There is a group at the University of Wyoming who will endeavor to bring tools, procedures, and information to the campus community for computer, data, and identity protection. This group is the Computer Security Initiative: University of Wyoming team; otherwise known as **CSI: UW**.

The primary focus of the **CSI: UW** team is to make faculty, staff, and students aware that you are responsible for your own computer and data security and instill a personal commitment to online safety. Well-known security issues such as passwords, viruses, spyware, hacking, and phishing will be discussed, along with some possible solutions. We will describe physical and system security precautions, establish realistic expectations, describe best practices to share with peers, and improve security in the workplace and at home.
What’s the Problem?

AND WHY SHOULD I CARE?
SPAM has grown into a massive problem – not just at UW but nation-wide. Studies estimate that SPAM represents between 40 and 60 percent of all email. The SPAM problem is a difficult one to solve. Although SPAM filtering software is well developed, even the most sophisticated software occasionally misreads some legitimate messages, treating them like SPAM. Techniques used by spammers to evade SPAM filtering software are constantly evolving, as are the rules used to detect the SPAM.

Information Technology has reviewed various software alternatives to help reduce the flow of SPAM into the campus community. IT uses SPAM filtering software – UWSPAM Quarantine – which reads messages as they come in and either lets them through to your inbox, or collects them as SPAM and sends the list to you on a daily basis.
Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; once installed, the spyware monitors user activity and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Licensing agreements that accompany software downloads sometimes warn that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely.


A particularly bad type of spyware is the toolbar program Hotbar. This program allows you to apply skins to program windows, menus, mail, and other applications. After you install it, it records all the Internet activities of all users on the installed computer and adds the information to its database. The program periodically sends the information in the database “home.” Even if you remove Hotbar, it leaves pieces that allow it to reinstall itself if they are not removed manually.

http://uwadmnweb.uwyo.edu/InfoTech/security/episode1.htm
Malware

Short for *malicious software*, designed specifically to damage or disrupt a system, such as a virus or a Trojan Horse.

Excerpted from [http://www.webopedia.com/TERM/m/malware.html](http://www.webopedia.com/TERM/m/malware.html)

Malware may enable pop-up ads, change browser behavior, or collect personal information about your browsing habits, credit card information, passwords and email addresses. Malware can severely degrade and disrupt the performance of a PC.
Phishing

The act of sending an e-mail falsely claiming to be an established legitimate enterprise in an attempt to scam the recipient into surrendering private information that will be used for identity theft. The e-mail directs you to visit a Web site where you are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal your information. Phishing, also referred to as brand spoofing or carding, is a variation on “fishing,” the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

8/10/08 - - look at spelling, punctuation; and it’s asking for passwords.
The source code for the message shows that the hyperlink for UWmail redirects to the address: [https://webmail.jmu.edu](https://webmail.jmu.edu)
By the way, JMU = James Madison University
And Emergencymail.com is for an ISP in Dallas, TX called Colo4Dallas
How many of you received this message?

When you click on the link, it takes you to a cleverly disguised page requesting your account information.
Hacking

Hack - To write program code, or to modify a program, often in an unauthorized manner, by changing the code itself.


To break into a computer system.

http://www.iss.net/security_center/advice/Underground/Hacking/
Viruses

A virus is a computer program file that can attach to disks or computer files and replicate itself without your knowledge or permission. A virus might run when the file it infected runs, or it might sit in your computer’s memory and infect files as your computer works with them. Viruses can be intentionally destructive, or they may just be annoying.

A worm is a sub-class of a virus, and it is more common today than a virus. It can replicate without your help, like an e-mail address book attack. Worms do not infect other computer files on your machine. Worms are usually spread through e-mail.

