CG Column
June 2010

Computers have become as prevalent and necessary to daily life as cars, yet if we operated cars like we do computers we would be speeding blindly against traffic on the wrong side of the road, without wearing any seatbelts, riding on bald tires, and picking up hitchhikers along the way.

Safety is a word normally associated with accidents, stairs, and summer, but not computers. Yet, safety should be a watchword when operating our computers, they are not safe havens where information can be stored with impunity.

According to the FBI's Internet Crime Report, $559.7 million was reported lost through cyber crime in 2009; up from $264.6 million in losses in 2008. "Popular scam trends for 2009 included … astrological reading frauds, economic scams, job site scams, and fake pop-up ads for antivirus software," according to the report.

The threat to our nation's computer networks is substantial. According to William J. Lynn III, deputy secretary of defense, they are scanned "millions of times a day."

With the threat real and increasing each day, consider using your computers like you would use your cars with a few simple rules.

Lock the car. You would never consider leaving your car unlocked nor would you "hide" your key to make it easier to open the car. Make sure you have a password that is strong enough to deter most hackers, and don't write it down. Department of Defense policy recommends 8-12 characters using a mixture of upper, lower case, numbers, and special characters. I strongly suggest the same for your personal computer at home.

Hitchhikers. There used to be a time in the United States when hitchhiking was a safe pastime, but no longer. Today, downloading unknown documents or responding to emails from unknown addresses is the equivalent of picking up hitchhikers with your computer. It isn't smart, and it certainly isn't safe.

Don't park in a dark alley. We are all very aware of our surroundings when in a car; take the same precautions when in your computer. WiFi hot spots are very popular, but you should be aware of your surroundings. Don't leave your computer unattended, watch for those who might be looking over your shoulder, and remember – public WiFi hot spots are unsecured networks.

Lastly, (and probably most importantly) new drivers. Before giving the car keys to our children, we generally ensure they receive driver's ed, we ride with them, and we show them basic maintenance procedures. These are good rules to go by with computers, too. Believe me, getting a fender-bender is not as bad as having their identity stolen and credit history ruined before they're 18. Our young people need to be educated about passwords, common malware delivery ploys, staying away from enticing but dangerous websites, and made aware of the dangers associated with social media sites.

According to McAffee's 2010 Report on threat predictions, "Social networking sites such as Facebook will face more sophisticated threats as the number of users grows … As users' expectations of their Web 2.0 services evolve, we expect to see many rogue services set up with the hidden purpose of capturing credentials and data."

Taking some simple steps and using the car analogy may help protect our networks and our personal computers.

Jeffrey Carr states emphatically in his recent book, Inside Cyber Warfare, "the biggest problem we're facing isn't the attack itself, it's the head-in-the-sand attitude that prevents organizations from putting the security practices and safeguards in place that would make an attack less likely to succeed, and less harmful if it did succeed."

We need to buckle up, drive straight, and protect ourselves while on the information super-highways.

SECURE THE HIGH GROUND