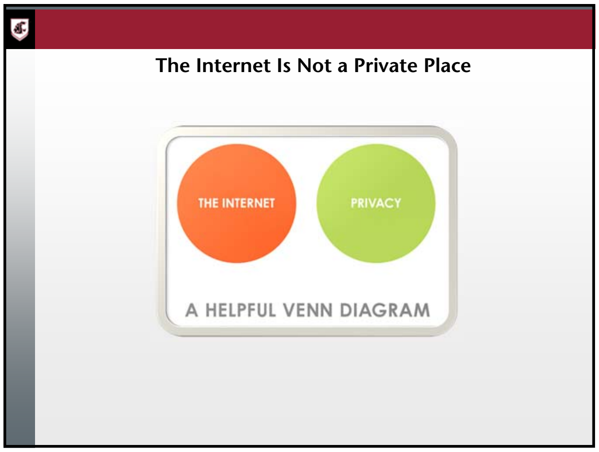
Your online reputation can be a good thing

Keep personal info personal

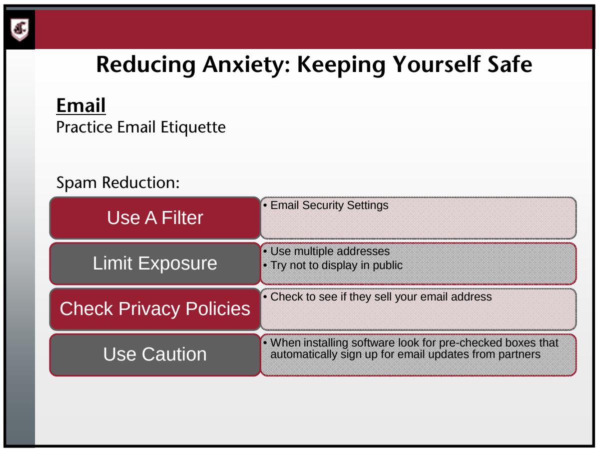
Privacy and security settings exist for a reason

Know and manage your friends

Be honest if you're uncomfortable



The Internet Is Not a Private Place



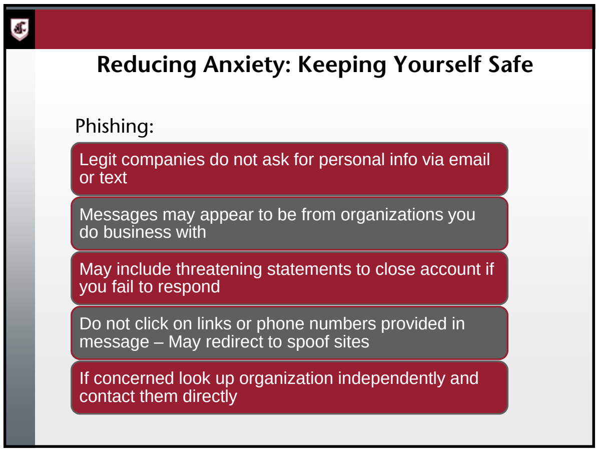
Reducing Anxiety: Keeping Yourself Safe

Email

Practice Email Etiquette

Spam Reduction:

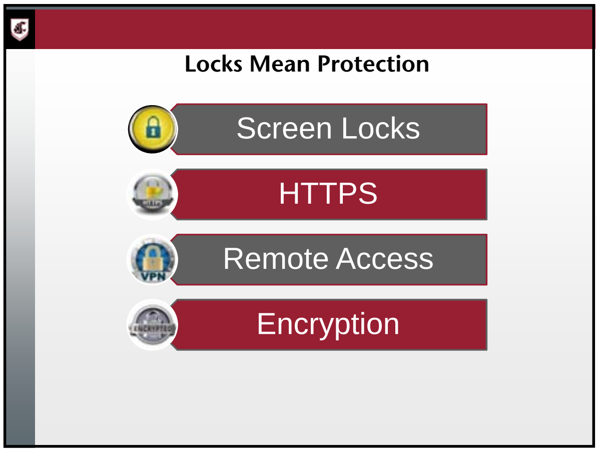
Use A Filter	• Email Security Settings
Limit Exposure	• Use multiple addresses • Try not to display in public
Check Privacy Policies	• Check to see if they sell your email address
Use Caution	• When installing software look for pre-checked boxes that automatically sign up for email updates from partners