A Trojan Horse is a program that seems to be good, but is really harmful, and does something you do not expect. It can erase your computer data, corrupt your files, spread other viruses and worms, spy on your keystrokes, or install a backdoor on your system. Trojan horses are usually spread through e-mail, and contained in an attachment.
<table>
<thead>
<tr>
<th>UW Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Departmental servers compromised</td>
</tr>
<tr>
<td>• Research super computer cluster compromised (hacked)</td>
</tr>
<tr>
<td>• Student victimized by phishing scam; bank accounts were emptied</td>
</tr>
<tr>
<td>• Servers installed with default passwords, hacked within two days</td>
</tr>
<tr>
<td>• Man-in-the-middle attacks</td>
</tr>
<tr>
<td>• UniWyo phishing scam</td>
</tr>
</tbody>
</table>

• Departmental servers were compromised and had to be taken off of the network until they could be rebuilt and confirmed as secured

• Research super computer cluster was compromised (hacked) and had to be decommissioned per orders from government authorities (FBI)

• Turnkey system was delivered to UW, servers were installed with default passwords, and within two days they were hacked

• Man-in-the-middle attacks: A student in the residence halls had software that would capture the usernames and passwords that were entered on that network's subnet. IT had to notify the residents to warn them of possible identity theft and account breaches. The student withdrew from the University.

• A student fell victim to a phishing scam. By the time she realized what she had done, her banking accounts were emptied.

• The UniWyo phishing scam is another example of how social engineering is becoming targeted towards specific audiences, proving that internet users must be diligent and cautious.
<table>
<thead>
<tr>
<th>What Can Happen</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Lost data</td>
</tr>
<tr>
<td>• Open “back door” to computer</td>
</tr>
<tr>
<td>• Hijacking</td>
</tr>
<tr>
<td>• Capture logins and passwords</td>
</tr>
<tr>
<td>• Capture personal data/identity theft</td>
</tr>
<tr>
<td>o Annoying for you</td>
</tr>
<tr>
<td>o Potentially a lot more dangerous depending on how your information is used – expose sensitive data.</td>
</tr>
<tr>
<td>• Network and your computer can become unstable</td>
</tr>
</tbody>
</table>

• **Lost data** - When a computer becomes infected with a virus, that virus can delete data stored on the computer’s hard drive.

• **Open “back door” to computer** - A “back door” can allow a hacker to gain access not only to the individual computer but to any network to which the computer is connected.

• **Hijacking** - A “hijacked” computer can be taken over by others and used to distribute SPAM or viruses. These “Zombie” computers are thought to account for the delivery of 80% of SPAM.

• **Capture logins and passwords** - Spyware can “watch” as you log in to the network and into your Internet accounts, giving others access to those accounts.

• **Capture personal data/identity theft** - once others have access to those accounts, they can steal personal data, and steal your identity

• **Annoying for you**

• **Potentially a lot more dangerous depending on how your information is used**

• Once your personal data has been compromised, it can be used to create identities for others, who do not qualify on their own

• **Account compromises** - Once these identity thieves have your account information, they can use your credit cards and bank accounts without your knowledge.

• **Expose sensitive data** - If they access your social security number, they can take over your life.

• **Network can become unstable** Attacks against the network, whether it is flooding the network with SPAM, or other types of attacks can make the network unstable.

• **PCs can become unusable** Attacks against individual computers can make them
• YOU are the first line of defense
• If you are diligent about protecting your own computer, you can save yourself time and the University money
• Practices established on your campus computer can also be used to protect your home computer
Tidbits of information...

- **IN A SURVEY BY TREND MICRO:**
  - 63% of companies felt that internal employee mistakes and carelessness was their biggest threat to a data leak.
  - On a scale of 1-5 (5 being most serious), concern over data leakage was rated an average of 3.9.
  - Only 26% of companies feel well protected against internal threats of data leakage.
  - Actions that are being taken to reduce this threat include employee education and training, antivirus software, firewalls, better monitoring technology, and encryption.
True Stories
Higher Ed Security Incidents

January 2008

- New Mexico State University (theft)
- University of Georgia (hacked)
- University of Iowa (unintentional disclosure)
- University of Akron (lost)
- Tennessee Tech University (lost)
- University of Wisconsin (unintentional disclosure)
- Brigham Young University (unintentional disclosure)
- Colorado State University (unintentional disclosure)
- Baylor University (hacked)
- Penn State University (theft)
- University of Oregon (unintentional disclosure)

1/05/08 – New Mexico State University (unknown) – Theft

1/09/08 – University of Georgia (4,250) – Penetration

1/11/08 – University of Iowa– (216) – unintentional disclosure

1/14/08 – University of Akron– (800) – Loss

1/15/08 – Tennessee Tech University– (990) – Loss

1/16/08 – University of Wisconsin– (200) – unintentional disclosure

1/17/08 – Brigham Young University– (89) – unintentional disclosure

1/18/08 – Colorado State University– (300) – unintentional disclosure

1/23/08 – Baylor University– (526) – Penetration

1/25/08 – Penn State University– (677) – Theft

1/31/08 – University of Oregon– (33) – unintentional disclosure

For Up-To-Date information go to http://www.privacyrights.org/arl/ChronDataBreaches.htm

