January 2014

TechTidbit.com

brought to you by Tech Experts

Windows XP: High Risk For Your Business

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Microsoft will end all support for Windows XP on April 8, 2014. This means that everyone using XP beyond this date will no longer be able to receive security updates from Microsoft, which will turn Windows XP into a liability.

Despite the fact that Windows XP is a dozen years old and sunsets in under five months, it is still widely used by millions of users and claims a 21% market share. Rest assured, the hackers are gearing up for an all-out assault on XP users this spring.

Security reports from the Malicious Software Removal Tool and Microsoft's free Security Essential program (which scans 400 million Outlook.com accounts and millions of Office 365 accounts), reveals that XP is by far the most infection-prone operating system.

Here are the latest infection rates (the number of infected computers for every 1,000 systems scanned) broken down by OS that contained malware.

Windows XP SP3:
9.1 per 1000 scanned.
Windows Vista SP2:
5.5 per 1000 scanned.
Windows 7 SP1:
4.9 per 1000 scanned.
Windows 8:
1.6 per 1000 scanned.

The data show that Windows XP is almost twice as likely to get an infection compared to Windows 7, and it is six times more likely to be hit with malware than Windows 8. Those figures should prompt even the most ardent XP user to start planning for an upgrade.

It is important to remember that malware is written to attack any system it encounters, and we can see that, by looking at the malware encounter rate from these same security reports, the percentages of computers having encounters with malware is fairly even across the different operating systems.

Windows XP SP3: 16.3%
Windows Vista SP2: 16.5%
Windows 7 SP1: 19.1%
Windows 8 RIM: 12.4%

This report shows that using the latest operating system, such as Windows 7 or Windows 8, is the safest.

Researchers provide a technical explanation as to why newer Windows operating systems have better security: "Microsoft has steadily incorporated defensive technologies into Windows with each new version. The only major technology XP had was Data Execution Prevention (DEP), and even the implementation of that has improved greatly in subsequent versions."

It is human nature to put off a large upgrade project, especially for a small business where budgets are tight.

Part of our service includes a comprehensive evaluation of your systems and network, with the goal of providing you a report showing which machines on your network are vulnerable, which can be upgraded, and which should be replaced.

We use automated tools for much of this process, so we're able to offer this service to clients, and prospective clients, at a markedly reduced consulting fee. Please call the office at (734) 457-5000 to schedule your appointment.

Online Banking: Safety And Security Precautions

by Jeremy Miller,
Technician

There are many avenues of attack when banking online safely. Many people simply use a computer that is attached to the Internet with little to no precautions at all. Some bank online even if they know there are issues with their computer or virus infections on their computer.

I will cover three levels of precaution that you can take to ensure your online banking information stays secure: simple, advanced, and paranoid. As the level of precaution increases, it will be more time consuming and difficult but worth it if you want to keep your online banking experience safe and secure.

Simple Precautions

To keep your information secure you must make sure that your computer is fully up-to-date with all Windows Updates and other software patches. Software vendors like Microsoft release security patches regularly to close exposed security holes in their software. Without patching hackers can use known-vulnerabilities to attack your computer.

Next you must make sure that you have anti-virus software installed and it is up-to-date with the latest virus definitions. You must also have your anti-virus run scans regularly to make sure the computer is clean of any known infections.

You should always look in the Uniform Resource Locator (URL) bar to make sure the web address you are accessing is the correct one. Also make sure that the first five characters are HTTPS.

This will ensure that your traffic is encrypted, which will make your entire web traffic look like gibberish. If your first characters are only HTTP and not HTTPS then hackers would be able to read your password in plain text.

Lastly, you must only do online banking from trusted-networks like your home network or in some cases your work network.

Anyone else attached to your network has the possibility to access your bank information if they have the know-how.

To be sure you are on a secure network, you should not use online banking from public or free networks that anyone can access.

When you do this you ensure that only you and your Internet Service Provider (ISP) can view your online traffic.

This will also protect you from man-in-the-middle attacks (MITM). These attacks are when a hacker is in between you and your target destination usually a router. Hackers using MITM attacks will be able to see all unencrypted traffic.

Advanced Precautions

You must ensure you are implementing all simple precautions, including a few more steps you can take to up your protection level.

Run a full virus scan before accessing your online bank account each time. Your system will be clear of known infections, plus it gives you significantly less risk of an infection since your last scan. A full scan looks at every file on your computer and checks it against a known virus database.

You can also configure Windows Firewall to prompt you before allowing traffic in or out of the computer, or you can install a software-firewall to scan your active Internet traffic.

