



Cyber-Security Newsletter

November 2008

STEPHEN F. AUSTIN STATE UNIVERSITY

Threats vs Vulnerabilities—know the difference

A **threat** is a circumstance or event that can potentially harm your system by destroying it, disclosing information, adversely modifying data and making the system unavailable. Environmental threats are natural events (lightning, hurricanes or floods) and system environment (poor wiring or insufficient cooling). Human threats can be either internal (disgruntled employees or unintentional damages) or external (hackers).

Vulnerability is a weakness in an information system or its components such as applications that can be exploited. Vulnerabilities are the often the result of a flaw in the coding of software. Vendors issue patches to fix vulnerabilities. End-users can limit exploits to the vulnerabilities by installing the patches to operating system and applications running on the machine.

Social Engineering—hackers in disguise

Social Engineering is a hacking technique that relies on human nature. Hackers pose as legitimate personnel to trick individuals to reveal passwords and other information to compromise the security of the system. Phishing is a type of social engineering scam which uses email or web sites to deceive users in disclosing information. Phishing email messages tend to sound urgent and require immediate action to update or validate personal information. If the user clicks on the link provided, the user will be redirected to a bogus website where personal information will be stored. Once you have done this your identity will be stolen. Remember legitimate companies do not ask for personal information via email or pop-up windows. **SFA will never solicit your user name and password through an email. If you have not initiated help from Technical Support staff be wary of emails claiming to be from the helpdesk or support personnel.**

Internet Security

There are several security risks associated when browsing the Internet. One common risk is known as cookies. Cookies are a text file that a web server stores on your hard drive when you visit a website. When you revisit the website, the web server recognizes you. The security issue occurs when the cookie stores unencrypted personal information such as social security numbers or credit card numbers. To protect yourself set up your browsers not to accept cookies. Another security risk is mobile code such as ActiveX and Java which are scripting languages used for internet applications. Mobile code can run automatically without you knowing.

Peer-to-Peer (P2P) refers to file sharing applications that enable computers connected to the internet to transfer files to each other. There are legal, ethical and security concerns associated with unauthorized applications. Music and movie files are most commonly transferred. Sharing music and movie files through P2P could result in a copyright violation leading to criminal prosecution. As the ISP provider, SFASU is required to comply with any "shutdown" notices. SFA receives hundreds of email notification of illegal downloads and sharing of copyrighted music and movies from RIAA and MPAA. This is a violation of the University's Digital Millennium Copyright Policy (D-42). P2P increases your system's security risk by opening your computer to outsiders and exposing SFA's network to unauthorized access.



How Anonymous Are You?

You may think that you are anonymous as you browse web sites, but pieces of information about you are always left behind. You can reduce the amount of information revealed about you by visiting legitimate sites, checking privacy policies, and minimizing the amount of personal information you provide. Some of the information left behind when visiting a web site include the IP address, domain name, and software details.

Each computer on the internet is assigned a specific, unique IP (internet protocol) address. IP Addresses are like phone numbers allowing others to communicate with you. Internet Service Providers (ISP) own a block of IP addresses to assign. SFA is the ISP for computers on the university's network. Domain name is like a phone directory that is used to lookup your IP address. The internet is divided into domains for example .edu is for educational institutions; .gov is for government agencies; .org for organization and .com for commercial use. The list of active domain names is available from the Internet Assigned Numbers Authority (IANA).

You can limit the amount of information exposed by increasing the security settings on your web browser and looking for the padlock or https address when supplying personal information such as your credit card or social security number. Internet Explorer 7 has a Phishing Filter that automatically checks Websites against a list of *known* phishing sites. You can still visit a phishing site and have your identity stolen.

Last Words—A risk to one is a risk to all.

It is easy for the security message to become overkill with the large number of stories of hackers, botnets, and breaches involving identity theft along with the constant reminders of patch early patch often, update your virus definitions, install a firewall etc.



But by understanding your responsibility for protecting information resources, you can prevent attacks and contribute to the safety of SFASU systems. The goal of information security is to protect the University's data and information systems from unauthorized access, unwarranted modifications, and to have the information and systems available when needed. Information security is everyone's responsibility. As part of our awareness campaign, ITS will be hosting various webinars and information sessions in upcoming months.

Suggest a topic to or submit questions to ITSecurity@sfasu.edu. - Monica

Test Your Knowledge

1. An email claiming to be from the webmaster or email administrator requesting your user name and password is known as _____.

2. A high-tech scam that uses email or website to deceive you into disclosing your credit card numbers, bank account information, social security number is known as _____.

3. A plug-in that can automatically run hostile programs on your computer without your knowledge simply because you visited a website is known as _____.