Go to the bottom of the list for an up-to-date total of information breaches.
### Higher Ed Security Incidents

**February 2008**

<table>
<thead>
<tr>
<th>Institution</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Minnesota</td>
<td>(hacked)</td>
</tr>
<tr>
<td>Salt Lake Community College</td>
<td>(theft)</td>
</tr>
<tr>
<td>Ave Maria University</td>
<td>(unintentional disclosure)</td>
</tr>
<tr>
<td>Harvard University</td>
<td>(hacked)</td>
</tr>
<tr>
<td>Texas A&amp;M</td>
<td>(hacked)</td>
</tr>
<tr>
<td>Ivy Tech Community College</td>
<td>(hacked)</td>
</tr>
<tr>
<td>Middle Tennessee State Univ</td>
<td>(unintentional disclosure)</td>
</tr>
<tr>
<td>Kansas State University</td>
<td>(theft)</td>
</tr>
<tr>
<td>East Carolina University</td>
<td>(unintentional disclosure)</td>
</tr>
<tr>
<td>Memorial University</td>
<td>(unintentional disclosure)</td>
</tr>
<tr>
<td>University of Iowa</td>
<td>(theft)</td>
</tr>
<tr>
<td>University of Oregon</td>
<td>(theft)</td>
</tr>
</tbody>
</table>

For Up-To-Date information go to [http://www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)

Go to the bottom of the list for an up-to-date total of information breaches.
Higher Ed Security Incidents
March 2008

- Texas A&M—(theft)
- University of Iowa (unintentional disclosure)
- Trafford College (unintentional disclosure)
- Western Carolina University (hacked)
- Lasell College (employee fraud)
- Binghamton University (unintentional disclosure)
- University of York (unintentional disclosure)
- University of Utah (hacked)
- Duke University (theft)
- Ohio University (unintentional disclosure)
- Asahikawa Medical College (hacked)
- Antioch University (unintentional disclosure)

For Up-To-Date information go to http://www.privacyrights.org/ar/ChronDataBreaches.htm
Go to the bottom of the list for an up-to-date total of information breaches.
Higher Ed Security Incidents
April 2008

- University of Colorado, Boulder—(hacked)
- Southern Connecticut St Univ (unintentional disclosure)
- University of Massachusetts (hacked)
- Keio University (theft)
- Connecticut State University (theft)
- Nipton Medical School (theft)
- University of Toledo (unintentional disclosure)
- Bowdoin College (unintentional disclosure)
- Lucknow University (unintentional disclosure)
- University of Michigan (hacked)
- University of Connecticut (unintentional disclosure)
- University of Tokyo (employee fraud)

For Up-To-Date information go to http://www.privacyrights.org/ar/ChronDataBreaches.htm

Go to the bottom of the list for an up-to-date total of information breaches.
## Higher Ed Security Incidents

### May 2008

- New York Institute of Technology (unintentional disclosure)
- University of California, San Francisco (unintentional disclosure)
- Staten Island University Hospital (theft)
- Ohio State University (unintentional disclosure)
- University of Louisville (theft)
- Oklahoma State University (hacked)
- Princeton University (unintentional disclosure)
- Dominican University (unintentional disclosure)
- University of Nebraska-Lincoln (unintentional disclosure)
- University of Colorado-Boulder (hacked)
- Duke University (unintentional disclosure)
- University of California, San Francisco (unintentional disclosure)
- Ohio State Univ. - Agricultural Tech Inst. (unintentional disclosure)

For Up-To-Date information go to [http://www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)

