Getting users involved in protecting their home systems and those of their families and friends is good for everyone. In that connection, my friend and colleague in the MSIA Program at Norwich University, Adjunct Professor Kip Boyle, wrote to me recently about his new blog and I invited him to share his news with readers of this column. What follows is entirely Kip’s own work with minor edits.

* * *

One day, while working hard as the chief information security officer at an insurance company, I realized that much of our organization’s network security was in the hands of ordinary users of our computers. No matter how much my team did to safeguard our customer’s confidential data, no how much money we spent on our mission, all it would take was one average Internet-using employee to cause major damage, either deliberately or accidentally.

That unhappy thought got me thinking about all the friends and family who have ever asked me to figure out why their computers were so slow or just misbehaving. I thought about all the electronic crud I typically find when I get my hands on their machines. I remembered how it is often impossible to undo the digital damage, which forces a frantic search for software license keys and a reformat of their hard drives. And as for backups, forget it!

As the shocked amateurs receive their reformatted systems, I hear the same questions: How did this happen? Where did I go wrong? How can I keep this from happening again? Did anything bad happen to my bank accounts? My friends and family feel vulnerable, embarrassed and mystified.

My team spends time and effort educating our work force and protecting them with many sophisticated and expensive defenses that are usually invisible to them. My organization is meeting its due care obligation but it is difficult for employees to fully understand and internalize the Internet security issues facing all of us. How can they manage to cope with the range of threats when they do not understand technology well, have no immediate economic incentives, and neither see nor understand all that is done by my team on their behalf?

Indeed, the problem is global. A recent study by (ISC)^2 and Infosec Europe 2009 summarized by Warwick
Ashford in _ComputerWeekly_ on April 17, 2009 reported that “Half of UK security managers are concerned about end-users' lack of security awareness, a survey has revealed. In a poll of more than 700 security professionals, the biggest concerns were a lack of training (48%), an unsupportive company culture (48%), poor employee understanding of policy (46%) and a lack of defined accountability (42%).”

However, as discussed in “Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy” <http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf> increased personal Internet security involvement leads to increased corporate Internet security. People who take responsibility for their own online safety and security naturally bring those behaviors into their workplace. Educated employees become better netizens and that increase in knowledge and involvement helps everyone who uses the Internet. When users behave more securely, there are great benefits for the common good.

When I start thinking about acting for the common good, my desire is to have a large impact. Therefore, a current point of frustration for me is that my team’s impact is limited to our small corner of the Internet. To broaden my reach, I have started a blog to help average people who use the Internet to stay safe and secure online.

In this context, I define an average Internet user much as we would define an average car driver. There is no need, and usually no desire, for drivers to understand what is happening under the hood. Yet thanks to good automotive design, laws, insurance, and reliable infrastructure, average people can still enjoy the benefits of driving without taking undue levels of risk.

The point of my blog is to connect with Internet users of all experience levels so we can figure out how average Internet users can be safe and secure online right now. Although the Internet currently lacks many necessary safety and security features to protect individuals, as well as lacking adequate protection for the commons, my hope is that we will discover lots of practical things that anyone can do right now, if they are motivated, without becoming systems experts.

We will talk about why the Internet can be so dangerous and why we are lacking incentives for government and private industry to step up and do what only they can do to protect the online commons. I have my own opinions on these topics and I intend to share them. No, I do not think the situation is hopeless, nor are the people involved in shaping the governance of the Internet stupid. Nevertheless, there are major challenges and we need all of our collective intelligence to share what we know and to work on the problems with creativity and collaboration.

I invite you to join the conversation! Just follow this link.<http://www.personaldataprivacy.com/>

See you there!

* * *

Kip Boyle, MSc, CISM, CISSP has been active in information technology management and security since he was Director of Information Systems for the 83rd Fighter Weapons Squadron at Tyndall Air Force Base in Florida starting in 1992. In 1995, he became the Director of Enterprise Network Security for the F-22 System Program Office at Wright-Patterson AFB in Ohio and then joined the Stanford Research Institute (SRI) as a Senior Consultant in the Information Security Group in 1997. He became the CISO of PEMCO Insurance in 2005 and is responsible for setting the strategy and direction of their information security program. You may write to him
by e-mail <mailto:kip.boyle@gmail.com>.

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 Kip Boyle & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.