Reducing Anxiety: Keeping Yourself Safe

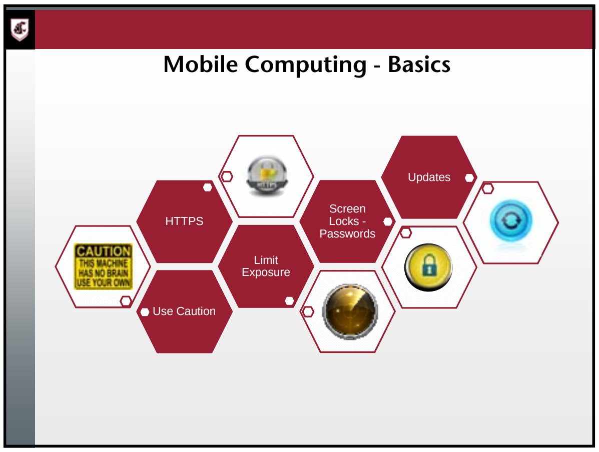
Phishing:

- Legit companies do not ask for personal info via email or text
- Messages may appear to be from organizations you do business with
- May include threatening statements to close account if you fail to respond
- Do not click on links or phone numbers provided in message – May redirect to spoof sites
- If concerned look up organization independently and contact them directly

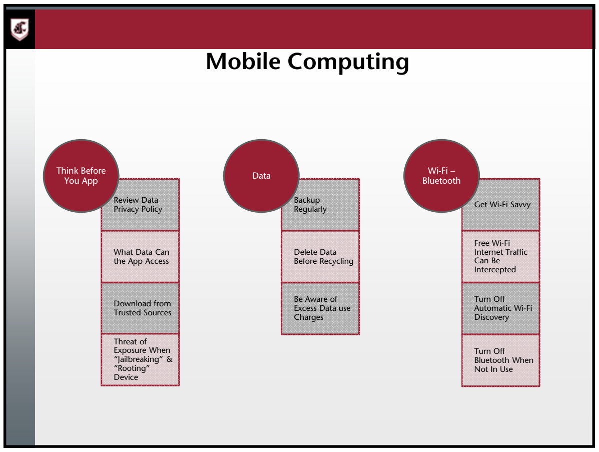


Locks Mean Protection

- Screen Locks
- HTTPS
- Remote Access
- Encryption



Mobile Computing - Basics

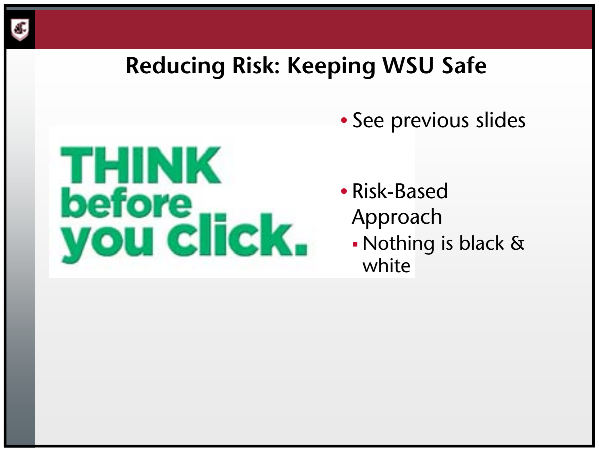


Mobile Computing

Think Before You App
- Review Data Privacy Policy
- What Data Can the App Access
- Download from Trusted Sources
- Threat of Exposure When “Jailbreaking” & “Rooting” Device

Data
- Backup Regularly
- Delete Data Before Recycling
- Be Aware of Excess Data use Charges

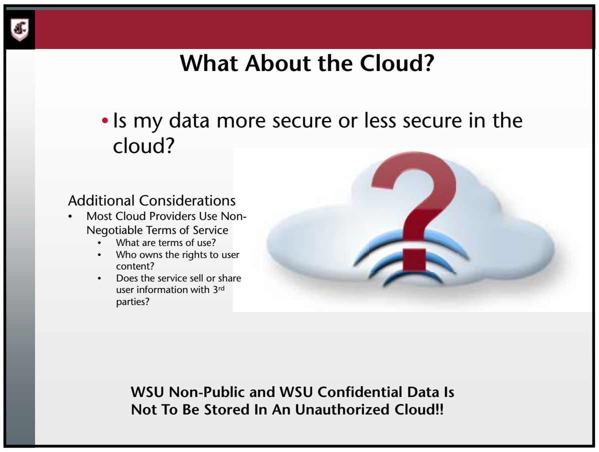
Wi-Fi – Bluetooth
- Get Wi-Fi Savvy
- Free Wi-Fi Internet Traffic Can Be Intercepted
- Turn Off Automatic Wi-Fi Discovery
- Turn Off Bluetooth When Not In Use



Reducing Risk: Keeping WSU Safe

THINK
before
you click.