Go to the bottom of the list for an up-to-date total of information breaches.
<table>
<thead>
<tr>
<th>University of Utah (theft)</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Florida (unintentional disclosure)</td>
</tr>
<tr>
<td>University of South Carolina (theft)</td>
</tr>
<tr>
<td>Southeast Missouri State University (employee fraud)</td>
</tr>
<tr>
<td>East Tennessee State University (theft)</td>
</tr>
<tr>
<td>Arizona State University, Northern Arizona University, University of Arizona (unintentional disclosure)</td>
</tr>
<tr>
<td>Stanford University (theft)</td>
</tr>
<tr>
<td>Columbia University (employee fraud)</td>
</tr>
<tr>
<td>University of California-Irvine (hacked)</td>
</tr>
<tr>
<td>Oregon State University (hacked)</td>
</tr>
<tr>
<td>Cornell University (theft)</td>
</tr>
<tr>
<td>University of Iowa (hacked)</td>
</tr>
</tbody>
</table>

For Up-To-Date information go to [http://www.privacyrights.org/ari/ChronDataBreaches.htm](http://www.privacyrights.org/ari/ChronDataBreaches.htm)

Go to the bottom of the list for an up-to-date total of information breaches.
Higher Ed Security Incidents

July 2008

- Ohio University (unintentional disclosure)
- Hillsborough Community College (theft)
- Moraine Park Technical College (hacked)
- University of Houston (unintentional disclosure)
- Virginia Tech (unintentional disclosure)
- University of Maryland (unintentional disclosure)
- Indiana State University (theft)
- Cal State University-Chico (unintentional disclosure)
- University of Texas-Austin (unintentional disclosure)
- University of Nebraska-Kearney (theft)
- Connecticut College (hacked)

For Up-To-Date information go to http://www.privacyrights.org/ar/ChronDataBreaches.htm

Go to the bottom of the list for an up-to-date total of information breaches.
What is Currently Being Done By Information Technology?
Current Steps

- UW Firewall (to be upgraded 2008)
- Trend Micro Office Scan Anti-Virus Protection on campus
- Internet Security (formerly PC-cillin) available for home computers (FREE)
- Virus scanning on all servers and mail gateway

Current:

- **UW Firewall** – Information Technology has installed a firewall device between the campus network and the Internet. The firewall provides greater security for the campus network from the escalating attacks of hackers. The firewall isolates the campus network from the outside Internet while allowing campus users to access the Internet.

- **Anti-Virus Protection for all computers** – Trend Micro Office Scan software installed on all university owned computers. If you don’t have Trend Micro installed on your University computers, you should request it.

- **Internet Security** (formerly PC-cillin), also from Trend Micro, is available for use on home computers belonging to faculty, staff, and students.

- **Virus scanning** is done on all servers and the mail gateway
• **System Update Services (SUS) for Windows updates**

  Distributes critical Windows operating system updates automatically. This process was developed by Information Technology. The updates are distributed after being tested in the UW environment. All UW computers on the UWWYO domain using Windows 2000 or Windows XP, with a few exceptions, are automatically participating in this service. These updates are only Windows updates, and not Office or browser updates.

• **Anti-SPAM Software** *(UWSPAM Quarantine)*

  - [www.uwyo.edu/spam](http://www.uwyo.edu/spam)

• **Network scanned for unusual activity**

• **Ports with suspicious activity are disabled**

---

• **System Update Services (SUS) for Windows updates** distributes critical Windows operating system updates automatically. This process was developed by Information Technology. The updates are distributed after being tested in the UW environment. All UW computers on the UWWYO domain using Windows 2000 or Windows XP, with a few exceptions, are automatically participating in this service. These updates are only Windows updates, and not Office or browser updates.

• **Anti-SPAM** – Beginning March 2007, all UW Exchange began receiving a daily email message from **UWSPAM Quarantine** listing quarantined spam messages. For information about options for this service, including how to opt-out and continue to have spam tagged and delivered to your Inbox, see the **Spam Blocking at UW** web page (www.uwyo.edu/spam/uwspam/).

• **Network scanning** for unusual activity

• **Disable ports**, or connections to the network, if they have suspicious activity, such as continued attempts to log in.
Require Virtual Private Network authentication and secure access required from remote locations.

VPN allows authorized users to securely connect to the UW data network from the campus wireless network or from off campus using various commercial Internet Service Providers. Using VPN, wireless and remote users are connected to the University's internal network as if they were directly connected to the campus network. This allows UW wireless and remote users to access servers and other devices restricted to UW network users and isolated from the outside.

Anti-Malware Software – Spybot Search & Destroy and Microsoft Windows Defender, Beta 2 are available for free download.

