

SecuritySecuritySecurity!

It was the best of times and the worst of times...

I suspect Dickens would be quite surprised to learn how prophetic his words would be over 150 years after he penned them.

THE BEST OF TIMES...

Computers are faster and more powerful than ever, and that trend will continue, at least for the foreseeable future. The components inside computers are getting smaller and smaller at the same time they're getting more and more powerful. Laptops are getting lighter and lighter because of this miniaturization. As a result of this continuing smaller, lighter, faster and more powerful trend, smaller computers like smartphones and iPads and their ilk are on the rise. If you use a computer, or any sort of electronic device for that matter, life is good...and getting better

THE WORST OF TIMES...

Our computers and smartphones (iPhones, Blackberries, etc.) are more and more under attack by the bad guys on the Dark Side. As computers have become more prevalent in cars, refrigerators, coffee pots, Blu-Ray players, etc., they'll come under attack, too...if they have not already come under fire.

Why is the Dark Side attacking us? Well, the attackers used to be mostly teenagers just doing what teenagers do, exploring and experimenting, just to see if they could hack into someone else's computer. Then the teenagers grew up. Now all the attacks, spam, phishing scams, trojans, viruses, keyloggers, nagware, spyware, etc. are mostly about money. If the malware gets into your computer, there's a good chance somebody's making some money.

So how can we protect ourselves? What follows is directed at Windows computers in the home, home office and small businesses. Computers that are part of (connected to) a LAN (Local Area Network) that usually exists in larger businesses typically have an IT person responsible for the health and welfare of the company's computers.

In the war against the bad guys, I think it's important to have reasonable expectations. In this case, a reasonable expectation means accepting the fact that it's impossible to guarantee protection against all types of malware threats. The primary reason is because the attackers (Dark Side guys) will always be one step ahead of the defenders (companies that create the various anti-malware programs).

Another reasonable expectation is an understanding that almost all of the computer programs we use in our everyday computer lives are so complex that they have errors in their logic, meaning the way they're written. These program errors often times create security holes in the program the bad guys use like open doors to attack your computer.

Examples of programs that receive frequent security updates to close these open doors include Adobe Reader, Adobe Flash, Internet Explorer, Firefox, Word, Excel, Java and...drum roll...Windows.

Lastly, because of the above, there is no one program or group of programs we can run on our computers that guarantees protection from all threats.

That being said, what can we do is take reasonable precautions? Below I offer my suggestions, without guarantees, of course, to help you keep the Dark Side at bay.

REASONABLE PRECAUTION #1

Ensure that Windows Automatic Updates is turned on. You must also make sure you install the updates when you're notified they've been downloaded and are ready to install. How do you know when they're ready?

REASONABLE PRECAUTION #2

Become familiar with the little, or maybe not so little, group of icons in the lower right corner of your screen next to the clock. This is called the Notification Area in newer versions of Windows. Put your mouse pointer over each icon and a little popup will tell about each icon.

The Windows update icon will show up here, as will the Adobe Reader update and Java icons. You should know what your regular set of icons looks like, so you'll be able to recognize any change...and possibly spot an upcoming problem.

Often times a program update will have an optional check box that by default will install a program, for which you have no particular use, from some other company. JAVA, Adobe Reader and Flash are prime examples. While these "extras" aren't security problems, they just add needless junk to your computer, and may in fact slow it down. Uncheck these kinds of checkboxes.

REASONABLE PRECAUTION #3

Have an antivirus program installed on your computer. It can be a free program or one for which you pay. It's amazing to me that in this day and age, I still come across computers that have no antivirus program installed. And if an antivirus program is installed, it's frequently not been kept up-to-date. Sigh...

FREE

Security Essentials from Microsoft

http://www.microsoft.com/security_essentials/

Avira AntiVir Personal

<http://www.avira.com/en/avira-free-antivirus>

PAID

NOD32 Antivirus

<http://www.eset.com/home/nod32-antivirus>

Cost: \$58.99 for 1 computer for a 2 year subscription

I've been using and recommending for years

REASONABLE PRECAUTION #4

Keep the programs on your computer up-to-date. This is an almost impossible task to do on your own. I run a FREE program from Secunia. It constantly scans my computer to see which programs I have installed, then notifies me when any of them has had an update published.

Personal Software Inspector

http://secunia.com/vulnerability_scanning/personal/

REASONABLE PRECAUTION #5

SPAM. SPAM is a fact of life, so stop wasting your energy getting upset about it, and take control of the problem. We've all heard for years that we should only open e-mail from trusted sources. Easier said than done. SPAM is designed to fool you. I've had clients fooled, and I've been fooled, too.

I use a program called MailWasher Pro 2011 as a sort of a pre-processor for my e-mail. It allows me to have a secure quick look at my e-mail BEFORE I either download it into my e-mail program or access it with Yahoo or Gmail, etc. It has tools to help identify SPAM and allows me to identify additional items or correct a misidentified e-mail. Afterwards I click the Wash Mail button, and the SPAM is deleted from the e-mail server before it ever gets to my Inbox.

