RANDOM THOUGHTS
Communications With A Purpose

William Blinn
COMMUNICATIONS
179 Caren Avenue
Worthington, Ohio 43085
614-785-9359
Fax 877-870-4892
www.Blinn.com

December 2004

Safer computing with a Mac or Linux computer?

It seems that every time I turn around, there's another security problem with Windows. Or with Internet Explorer. Or Windows Media Player. Even Mozilla. I install security patches at least once a week on average. And that doesn't include daily antivirus, firewall, and anti-spy checks.

You too probably spend too much time keeping away the creeps who want to steal your identity or use your computer to send spam, serve stolen software, or house pornography.

To hear the Linux and Mac camps tell the story, my life would be peaceful if only I would see the light, throw away my Windows machines, and replace them with (depending on the stripe of the evangelist) a Linux box or a Mac box.

I have a Mac. Three, really, although one belongs to my commercial-art student daughter. Mac owners download and install security updates regularly, too. Antivirus software has to be updated. I like Macs, but they're just computers. When Kaydee's Mac became unable to her 2000 or so digital images, we could see that the files were still there even though Iphoto couldn't show them.

A quick Internet search turned up a utility program and an explanation that this isn't a particularly uncommon problem, but the explanation solution were not on Apple's website. Some other victim had solved the problem and posted the information to help others. No, that's not a security issue; it's just a reminder that all computers have problems.

Linux? The Web server for Linux is called "Apache" because it has so many patches. It's "a patchy" application. Security alerts are common for Linux, too.

Why is it just Windows, then?

Why are Macs and Linux machines relatively safer? Or are they? Actually, I think they are and I see a good reason. My theory is one that has Mac and Linux evangelists calling for the wrath of Steve Jobs and Linus Torvalds to rain down on my head: People who write applications to take over other computers will always shoot for the largest possible target. That target is Microsoft's operating systems.

Why write a Trojan that will turn 5% of the machines on people's desktops into zombies when you can write one that has the potential to grab 80% of the machines? These guys may be creeps, but they're not stupid.

So the best thing for the Mac and Linux crowd now is just to keep quiet. Convince enough people to switch, and they'll be targets, too.

Smiling Apple, leaping Linux

Apple has put a friendly face on Unix and watching the Mac gurus who used to make fun of the DOS/Windows command prompt suddenly discover the power of the Unix command prompt is like watching a toddler begin to walk.

Although I complain about the shortage of software for Linux machines, enough applications are available now that Linux is becoming a viable desktop computer. Not yet for me, though, because many applications I consider essential to what I do are Windows-only.

As I talk to some of the more evangelical users of both Macs and Linux machines, I'm struck by how much trouble they're willing to accept from their machines – things that would make them swear at Microsoft and Bill Gates.

An Apple ad parody talks about applications "just quitting" on the Mac. You're using the application and – Poof! – it just goes away. It's a funny bit. And it's also true. My OS X Macs crash far more often than my Windows XP machines. An acquaintance has been through four motherboards (replaced under warranty) on her Mac Ibook.

In other words, the Apple computers and Linux computers have the same kinds of problems Windows computers have. I'm not dissing the OS X, Linux, or Apple – just telling the truth.

I don't see the blind devotion as much on the Windows side, but I have seen it. I recently had an unpleasant conversation with a former Microsoft employee who develops applications for Windows machines. He felt that the Windows operating system was better in every way than what Apple has provided.

Until Apple's OS X came along, I might have agreed, but an operating system based on Unix finally brings Apple into the modern world. The gentleman I was talking with eventually admitted that he hadn't seen any Mac operating system later than System 9. But I digress.

Microsoft security is no longer an oxymoron

The Windows XP service pack 2 consisted mostly of security updates. Microsoft understands, more or less, that security is at least as important as usability.

Not understanding that key concept is what got Microsoft in trouble initially. The company began with DOS, a single-user operating system that didn't allows machines to be connected to each other at all. Security wasn't an issue. With networks, and particularly with the Internet, everything changed. But Microsoft came late to the security party.

Random Thoughts (ISSN 1543-1525 [print] – ISSN 1543-1533 [electronic]) is a publication for clients and friends of William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085.