System Imaging – IT began using imaging as a method to quickly restore a computer that has been compromised. The image is a standard image using a supported Windows operating system, Microsoft Office, Outlook, Trend Micro OfficeScan anti-virus software, Adobe Acrobat Reader, and VPN on laptops. When a computer is imaged, it will go back to the default state of a standard image. The new image that is installed will have a standard set of security settings that may help to prevent some vulnerabilities that lead to compromises. This process will take a fraction of the time it used to take an IT consultant to rebuild an infected computer. If your computer becomes infected, you will be responsible for retrieving any data that had not been backed up before the compromise.

Increase awareness – That’s why we’re here!
Proactive Procedures
You Can Do

PREVENT PROBLEMS
BEFORE THEY OCCUR!
What you can do

- Do not store sensitive financial, student, or employee data on local computers or USB drives
- Do not use SSNs to identify students
- Remove data from computers sent to Property
  - UW – ‘DBAN’; also – google ‘Eraser’
- Do not allow “Walk-ins” use of admin computers
- Lock your Computer

•Do not store sensitive financial, student, or employee data on local computers - Sensitive data should only be stored on centrally managed servers. It is too easy to steal a computer or USB drive from an office, even yours.

•Do not use SSNs to identify students - SSNs are the keys to the information kingdom.

•Remove data from computers sent to Property - Info Tech recommends DBAN to remove data from hard drives.

•DBAN stands for Darik’s Boot and Nuke. DBAN is available from InfoTech. Free program, prevents most forensic data recovery techniques

•Do not allow “Walk-ins” use of admin computers - It is too easy for anyone to sit down at your computer, insert a USB drive, and walk off with all the information stored on that computer. There are lots of computers in lots of labs for faculty, staff, and student use.

•When you step away from your computer, lock it by CTRL-ALT-DELETE and select ‘Lock Computer’
• **Free anti-virus software**
  - UW Computers: resulted in a decrease in infected computers
  - Personal computers: free anti-virus software for UW employees
    - To download, go to [www.uwyo.edu/antivirus](http://www.uwyo.edu/antivirus)

• **Keep anti-virus software updated**

• **Keep browser and e-mail software updated**

---

**Free anti-virus** – Resulted in a decrease in infected computers. Anti-virus software is available for both UW-owned and personal computers.

**Keep anti-virus software updated** - It is as important to keep your home computer updated as it is your office computer if you connect to UW in any way. Whichever anti-virus software you choose, keep it updated. If you have a dial-up connection at home, set an appointment each week for yourself to update that software.

**Keep browser and e-mail software updated** - If your browser and e-mail programs are up to date, you cannot “catch” a virus by simply opening an e-mail. However, many viruses take advantage of known “holes” in Outlook and Outlook Express. Microsoft especially has greatly improved their response to security holes in their software, but you have to do your part to stay current.
Passwords

**DO’S AND DON’TS**
Could someone really hurt you if they had your **password**?

- Items could be purchased on web sites where you have enabled one-click shopping.
- Your bank and other sensitive account information could be accessed and used without your knowledge.
- Your credit rating could be affected.
- Your identity could be stolen.
- **People could get access to University systems that contain sensitive employee, student, and financial information.**
Passwords

- Weakest link in computer security
- Cracking tools are more powerful
- Cracking takes three approaches
  - Intelligent guessing
  - Dictionary attacks
  - Automation
- With automation, any password can be cracked

- Passwords are the weakest link in a computer security scheme.
- Strong passwords are important because password cracking tools continue to improve and the computers used to crack passwords are more powerful than ever. Network passwords that once took weeks to crack can now be cracked in hours.
- Password cracking software uses one of three approaches: intelligent guessing, dictionary attacks, and automation that tries every possible combination of characters.
- Given enough time, the automated method can crack any password. However, it still can take months to crack a strong password.
<table>
<thead>
<tr>
<th>Password</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sublimate</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Checkmate1</td>
<td>3 seconds</td>
</tr>
<tr>
<td>CheCkmate</td>
<td>&lt; 1 second</td>
</tr>
<tr>
<td>ChEck12</td>
<td>26 seconds</td>
</tr>
</tbody>
</table>

How many of us have passwords that look like one of these?
How many have passwords that look like this?

