# ***The Three changes needed to make the Internet safe.***

Let’s face it, the Internet is not a safe place. Several times a week I get bombarded by people trying to rob me: phishing schemes asking for my credit card number and other personal info, ridiculous letters from Nigeria asking for cooperation in return for a few million dollars and other too good to be true schemes, random packets flung at my PC every few minutes at least – many obvious hacker attacks and probes, and I’ve received three viruses just this morning in my email.

How often do con artists try to interact with me in the physical world? How often does anyone try to break into my office, car or home? How often do vandals try to attack? Clearly these events occur far far less often than similar events on the Internet!

Before the Internet becomes relatively safe (use your own definition) three changes are needed:

1) **Hacking has to be recognized as a serious crime.**

Not long ago, many people thought hackers were doing little or no harm. The common perception was that most of them were smart yet maladjusted kids who were just causing a little mischief.

Today there is an increased awareness that hackers cause serious damage.

- The release of a particularly nasty and effective virus is closer to the sacking of Rome than simple trespass, causing millions of dollars or more of damage.
- In the last twelve months, U.S. bank’s customers have lost over US$2.4 billion from phishing scams according to The Gartner Group.
- Hackers are no longer primarily kids or young adults playing around – serious organized crime has taken to the Internet. Organized groups exist worldwide, including in China, Russia, Kazakhstan, and other hard to reach/prosecute areas.

According to the FBI Computer Crimes division, extortion is one of the primary growth areas of computer crime. A common drill goes like this: someone breaks into your confidential files, perhaps customer records, and then tells you they have found a “hole” in your security. They offer to help you “fix it” for a modest sum. And if you don’t “hire them,” you just may find your customer’s credit card numbers or other sensitive and embarrassing data publicly posted on the Internet (hint: paying extortionists doesn’t make them go away, it encourages them to ask for more money).

While still rare, we are seeing some hackers actually getting arrested and going to jail. This week's headlines show an arrest for domain hijacking, a plea bargain for spamming via unsecured wireless access points, and a three year conviction for pirating software – i.e. most computer crime went unpunished.

It is still true that relatively law-abiding youngsters who would never consider breaking into their high school or college and breaking all the windows and writing nasty slogans on the walls don't think that the electronic equivalent is a big deal. In fact kids still think "hacking is cool." I recently saw a very computer literate 10 year old who is usually never allowed unsupervised Internet access (a reasonable parenting practice) start searching for hacking websites and hacking tools as soon as he was left unattended. He's never been in any trouble, and when I asked him, he explained that he and his friends all thought "hacking is cool." I am sure that he could find and use hacking tools and cause serious damage.

We need a mindset change.

**2) Software complexity MUST decrease and its rate of change MUST slow down.**

Software is too complex:
There is an often quoted statistic that I'm not going to get absolutely right: 95% of all Microsoft Word users only use 5% of its functionality. This may or may not be entirely accurate, but it is clear the vast majority of users only use a small percentage of most software packages functionality. So why is most software so big and complicated??? The more complexity software has, the more bugs, the more security issues, the harder it is to test, the more likely it is to have serious security issues. It's as simple as that.
All other things being equal, **simpler software is more secure. We need more "Simpler Software."**

Software changes far too rapidly:
New and improved versions are "better," have more functionality, and are in many cases actually "improved and better." But **you can't secure a moving target**. Often any "new and improved" benefits are debatable, but the new software is usually larger, more complex, and less secure.

My car has a microprocessor and software code, but **I don't change the code in my car ever! I shouldn't be forced to change my OS and key applications frequently!** Personally, I wish my car was stupid – take the chips out of the damn thing! Simplify!

**3) The responsibility of Internet parties must improve.**

An automobile manufacturer couldn't sell cars without basic security – i.e. locks. It would be irresponsible. Even for country dwellers who may rarely or never lock their cars, the ignition lock is an essential safety feature. Imagine if a three year old could get in a car and start it!

Operating Systems need basic security built in and need to be secure by default. For example, an unpatched and unprotected Windows system on the Internet will be compromised in 20 minutes on average according to the SANS Institute! And this compromised machine can be used for denial of service attacks, to help hide malicious hackers tracks, to host kiddie porn or pirated software, to send endless spam, etc. In other words, your insecure machine on the Internet can adversely affect others, just like a drunk driver is a threat to more than just themselves.

Users need to bear responsibility as well. You can't get an old unsafe piece of junk car and drive it legally. Cars need to be inspected for safety on a regular basis. But anyone can put a computer on the Internet. Including ones with old unpatched operating systems and applications that have well known vulnerabilities that can be exploited by ten year olds as well as serious criminals. Users need to bear the responsibility to have their computers and applications regularly updated against common threats. There are emerging technologies and products that can help. For example Cisco's Network Admission Control can require devices to have up to date operating systems and virus protection before allowing them on a network.

ISPs and other Internet infrastructure parties need to be more responsible as well. Some do a great job but more quite simply do not. Impossible packets need to be dropped (e.g., ones with obviously incorrect IP addresses, ones that are clearly malformed, etc.). Emails from non-existent domains need to be dropped as well. Denial of Service attacks need to be stopped within the Internet Cloud when possible.

My ISP just stopped a virus emailed to me. My ISP doesn't catch them all, but they're trying. Does yours?

I am NOT recommending more government legislation – we have more than enough already! I do know there needs to be more individual and corporate responsibility! I imagine a few lawsuits, probably in the lawyer dense country of the U.S.A., will help define responsibilities . . . .

Hacking needs to be treated as a serious crime.
Software needs to be simplified.
Operating System vendors and Internet Service Providers need to assume more responsibility for security.
And Internet users need to have responsibly secure computers.

On the Internet, you **should** be paranoid, just as in real life. Just more paranoid on the Internet as more people ARE out to get you!!!

References:
The Anti Phishing Working Group
URL: http://www.antiphishing.org/index.html

"Phishing scams: 5 ways to help protect your identity"
URL: http://www.microsoft.com/athome/security/spam/phishing.mspx

Swartz, J, USA Today
"Hackers Evolve from pranksters into profiteers" March 2003
URL: http://www.usatoday.com/tech/news/computersecurity/2003-03-16-hacking_x.htm

eWeek
"Experts Say Hacking is Now for Profit" April 2004
URL: http://www.eweek.com/article2/0%2C1759%2C1573461%2C00.asp

Bruce Schneier, Crypto-Gram Newsletter
"Software Complexity and Security" March 2000
URL: http://www.schneier.com/crypto-gram-0003.html#SoftwareComplexityandSecurity

Loney, M; Lemos, R
CNET New.com
"Study: Unpatched PCs compromised in 20 minutes"
URL: http://asia.cnet.com/news/security/printfriendly.htm?AT=39190452-39001150t-39000005c