The company is learning about the vulnerabilities of the Windows operating system and is patching them. It's offering rewards for the arrests of virus writers. It's educating users about computer safety.

In a society that rewards victimization, this may be an unpopular point of view, but it's not Microsoft's responsibility to keep your computer safe and secure. It's your responsibility. As one pundit recently said, "Blaming Microsoft for not building in safety measures is a little like blaming Florida for being in the path of a hurricane." ß

Bank robbery made easy

In November, I was talking with the director of a company that's developing an application that's aimed at making the Internet a safer place to do business. In just today's e-mail, you've probably received at least one or two "phishing" attempts – messages from people who claim to be your bank or a business and want you to "confirm" your data with them. I've written previously about these creeps, but an organization that keeps an eye on phishing says that the number of events increased by 100% in October from the previous month.

Yes, a 100% increase in a single month! But phishing is easy to avoid. If you get a message that claims to be from your bank and offers you a link, don't take the link. Type the bank's URL into the address window of your browser and the phisher will come up empty handed.

Fiendishly clever

What I heard about in November is so simple and so easy that I'm surprised nobody thought of it before. Imagine this:

You own a dog and you get an e-mail from someone telling you about a great new site for dogs. You go to the site, see that there's lots of good information and there's an offer to send you some kibbles for your dog if you sign up for a free account on the website.

You fill in a user name (the same one you use for everything) and a password (the same one you use for everything). You also provide your name and address. Seems simple enough, doesn't it? It's a reasonable offer – all above board – or so you think. But something bad has just happened.

The operator of the website has stolen all of the good information from other websites to make his site look legitimate. He'll never send those kibbles he promised for your dog. But he will find every bank in your town and try your user ID and password.

The next time you visit your bank's website, you may find that your balance is a lot lower than you thought.

Just the beginning

If you think that sounds bad, here's another scenario you won't like, either:

Last week, when you were trying to visit Microsoft's website, you accidentally mis-typed the domain name and landed on a site you didn't want to visit. You closed your browser, but in the few seconds the site was open, it used an Active-X applet to install a small piece of software on your computer.

This small applet is called a "keystroke logger" and all it does is watch what you type. Every 10,000 characters or so, it e-mails everything you've typed to an address in Ukraine.

And, yes, that's as bad as it sounds. Every user ID, every password, every account number you've typed – along with your address, your full name, and maybe even your social security number – they're now all in the hands of an organized crime operation in Kiev.

They're still not done with you

Besides installing the keystroke logger, the rouge website you visited by mistake also loaded up a small "back door" applet that lets your new friends in Kiev connect to your computer whenever it's on.

Now they're using your computer, without your knowledge, to host a phishing website. Tomorrow they'll start using it to send spams for Rolex watches. And next week maybe they'll create a directory that's buried so deep you'll never even suspect it's there and start using it to host a kiddie porn site.

Impossible? Unfortunately, everything I've just described can be done today and is being done today. Millions of computers around the country have back door applications that allow fraudsters to use them for spam and phishing. That's what's behind the 100% increased in phishing messages over a 30-day period. These guys don't buy computers and fill data centers with them. They steal computers and the owners never know.

Opt out!

No one-size-fits-all solution exists to keep you, your identity, your computer, and your data safe.

To avoid this fate, you first need to be sure that your operating system is up to date. Most people should probably turn on Microsoft XP's automatic update feature. I still like to know what's being installed and when it's being installed. If I'm in the middle of an important job, I don't want an automatic update to tell me that I have to reboot the computer.

Next, make sure you have a hardware or software firewall. Maybe both. The free Zone Alarm firewall from Zone Labs is a good choice even if you have Windows XP with service pack 2 because Microsoft's firewall is incomplete. Adding a hardware firewall increases your setup's complexity, but you should consider it if your computer is on line more than a few hours a day.

And third, dump Internet Explorer in favor of Mozilla's Firefox. No browser is 100% safe and you'll still need Explorer for some sites, but use it only for sites you truly trust.

Some new security solutions are in development now, but the best security will always be a cautious, skeptical user. ß

CORNER on the market by A.J. Stinnett

"Charles Price, the CEO of CityGroup quotes John Reed on what organizational culture" is: 'Organizational culture is a set of shared unspoken assumptions.'"