



PRACTICE SAFE SURFING

The numbers don't lie. According to data published in the "2009 Digital Future Report" by the Annenberg School at USC, 80% of Americans use the internet. Additionally, 40% of Americans 66 and older go online, up from 29% in 2000; 24% of American households have 3 or more computers; on average, internet users spend 17 hours per week online. Wow! That's a lot of surfing the web! And, with cyber-crime on the rise, that's a lot of risk being taken. So, how can you protect yourself, your family, and your personal information?

The United States Computer Emergency Readiness Team (US-CERT) is a public-private partnership that is part of the Department of Homeland Security's National Cyber Security Division. US-CERT's website (www.us-cert.gov) has some outstanding information available about safe surfing. Here are some highlights.

Security Basics

Passwords are typically used to authenticate an individual's usage of a system like email or online banking. Choosing good passwords and protecting them is vital to maintaining security. Use a combination of upper-case and lower-case letters. Mix in numbers and punctuation marks if the system will allow it. Avoid words that can be found in the dictionary or obvious numbers like your birthday, anniversary, or part of your social security number.

Install anti-virus software on your computer and keep it up to date. Anti-virus software can block viruses before they infect your computer. It is especially important to scan files attached to emails before you download them. You should set your anti-virus software to update itself daily with the most recent virus information and to run an automatic scan of your entire system periodically. Set it to run at 3AM and leave your computer on overnight one night per week. Use a firewall to restrict outside access to your computer. Firewalls are

a type of software that prevents an intruder from accessing your computer via the internet and capturing important information.

Install spyware detection/removal software. Spyware programs are malicious cookies that you pickup from websites you surf that remain on your PC for the purpose of harming you. One common type of spyware is called a key logger. It records all of your key strokes and can be programmed to

On average, internet users spend 17 hours per week online.

trigger an email containing your personal information when it records you typing sixteen consecutive numbers while on a website – like you do when you use a credit card to purchase something online. Imagine, your own email account sends an email to a scammer with your credit card, expiration date, etc. Before I do any online shopping, I always run two separate spyware programs specifically to protect myself from this potential threat.

Protect Your Kids

Children spend a lot of time online. Every minute they spend there, they are at risk. Online predators are rampant. Hardly a day goes by that you don't hear about police somewhere arresting someone who was pretending to be a kid and arranging to meet another child in person. It is among most parent's greatest fears.

Your best defense is knowledge ...

knowledge of where your child is going online, who they are chatting with and emailing, etc. Keep your computer in an open area of the house, not behind closed doors in the child's room. Regularly monitor activity. Warn them about the dangers and set rules about what they can and cannot do online. Partition your computer into different "accounts" and use parental controls functions to restrict your child's access to only those websites you want he/she to use.

Online Transactions

Scammers operate in a variety of ways. They target vulnerable computers with spyware. Fraudulent businesses are setup and unsuspecting buyers make purchases using their credit cards. Transactions that are made without secure encryptions are intercepted and personal information stolen.

Protect yourself by using up-to-date anti-spyware, anti-virus, and firewall software. Keep all of the software on your PC up to date. Install updates or patches to your web browser – most of those are released to fix known security holes. Run spyware and virus scans before shopping. Do your online shopping with reputable vendors.

You spend a lot of time on the internet today and based on trends, you will likely be spending more time there in the future. And, you will likely be conducting more business there – banking, bill paying, shopping, taking online classes, and more. Practicing basic computer security techniques is a must, because the criminals get more and more sophisticated every day. Visit www.us-cert.gov for more information on how to protect yourself.



Kathleen J. Luczynski is the Senior Vice President and Chief Information Officer of South Adams Savings Bank. Her writings about matters most affecting our customers (customer information, security, and technology) appear in bank publications and on our website.

You can email Kathleen directly at kluczynski@sasavings.com.