- See previous slides
- Risk-Based Approach
  - Nothing is black & white



What About the Cloud?

- Is my data more secure or less secure in the cloud?

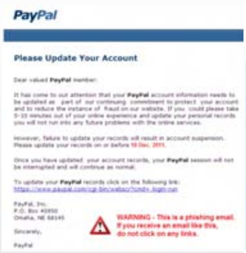
Additional Considerations
- Most Cloud Providers Use Non-Negotiable Terms of Service
  - What are terms of use?
  - Who owns the rights to user content?
  - Does the service sell or share user information with 3rd parties?

WSU Non-Public and WSU Confidential Data Is Not To Be Stored In An Unauthorized Cloud!!

Confidence

Examples

Phishing



Please Update Your Account

Dear valued **PayPal** member:

It has come to our attention that your **PayPal** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online services.

However, failure to update your records will result in account suspension. Please update your records on or before 10 Dec. 2011.

Once you have updated your account records, your **PayPal** session will not be interrupted and will continue as normal.

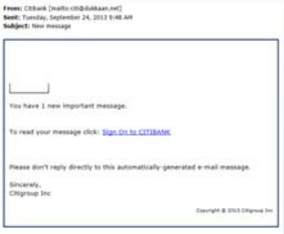
To update your **PayPal** records click on the following link:
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

PayPal, Inc.
P.O. Box 45950
Omaha, NE 68145

Sincerely,

PayPal

WARNING - This is a phishing email.
If you receive an email like this,
do not click on any links.



From: Citibank [mailto:citi@dukkaan.net]
Sent: Tuesday, September 24, 2013 9:48 AM
Subject: New message

You have 1 new important message.

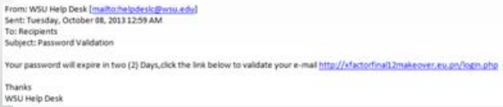
To read your message click: Sign On to CITIBANK

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,
Citigroup Inc

Copyright © 2013 Citigroup Inc

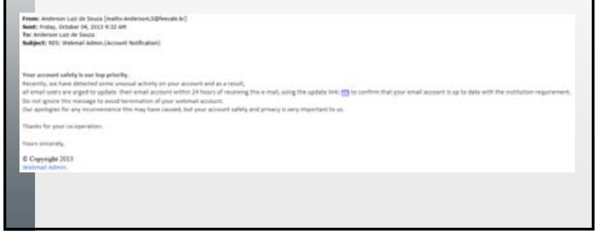
Spear-Phishing



From: WSU Help Desk [mailto:helpdesk@wsu.edu]
Sent: Tuesday, October 08, 2013 12:59 AM
To: Recipients
Subject: Password Validation

Your password will expire in two (2) Days,click the link below to validate your e-mail http://xfactorfinal12makeover.eu.pn/login.php

Thanks
WSU Help Desk



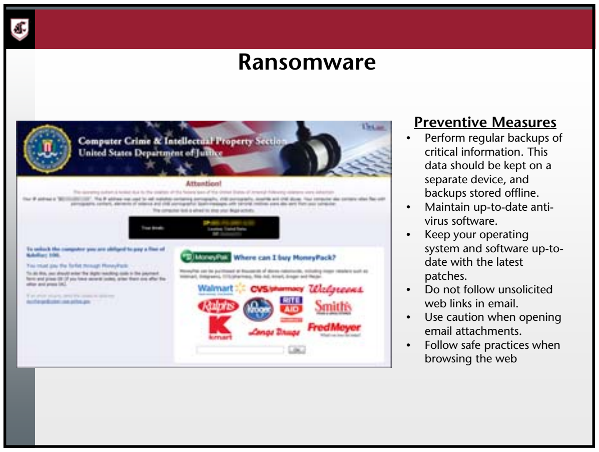
From: Anderson Luiz de Souza [mailto:Anderson.LS@feevale.br]
Sent: Friday, October 04, 2013 9:32 AM
To: Anderson Luiz de Souza
Subject: RES: Webmail Admin.(Account Notification)

Your account safety is our top priority.
Recently, we have detected some unusual activity on your account and as a result,
all email users are urged to update their email account within 24 hours of receiving this e-mail, using the update link: ITS to confirm that your email account is up to date with the institution requirement.
Do not ignore this message to avoid termination of your webmail account.
Our apologies for any inconvenience this may have caused, but your account safety and privacy is very important to us.