<table>
<thead>
<tr>
<th>Password Examples</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CheCk123</td>
<td>14 minutes 22 seconds</td>
</tr>
<tr>
<td>3x0n3rat3</td>
<td>4 hours 16 minutes 45 seconds</td>
</tr>
<tr>
<td>5ygn6thb</td>
<td>Could not be cracked, requires brute force</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Write it on a piece of paper</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Give to others</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Pick a password that is easy to guess</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Keep the same password forever</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Use your username</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Use any personal data</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Use “Cowboys”, or “password”</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Use the same password for every account</td>
</tr>
<tr>
<td><strong>DON’T</strong></td>
<td>Provide your password in an e-mail</td>
</tr>
</tbody>
</table>

- **DON’T** Write it on a piece of paper - Don’t record your passwords anywhere they could be vulnerable. Never post them on your monitor or under your keyboard.
- **DON’T** Give to others - Don’t give your password to anyone else. Not even your co-workers or managers. Ever. Period. Have we stressed that enough?
- **DON’T** Pick a password that is easy to guess - Don’t use simple keyboard patterns. A modified phrase works the best. For example, instead of "Sunshine", use "L3tTh3$$hIne". Instead of "Christmas", use "Xms25thovDec". Don’t use names of famous people, places, things, TV shows, etc., that can be associated with you.
- **DON’T** Keep the same password forever
- **DON’T** Use your username or simple permutations of your username.
- **DON’T** Use any personal data (any data someone might associate with you). This includes names, nicknames, pets, phone numbers, or birthdates.
- **DON’T** Use “Cowboys”, or “password” - Don’t use university, college, or state team names. These can be very easy to crack. Don’t use "password".
- **DON’T** Use the same password for every account - If your password is cracked, the hacker will have access to everything.
- **DON’T** Provide your password in an e-mail even if a trusted company or individual requests it.
Password Do’s & Don’ts

- **DO** Change your password often.
- **DO** Make your password over eight characters in length.
- **DO** Combine letters, numbers, and symbols.
- **DO** Make your password easy for you to remember.
- **DO** Misspell words to create a password (*CreeEight*).
- **DO** Use unusual capitalization.
- **DO** Use a passphrase.
  - Come up with a “pass phrase” – *I wish the wind would stop blowing*
  - Take the first letter of each word – *iwtwwsb*
  - Mix upper and lower case letters – *IwTwWsB*
  - Substitute symbols for letters - *!wTwW$b*

**DO** Change your password every 60 days.

**DO** Make your password over eight characters in length. Short passwords are easier to crack than long passwords.

**DO** Combine letters, numbers, and symbols.

**DO** Make your password easy for you to remember, but difficult for others to guess.

**DO** Misspell words to create a password, such as *CreeEight*.

**DO** Use unusual capitalization.

**DO** Use a passphrase.

  * Come up with a “pass phrase” – *I wish the wind would stop blowing*
  * Take the first letter of each word – *iwtwwsb*
  * Mix upper and lower case letters – *IwTwWsB*
  * Substitute symbols for letters - *!wTwW$b*
After all these warnings, is this how you feel?
• Avoid risky sites, such as gaming and adult content sites.
  • In a recent national survey, users who have reported spyware were more likely to have visited online game or adult sites.

• Only download from sites you trust.
  • Before you download from a site, make sure to really read their licensing agreements and privacy statements. Many sites offering cool free stuff are sending you more than you bargained for, and “giving” you malware.

• Public postings on web sites are just that – PUBLIC
  • Many “chat rooms” or discussion sites save the postings for years in archives. Those sites are PUBLIC. What you say can come back to haunt you.
Safe Browsing

- Limit use of cookies and Java Applets
- Avoid using ActiveX and Active Scripting if you can
- Delete cookies regularly
- Type in URLs from messages, instead of clicking on links
- Don’t use the Save Password option on web sites

- Limit use of cookies and Java Applets
  - In general, limit use of cookies and Java applets to those few sites that provide services you need.

- Avoid using ActiveX and Active Scripting if you can
  - This may help reduce the amount of malicious code you run across on the internet.

- Delete cookies regularly
  - Some people think you should set your browser to regularly delete cookies.

- Type in URLs from messages, instead of clicking on links
  - Do not assume a Web site is what it claims to be, unless you have typed in the URL yourself.
  - Make sure the address bar shows the exact address, not a near-miss.

