

The Last Cyber Warrior

January 2012



When it comes down to it, you — yes, you — are the last line of cyber defense against the endless hordes of cyber criminals, terrorists and foreign agents. Digital technology now touches almost every living person and as time moves on its reach will only continue to grow. With technology reaching us all and being incorporated into more parts of our daily lives, you can no longer rely on someone else to protect you. Whether it is defending your data at work, or defending your personal data at home, being an effective cyber defender is a continuous responsibility.

Many people put their personal and work cyber security in the hands of others, or hold the belief that technology alone will protect them. Some figure that cyber security is not their responsibility as their work duties have nothing to do with computers. Others believe that because of the job they have, or the low profile life they lead that they are not potential targets, and therefore not personally vulnerable. While others incorrectly think that the consequences of being a victim of a cyber attack will only be a minor annoyance. These are the people whose names will be added to the ever growing list of cyber victims. This is not said as a “boogie man” story, but rather it’s a simple fact.

There are also many who have relied upon an office cyber guru, a techie friend or a geek for hire to protect them. Yet even these cyber guardians and the technology they install cannot keep someone from facilitating a cyber attack by opening the wrong email, creating a weak password, or bypassing a firewall setting. What happens when these cyber guardians are not available? Have you been ignoring the warnings of current threats from your internal IT group, the digital industry press or even the general media? Do you know the basics of sound cyber security? Do you know what needs to be done to keep your personal information or your organization’s networks secure, even if you need support to accomplish those tasks? Awareness of your vulnerabilities and proactively responding to potential threats is the key to cyber security.

In very simple military terms there are three types of cyber threats. The first is an attack along a broad front like the wide release of a super-virus that attacks any vulnerable network or system. Then there is an attack against an established position as when hackers target the network of a particular organization or person. Finally there is infiltration, perhaps the most common. Cyber infiltrations use phishing schemes, bogus websites, and a host of other online scams to trick the unwary into divulging information or allowing access to malicious software. The frequency of all these attacks is extremely high, and range from the crude to the highly sophisticated. They come from a wide array of sources ranging from state sponsored cyber attacks units to kids pulling a prank. Regardless of all the cyber security support you may have, it comes down to you whether you can defend against the forces aligned against you. These threats are not going away.

This is not as daunting a task as it sounds. When you stop and think about it you protect yourself and your family from threats every day. You secure your house with locks and alarms, you use IDs, CACs and secure passwords at work, you protect yourself and your family by being a defensive driver, you avoid dark alleys unless necessary, and you brush your teeth three times a day. Adding cyber awareness to this mix of self preserving behaviors is not a big deal. The only question is “will you do it?” For your country, your family, your friends and yourself the answer needs to be “Yes.”