Thanks for your co-operation.

Yours sincerely,

© Copyright 2013
Webmail Admin.

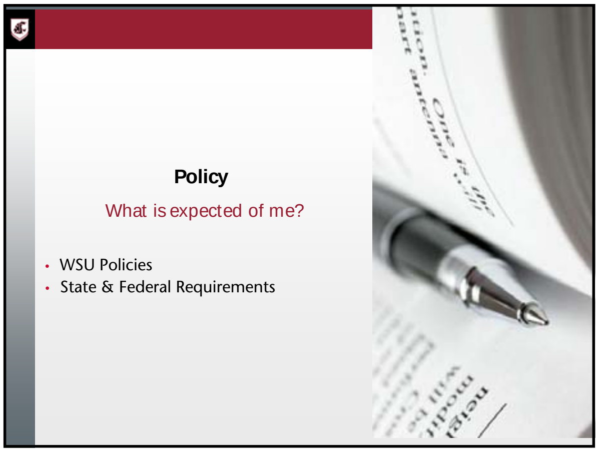


Ransomware

Computer Crime & Intellectual Property Section
United States Department of Justice
Attention!
MoneyPak
Where can I buy MoneyPack?
Walmart
CVS/pharmacy
Walgreens
Ralphs
Kroger
RITE AID
Smith's
Kmart
Longs Drugs
FredMeyer

Preventive Measures

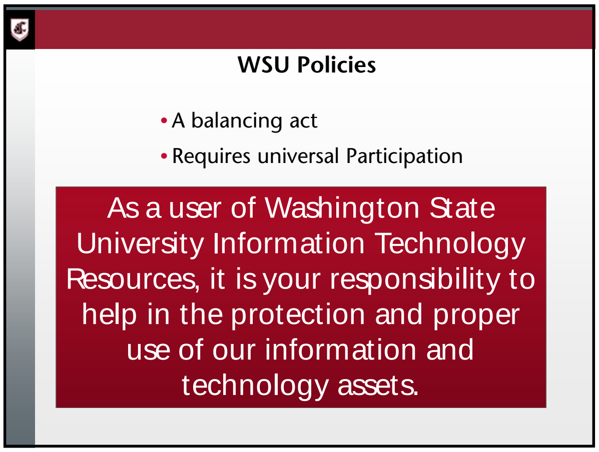
- Perform regular backups of critical information. This data should be kept on a separate device, and backups stored offline.
- Maintain up-to-date anti-virus software.
- Keep your operating system and software up-to-date with the latest patches.
- Do not follow unsolicited web links in email.
- Use caution when opening email attachments.
- Follow safe practices when browsing the web



Policy

What is expected of me?

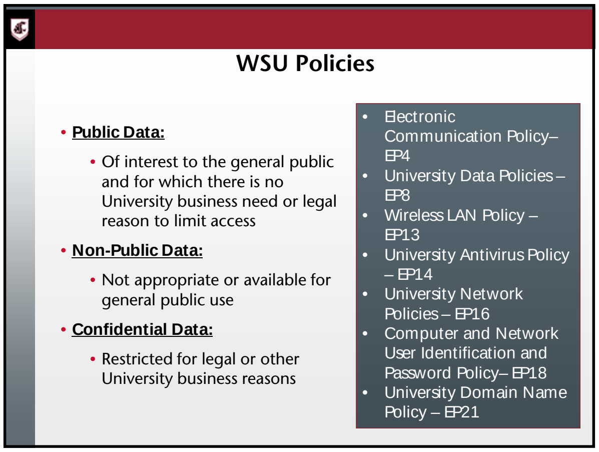
- WSU Policies
- State & Federal Requirements