- Don’t use the Save Password option on web sites
  - Don't enable the Save Password Option. If you receive a dialog box asking if you would like the computer to remember the password, choose No. This option lets anyone who uses your computer also use your pre-saved passwords on these accounts.
• Only enter information on secure sites
  Look for the lock –
  Look for the “S” on the https

• Limit personal data
  • Limit the financial and personal data you send to Web sites.

• Don’t give out unnecessary information
  • Do not give out information unless you see a value for you.

• Opt out of marketing notices
  • In general, opt out of marketing notices.
• Don’t store information for later use
  • If the Web site gives you the option of not storing your information for later use, take it.

• Use a credit card, not a debit card
  • Use a credit card for online purchases, not a debit card. A debit card gives thieves easy access to empty your bank account. Visa now has a ‘Zero Liability’ policy which covers Visa credit or debit cards. Check the card issuer’s policy on your responsibility for fraudulent charges.

• If you must send your credit card numbers to businesses, DON’T.
E-Mail Tips

• If you don’t know where it’s been, don’t open it
  • If you don’t recognize the sender, the subject is missing, or words in the subject are misspelled, there may be something wrong.

• Check the Junk Email Options in Outlook
  • In Outlook, go to the TOOLS menu, Options and then the Junk Email button.

• Set reading pane options

• Do not “unsubscribe”
  • This verifies to the sender that your e-mail address is valid

• Do not turn off your virus detection program
  • If you are having trouble with an attachment, and getting messages from your anti-virus software, don’t turn off the program!

• Be careful with attachments
  • Save the attachment, then open it in the application in which it was created so your anti-virus software can check it
Signs of a Problem

- Computer is unusually slow
- Computer reboots without warning
- New icons appear
- Your homepage changes in your browser
- Excessive hard drive activity
- Warnings from installed software
Fixes

- Back up your data (scan for viruses) and get all software reinstalled from a standard image
- Reformat and Reinstall
- Department Power User or IT
- Reinstall original software
- Reinstall from your backups
- Use a System Restore point

• Back up your data and get all software reinstalled from a standard image

• Reformat and Reinstall – if an image has not been created, you may need to reformat your hard drive and reinstall all of the software. Please note, if an IT consultant works on the system, it will be re-imaged. Otherwise, you or any internal departmental support staff may reformat and reinstall the operating system and all software.

• Department Power User or IT – call on these people for help

• Use local computer stores for home PC

• Reinstall original software – find the original installation disks for your operating system and applications and reinstall them

• Reinstall from your backups – reinstall data from your backups. That's right, your backups!

• Use a System Restore point – return the computer to the condition it was in a week ago or a month ago
Physical Hardware Security
Computer Settings

- Lock with [Ctrl]+[Alt]+[Del] when you step away
- Set standby to 5 or 10 minutes
- Set screensaver to ‘password protect on resume’
Treat your laptop as you would your wallet -- never let it out of your sight.

Backup your data before you travel and save as little as possible on the laptop itself

Store as little information on the laptop as possible. Ideally, sensitive data should not be stored on laptops.

Use VPN to connect back to the centrally stored data from remote locations as necessary. See www.uwyo.edu/vpn for instructions.

Protect your laptop with a strong password.

Carry your laptop in a concealing bag like a backpack
Laptop Tips, cont.

- Be vigilant at the security checkpoints
- Store it under the seat in front of you, not in an overhead bin
- Be wary of wireless (use VPN)
- Always assume someone is watching your network traffic
- Use an Encryption software, such as **TrueCrypt**

- Be vigilant at the security checkpoints
- Store it under the seat in front of you, not in an overhead bin
- Be wary of wireless
  - Many wireless “hot spots” are not secure and do not employ encryption.
- Backup your data
Laptop Tips, cont.

- **Software Encryption**
  - **TrueCrypt** (free encryption software)
  - Friday, August 15 - 9:00a.m. - Wyo Hall 425
  - [www.truecrypt.org](http://www.truecrypt.org)
Types of wireless connections on campus:

**UWyo**
- Secure and encrypted access to the UW network

**UWguest**
- Intended for guests to have easy access to the internet

**VPN (Virtual Private Network)**
- Recommended when using wireless away from campus
- Uses encryption and strong security protocols

[www.uwyo.edu/InfoTech/wireless/]
What types of questions do you have??