October 2008, Special CyberSecurity Edition

Weber State University's

IT's NEWS UPDATE

a monthly publication of the WSU Information Technology Division

October is National Cyber Security Awareness Month

By Julie Park, IT Security Office

Each year, the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) joins with the National Cyber Security Alliance (NCSA), the Multi-State Information Sharing and Analysis Center (MS-ISAC) and other partners to support National Cyber Security Awareness Month. This national campaign focuses on educating the American public, businesses, schools and government agencies of ways to secure their part of cyber space, and thus our nation's critical infrastructure.

"Protect Yourself Before You Connect Yourself", by taking simple and effective steps. NCSD identified the following as important security practices:

--Protect your personal information. It's valuable.
--Know who you're dealing with
Use anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure.
--Be sure to set up your operating system and Web browser software properly, and update them regularly.
--Use strong passwords or strong authentication technology to help protect your personal information.
--Back up important files.
--Learn what to do if something goes wrong.
--Protect your children online.

The Internet is a valuable tool for educators and students to communicate and learn. Unfortunately, some individuals exploit the Internet through criminal behavior and other harmful acts. Criminals can try to gain unauthorized access to your computer and then use that access to steal your identity, commit fraud, or even launch cyber attacks against others. By following the recommended cyber security practices mentioned above you can limit the harm cyber criminals can do not only to your computer, but to everyone's computer.

Since there is no single cyber security practice or technological solution that will prevent online crime, it is recommended that Internet users incorporate the NCSD's security practices to stay safe online and avoid becoming a victim of fraud, identity theft, or cyber crime.

The Threatening Faces of Cyber Criminals

By Bret Ellis, Vice President, IT Division

Crimes committed against us today, are not common or even easily understood. Today's criminals frequently do not have common faces or even recognizable names like those we used to see in the local post office. These are not your typical "garden variety" crimes. Often those intruding your personal space with harmful intentions are not from your community, state or even country. You will not catch these individuals directly sneaking into your office or home. Today's criminals use computer and networking from all parts of the world to get into our computers and steal our "wallets" and IDs (precious valuables) then go into systems such as financial institutions anywhere in the world, assuming your identity.

Hacking computers do not care who you are, where you live or what you do for a profession; their purpose is to capture unique information such as your passwords, credit card numbers or social security number. These computers wait patiently 24 hours a day and 7 days a week to artfully capture your vital information in a moment when you share it unintentionally in an unprotected environment.

What is the moral for us to take with us? **First**, stay educated about cyber crime. You can do that by reading this month's edition of IT's News. Every month there is a security awareness column in this newsletter. **Second**, review each charge on your financial statements regularly. Many consider bank statements junk mail and never review them. **Third**, be extra cautious when using public computers, especially in unfamiliar places. Try not to do transactions requiring you to share very sensitive account information. Be sure to logout of the computer completely when finished with Internet transactions. **Finally**, change passwords and pin numbers frequently; this will expose any computers that are tapping your accounts and reduce the likelihood of someone selling/using your information.

Please protect yourself. By doing so, you are also protecting those who share the computer network with you. If you suspect foul play on your machine, in your personal files or e-mail, please contact the IT Service Desk at extension 7777.

Host Intrusion Prevention Software (HIPS)

By Louis Aponte, Computing Support

McAfee Host Intrusion Prevention software (HIPS) is part of the McAfee product line. It defends against threats for which anti-virus programs alone are ill-equipped to handle. We are beginning to deploy the HIPS

component to areas on campus which regularly handle sensitive data.

The deployment process is planned to be a rather slow one because firewalls work differently for different users. Even when computers and software are identical, participants use their computers very differently. The potential exists for harmless software to trigger HIPS into thinking something bad is happening (a false positive report) when it really is not. Considering this annoying detail, we must release the software with the intention of working closely with users to make sure they have positive results.

McAfee Host Intrusion Prevention helps proactively protect desktops from complex threats. Host Intrusion Prevention monitors and blocks unwanted activity and further protects University computers. Automatic updates are handled by the ePolicy Orchestrator (ePO) already running on campus computers. The ePO is integrated into our recently upgraded McAfee Total Protection for Endpoint Suite of products which includes HIPS. No user interaction is required as this software protects the machine silently in the background. More information is available to those who are interested. If you would like your area considered for this extra protection please contact the IT Service Desk at extension 7777 to make your request.

Safe & Sound

by Julie Park, IT Security Office

Don't be put off by the word "firewall." It's not necessary to fully understand how it works; it's enough to know what it does and why you need it. Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for attempts to access your system and blocking communications from and to sources you don't permit.

Some operating systems and hardware devices come with a built-in firewall that may be shipped in the "off" mode. Make sure you turn it on. For your firewall to be effective, it needs to be set up properly and updated regularly. Check your online "Help" feature for specific instructions.

Source: www.staysafeonline.org

Chitester Security

By Gail Niklason, WSU Online

One major key to the popularity of Weber State's in-house developed assessment program is the ability to provide students with flexibility in completing the assessments required for their courses. At the same time, faculty can have confidence assessments are completed within the system are secure, even though they do not directly supervise the assessment process. Flexibility is provided when faculty give their students a window of time, generally 3 to 4 days, within which students can complete a particular test. Students are able to prepare for the test according to their own schedule, and take the test when they're most ready to do so.

Instructors are provided a number of options when configuring their tests, which enhance the security of the assessment. Students can be required to go to a campus testing center (where identification is verified prior to testing), or, in the case of distance learning students, can be required to secure an approved proctor. Question banks can be created from which questions are drawn so that each student in a class can be delivered a slightly different subset of questions; and questions can be delivered to students in a randomized fashion – making it difficult for students to share information about the test with each other.

Recent federal legislation requires schools involved in distance learning to verify that a student completing work for a distance learning course is the student 'of record.' Individual authentication using a unique username and password provided each time the course or related material is accessed, is one approved method of verification. WSU is ahead of the game with Chi Tester!

For information about Chi Tester, including training opportunities, please contact the Chi Tester development team at chitester@weber.edu

Our newest series:

Who's On Desk!?

Dave Bute

Dave has been working for the Information Technology Service Desk since January 2008. He is one of the top technical problem solvers on staff and well versed in both PC and Mac systems.

Dave is a GIS major, Geoscience Information Systems, a music afficionado whose favorites include Coheed & Cambria and Billy Talent.

His leadership among the Techs has made him invaluable to the IT Service Desk.

He is "the man in black" most days so that his fellow Techs say he is a Johnny Cash wannabe.