WSU Policies

- A balancing act
- Requires universal Participation

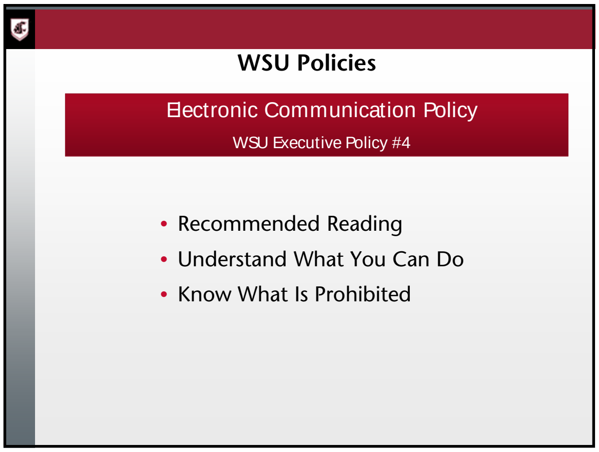
As a user of Washington State University Information Technology Resources, it is your responsibility to help in the protection and proper use of our information and technology assets.



WSU Policies

- **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

- Electronic Communication 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

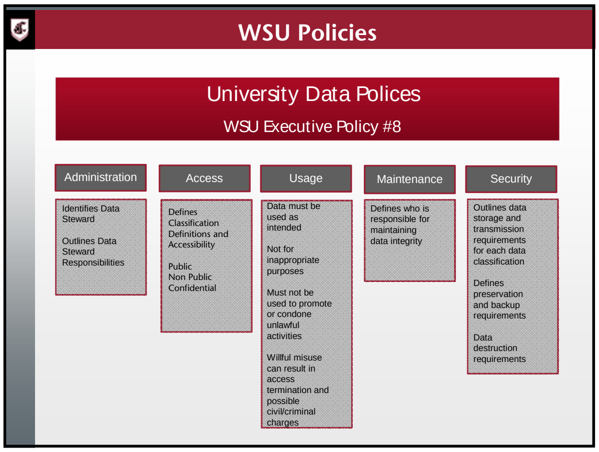


WSU Policies

Electronic Communication Policy

WSU Executive Policy #4

- Recommended Reading
- Understand What You Can Do
- Know What Is Prohibited

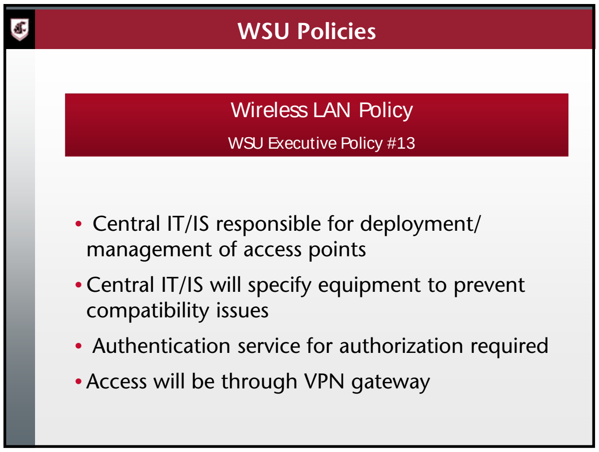


WSU Policies

University Data Polices

WSU Executive Policy #8

Administration	Access	Usage	Maintenance	Security
Identifies Data Steward Outlines Data Steward Responsibilities	Defines Classification Definitions and Accessibility Public Non Public Confidential	Data must be used as intended Not for inappropriate purposes Must not be used to promote or condone unlawful activities Willful misuse can result in access termination and possible civil/criminal charges	Defines who is responsible for maintaining data integrity	Outlines data storage and transmission requirements for each data classification Defines preservation and backup requirements Data destruction requirements

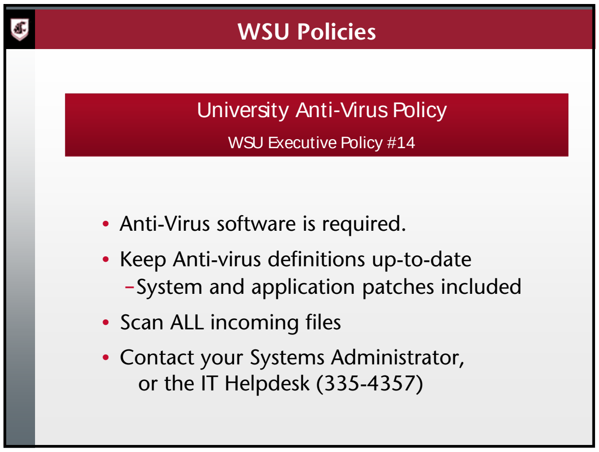


WSU Policies

Wireless LAN Policy

WSU Executive Policy #13

- Central IT/IS responsible for deployment/ management of access points
- Central IT/IS will specify equipment to prevent compatibility issues
- Authentication service for authorization required
- Access will be through VPN gateway

