SWCP PORTAL

Providing News, Views, & Clues from Your Local Internet Experts 201001

Annual Security Review

Staying Safe Online

By Jay Nelson, Editor

The new year is traditionally a time to take the long view and consider the progress you've made and directions you want to go. This makes it a good time to check your online security, take care of any gaps, and see what needs to be watched for during the coming months.

Back to basics

First, the fundamentals, so easily overlooked and sometimes annoying, but if they're not in good order, then any other steps may be quite useless.

- Choosing good **passwords**. No names or words. Mix upper and lower case, numbers and letters. It's also wise not to use the same one for everything, and to change them occasionally.
- Controlling **physical access**. Locks, user profiles, or password-driven access might be necessary if your machine could be used by others. Don't leave sticky notes with your passwords around either. When recycling, be sure to wipe hard drives thoroughly or better yet, remove and destroy them.
- **Virus protection** is still important. While Macs and Linux remain relatively untargeted and no major flaws in Windows 7 have been reported yet, this could change at any time. There are still some excellent free antivirus programs like AVG available, and SWCP is about to become an authorized resaler of AVG's more powerful professional product. Call or email Tech Support for more info.
- **Firewall** fortification is absolutely essential to keep out intruders, especially if you use Wifi. Many modern devices have a firewall built in. If not, free and commercial software firewalls are available.
- **Using email safely** is a good habit to get into. Be careful about opening attachments, especially from strangers, and never, *ever* respond to spam. Also, SWCP has put together a suite of powerful antispam tools for your use, including Spamassassin and Spamprobe, to give you more precise control over what gets into your inbox. Roundcube, one of our Web-based email interfaces, can also allow you to check suspect mail and manage spam safely.
- Check your **browser security** settings, so that you can control scripts and cookies.
- **Back up** your files regularly "just in case". This can save you a lot of misery from hardware as well as software disasters. SWCP BUS, our online backup system, is an easy, cheap, and automatic way to make sure you never lose your vital data, whatever it might be.
- **Clean out** your computer. Even if you have no problems, your desktop or laptop will run smoother if the caches are flushed occasionally, the drive defragmented, etc. If you do have problems from viral infections, malware, or clogs, SWCP's Computer Repair and Tune-up services, some of which are free to members, can remove the garbage and install protection to help you stay safe, too.

Looking out ahead

New threats emerge all the time. **Phishing**, where bogus alarms scare users into visiting a fake website in order to steal their personal information or install malware, remains a major concern. A simple rule is: ***Never share your personal information online***.

In particular, **beware of pop-up windows** while surfing that warn your computer is infected and which do *not* come from your antivirus program. Click on the link and it surely will be infected, by very nasty bugs, too.

Alas, the bad guys are clever and constantly working on new tricks. It is very important to **keep your OS and all your software updated**. Recently, for instance, serious flaws have been found in both the popular Flash animation and Adobe Acrobat PDF-reader programs.

Possible dangers coming up that already worry security experts include **smartphone viruses** and spying on users of **cloud computing**. The wave of the future, cloud computing uses online resources rather than programs installed on your computer, and is already employed not only by Google, but Amazon, Twitter, and Facebook.

This all just shows how important the Internet has already become to our daily lives. As the Net grows ever more vital, so must efforts to protect it. Southwest Cyberport will do our part to keep you safe and well-informed. For more tips on staying secure, see articles on our website, www.swcp.com. Contact **Tech Support** at (505) 232-7992 or help@swcp.com with your questions or concerns.

Securing Online Transactions

What is a certificate, and why would I need one?