MailWasher Pro 2011

<http://www.firetrust.com/en/products/mailwasher-pro>

Cost: \$29.95/yr for 1 computer

REASONABLE PRECAUTION #6

Malwarebytes Anti-Malware is the current champion for the removal of spyware infections. While it's a great idea to have this free tool already installed on your computer in case of attack, it's even better to purchase it and have it running full time on your computer.

Malwarebytes Anti-Malware

<http://malwarebytes.org/>

Cost: \$24.95

REASONABLE PRECAUTION #7

Your computer should be behind some kind of hardware based firewall. Yes, Windows has its own firewall, and some of you may be using Internet protection suites from McAfee, Symantec, Eset or others that include and take the place of the Windows

firewall. These are all software based firewalls, and they just aren't enough. We need yet another layer of protection.

A hardware based firewall usually comes in the form of a router. Sometimes the router is a separate box that you've purchased to be used in conjunction with your DSL or cable modem. Many newer DSL and cable modems come with the router technology already installed within them, negating the need for a separate router.

The key thing is to find out whether or not your computer is behind a router's firewall. This is very easily accomplished by following the steps listed below.

1. Click the Start button to display the Start Menu.
2. Click All Programs, or Programs, depending on your Windows version.
3. Click the Accessories folder.
4. Click Command Prompt. This will open a small black window with white lettering.
5. Key-in: ipconfig, then press the <Enter> key. A bunch of tech gibberish will be displayed.
6. Look for IP ADDRESS
7. Following the IP ADDRESS will be a set of 4 numbers with dots between them and will look something like 192.168.1.100.
8. We're only concerned with the first number group, 192 in the example above.
9. The first number group should be 10, 172 or 192, with 192 being the most common.

If your IP address starts with any number other than the three numbers listed above, you must purchase an Internet router because your computer is very visible on the Internet. What this means is that your computer is more "hackable" by the bad guys.

Routers may be purchased at almost all stores that sell computers. They are fairly inexpensive, starting at about \$50. They are also extremely easy to install. It's usually only necessary to connect the network cables and power according to the picture in the instructions. I've NEVER found it necessary to use the software CD that comes with most routers. All they do is usually install needless software.

REASONABLE PRECAUTION #8

Passwords

Let's face it, passwords are a pain in the butt! Let's face it, passwords are a fact of life, Internet and otherwise. It is what it is, so get with the program and get serious about passwords. Why? Because we continue to see web sites of all kinds getting hacked on a regular basis with our personal information being stolen by the bad guys.

Do you use the same password as often as you can on the internet? Do you only change your password under duress from a website? Is your password as short as possible? Is your password all lower case or all numbers? Did you just say "D, all of the above"...like most of us?

It's time to take passwords seriously, and make an effort to begin using strong passwords. Strong passwords are:

1. At least 8 characters long
2. Contain at least 3 of the following 4 components:
 - a. Uppercase letters A, B, C ...
 - b. Lowercase letters a, b, c ...
 - c. Numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
 - d. Contain any of the following special characters: ` ~ ! @ # \$ % ^ & * () _ + - = { } | \ : " ; ' < > ? , . /

More password Best Practices:

1. Does not contain your user name, real name, or company name.
2. Does not contain a complete dictionary word.
3. Is significantly different from previous passwords.

We try to strike a balance between security and ease of use. In this cause we are helped by Roboform, a very secure, easy to use password manager and website form filler. Aside from remembering your website password and be able to login automatically, Roboform can fill in online forms for you. This is extremely use and time saving if you do a lot of purchasing on the Internet. As a bonus, Roboform has a clickable button to generate strong passwords!

Roboform

<http://www.roboform.com/>

Cost: Free for limited use or \$19.95 for unlimited use

REASONABLE PRECAUTION #9

Backup...Backup...Backup

I don't care what program you use, but get yourself an external hard drive for backup. Many of them come with some kind of backup program already installed.

My favorite backup program for many years has been Bounceback Ultimate from CMS. The reason I prefer this program is because it backs up files in their native format. That means you can look at your backup and easily recognize the files on the external backup drive. You don't need any special program or even Bounceback itself to recover files.

Bounceback Ultimate

http://www.cmsproducts.com/products/backup_software/bounceback/default.html

Cost: \$69.00

THE BEST PRECAUTION of all...

is to use your own native intelligence and common sense. As long as you remain aware that threats exist when using the Internet and use common sense when looking at e-mail and visiting websites, you'll have a much better chance of remaining safe.

Personally, I refuse to be intimidated by the various threats that go along with using the Internet in this early part of the 21st century. For me, it is most definitely the BEST of TIMES!

December 2010

Mark Perlstein
mark@perlstein.us
www.perlstein.us

Copyright 2010 Mark Perlstein. All rights reserved.