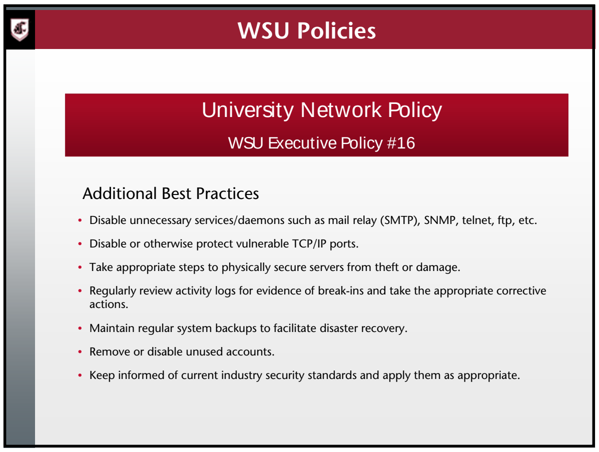


WSU Policies

University Anti-Virus Policy

WSU Executive Policy #14

- Anti-Virus software is required.
- Keep Anti-virus definitions up-to-date
  - System and application patches included
- Scan ALL incoming files
- Contact your Systems Administrator, or the IT Helpdesk (335-4357)



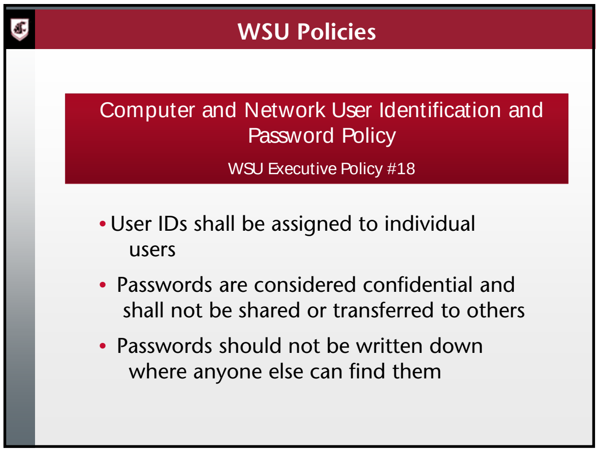
WSU Policies

University Network Policy

WSU Executive Policy #16

Additional Best Practices

- Disable unnecessary services/daemons such as mail relay (SMTP), SNMP, telnet, ftp, etc.
- Disable or otherwise protect vulnerable TCP/IP ports.
- Take appropriate steps to physically secure servers from theft or damage.
- Regularly review activity logs for evidence of break-ins and take the appropriate corrective actions.
- Maintain regular system backups to facilitate disaster recovery.
- Remove or disable unused accounts.
- Keep informed of current industry security standards and apply them as appropriate.