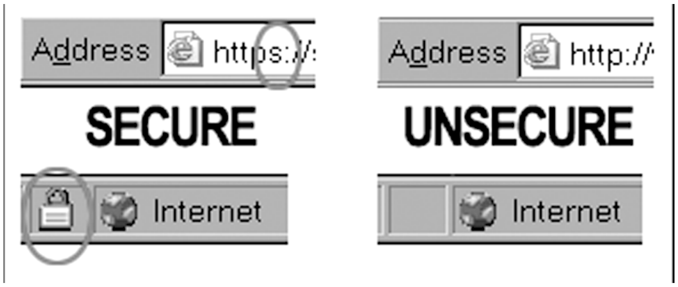
By Kurt Boucher, Broadband Manager

Sometimes you may visit a website which requires that you provide information that is best kept private, such as credit card numbers or other personal information. An **SSL Certificate** enables encryption of this critical, sensitive information during these online transactions to keep it secure. But how does it work?

Data can easily be disguised by computers to keep it safe. That is, an **encryption algorithm** is used to make it unreadable by snoops. These algorithms are number sequences that follow a particular formula to scramble and unscramble that data. The encryption algorithm is the key to your data. An easy way to think of it would be like a "secret decoder ring", but imagine this ring is unique for each conversation.

Computers are quite good at encryption, but how can we be certain that the information is being sent to the right place? That is, how do we know that, when we're about to place an order on a website, that they really are who they say they are, and the site is not the work of someone doing something unscrupulous?

The first clue is in the browser Location bar. The website's address should be displayed beginning with "**https**:" rather than the usual "**http:**". The final "**s**" indicates a secure site. Another indicator may be the icon of a closed lock, usually somewhere in the bottom bar of the browser. Unsecure sites will display an open lock, or none at all, depending on your browser.



But how does your browser know it's secure? That's where **authentication** comes in. When connecting to a secure website, the web server authenticates itself to your web browser by presenting its **digital certificate**. This certificate is verified by an independent, trusted third party that the website is, indeed, just what it claims to be. While your computer exchanges information with the website, the certificate authority works in the background to verify the identities of both computers. Once that verification is made, a unique encryption key is sent to both parties. From there, the computers are free to exchange information safely.

A **standard certificate** will handle the encryption of data securely and reliably, however, there are also new "Extended Validation" certificates, which are able to more authoritatively confirm the identity of the web site you're talking to. You can tell if you are visiting a site with an Extended Validation certificate because your browser's location bar will turn green. Most bank websites use Extended Validation certificates already.

If you have a website where you accept credit cards or other data that must be kept secure, an SSL Certificate is needed for this third-party verification process. This SSL (for "Secure Sockets Layer)" Certificate gives your website's visitors undeniable proof of its identity, creating customer confidence in the integrity and security of your online business. A valid certificate assures your clientele that they are sending their personal information securely and to the correct website.

As a consumer, your web browser already contains support for SSL Certificates. It is up to each website owner to obtain a certificate if the site needs to support secure communication.

Consumers in general are becoming increasingly aware of the advantages of SSL security and will often not buy online from non-secure businesses. All major online merchants use SSL security for their customers security while purchasing online.

As a state of the art Internet provider fully able to support the needs of online commerce, Southwest Cyberport is happy to provide SSL Certificates for our Professional Webhosting members now starting at only $95 per year. Check out more information on our website at *www.swcp.com/certs*. Or contact SWCP at (505) 232-7992 to order your certificate today!

Net Notes

The Deep, Dark Net

Beneath the glittery surface of the Internet lies a mysterious world beyond the reach of Google and Yahoo. Perhaps well over 500 times larger than the searchable Web, this dark realm consists of vast databases of consumer information and research data, background content for search-blocked websites, abandoned address spaces from defunct companies and even the US military's earliest online experiments. Littered throughout cyberspace behind technical errors, failed enterprises, and forgotten disputes between service providers, some of these areas are also often accessed by secret networks.

The notorious Russian Mob uses such hidden cyberspaces to send out spam, and even rents out illicit websites that quickly come and go. Various other criminal gangs as well as anarchists and dissidents seeking to avoid authoritarian government attention lurk there, too.

Google and other players are developing tools to explore this unknown underworld, but it may be too large to ever fully map. As the Web is slowly commercialized, opportunities for true anonymity diminish. But since the Internet is always a work in progress, cracks and crevices where darkwebs can flourish are expected to linger for some time to come.

— *The Guardian UK*