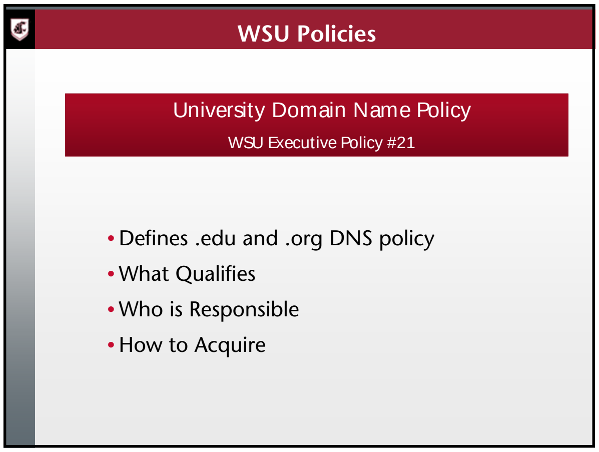


WSU Policies

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

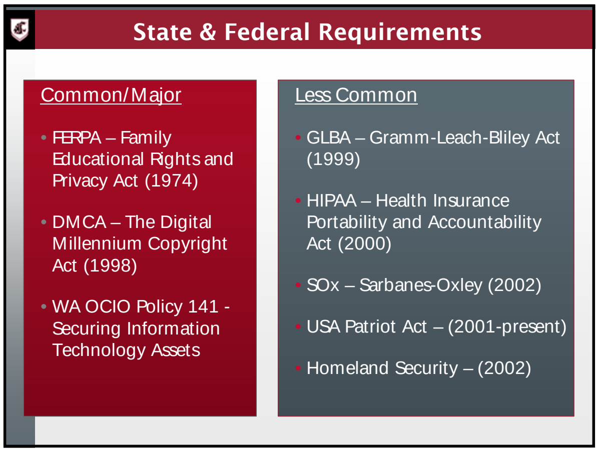


WSU Policies

University Domain Name Policy

WSU Executive Policy #21

- Defines .edu and .org DNS policy
- What Qualifies
- Who is Responsible
- How to Acquire



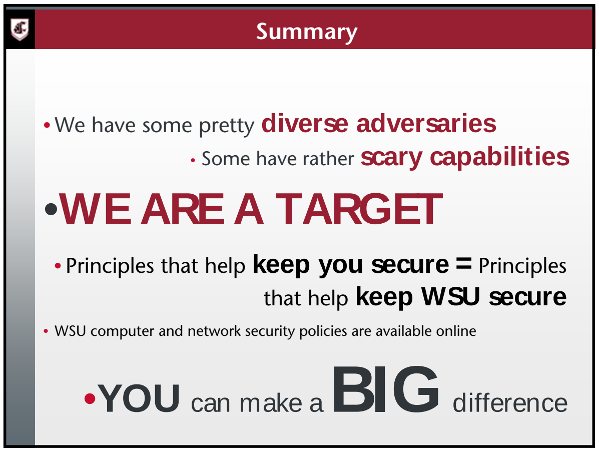
State & Federal Requirements

Common/Major

- FERPA – Family Educational Rights and Privacy Act (1974)
- DMCA – The Digital Millennium Copyright Act (1998)
- WA OCIO Policy 141 - Securing Information Technology Assets

Less Common

- GLBA – Gramm-Leach-Bliley Act (1999)
- HIPAA – Health Insurance Portability and Accountability Act (2000)
- SOx – Sarbanes-Oxley (2002)
- USA Patriot Act – (2001-present)
- Homeland Security – (2002)

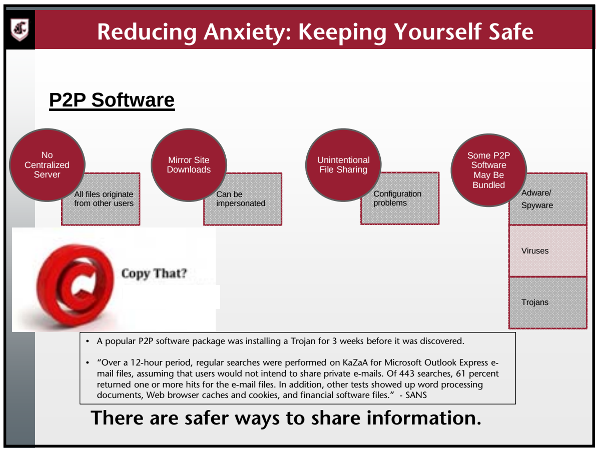


Summary

- We have some pretty **diverse adversaries**
  - Some have rather **scary capabilities**
- **WE ARE A TARGET**
  - Principles that help **keep you secure =** Principles that help **keep WSU secure**
- WSU computer and network security policies are available online
- **YOU** can make a **BIG** difference

WASHINGTON STATE UNIVERSITY

Questions?



Reducing Anxiety: Keeping Yourself Safe

P2P Software

- A popular P2P software package was installing a Trojan for 3 weeks before it was discovered.
- "Over a 12-hour period, regular searches were performed on KaZaA for Microsoft Outlook Express e-mail files, assuming that users would not intend to share private e-mails. Of 443 searches, 61 percent returned one or more hits for the e-mail files. In addition, other tests showed up word processing documents, Web browser caches and cookies, and financial software files." - SANS

There are safer ways to share information.

WASHINGTON STATE UNIVERSITY

This has been a WSU Training Videoconference

If you attended this live training session and wish to have your attendance documented in your training history, please notify Human Resource Services within 24 hours of today's date:

hrstraining@wsu.edu