The firewall will prompt you with pop-ups to ask if specific connections are allowed. This will allow you to approve or deny all traffic on your computer. Usually firewalls have different settings to allow you to choose the level of security this firewall will provide.

Paranoid Precautions

This is the most secure of the three and implements the previous precautions. It would be best to boot to a new operating system every time you need to access your online bank account. You need to know how to change your computers boot order and how to create a bootable USB drive or disk.

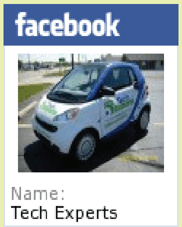
There are a number of free operating systems that you can load onto a disk or USB drive. WinPE will allow you to boot into a portable version of Windows. This will be a clean installation with no additional software installed.

You can also use the more widely available bootable Linux distributions as a clean bootable operating system to access your bank information. Ensure you are getting your distribution from a reputable vendor.

Most Linux distributions are free. Downloading a reputable vendor will ensure that there isn't malicious software pre-loaded into the operating system.

If you are interested in enjoying a safer browser experience you can contact us and we can answer any questions or concerns as well as help you implement any of these precautions.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

HIPAA Risk Analysis And Assessment

by Michael Menor,
Network Technician

The phrases “risk analysis” and “risk assessment” are becoming incredibly commonplace today. They’re littering the blogosphere, popping up in advertisements by newly-announced, so-called experts and being “webinar-ed” to death.

In reality, most people promoting these phrases don’t know what they’re talking about. They don’t know what they’re talking about, I’ve come to discover, because most people don’t understand what risk itself means.

Understand Risk To Conduct Analysis

In today’s increasingly more privacy- and security-minded world, and especially in healthcare, the state of risk management of information is a mess!

This problem comes about for many reasons, including but not limited to the following:

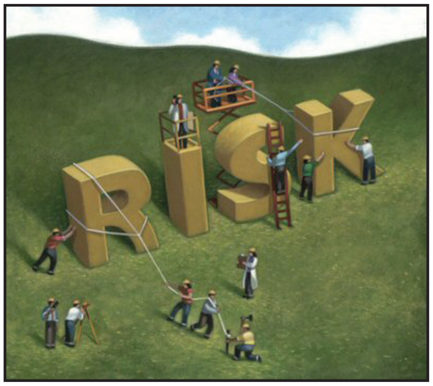
There is little agreement on standard terminology, approach and tools. Key risk-related terms such as assets, threats, vulnerabilities, controls, likelihood and impact are misused and sometimes used interchangeably. One does not find these terms in many other professions. All physicists know what velocity, acceleration, mass, energy, etc. mean. All accountants agree to definitions of basic terms such as debits, credits, balance sheets, assets, liabilities, etc.

Many so-called “experts,” some recently-minted and/or self-proclaimed as such, don’t understand basic risk fundamentals.

Most individuals do not understand that you simply can’t observe risk and that risk is a derived value.

You simply cannot begin to conduct a bona fide risk analysis if you don’t understand what risk is and what risk is not.

There is huge inefficiency and ineffectiveness in protecting the privacy and security of Protected Health Information (PHI) and electronic PHI (ePHI).



As of October 24, 2013 the PHI/ePHI of 26.9 million fellow Americans have been disclosed according to the HHS/OCR “Wall of Shame.” For example, laptops with unencrypted hard drives being stolen from Advocate Medical Group.

Actions To Take

First and foremost, organizations must understand some key, fundamental points about risk before they embark on completing a risk analysis. For example, I present you with five images and ask you to indicate the level of risk (high, medium, low, no risk) you observe in each image.

The images include a bald tire, the same bald tire turned into a tire swing in a backyard, a frayed rope tied to a beam, the tire swing in a tree perched over the edge of a cliff and, finally, a child swinging in the tire swing in a backyard.

What was the greatest amount of risk you observed? I would guess you “saw” high risk in more than one of the images! Some “saw” risk in all the images. 1) You cannot “see” risk; it must be evaluated; and, 2) In reality, there is no risk in any of these images.

Here’s what happens over and over again:

People make assumptions and make things up in risk analysis.

People don’t understand this fundamental truth about risk – you can’t have significant risk without the potential for significant loss or harm.

People tend to relate potential vulnerabilities (e.g., frayed rope, bald tire) with risk.

People forget that one must consider likelihood or probabilities of bad things happening and of impact or harm.

The most important actions organizations must take if they don’t understand risk are to “train up” and/or farm out the work to experts.

Continued on Page 4

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

**15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com**

How Much Power Are Your Devices Hogging?

by David Stone
Technician

Do you find yourself looking high and low for an outlet, a cord or a charger for one of your many electronic devices?

Today's world finds most people switching back and forth between a mobile device, car infotainment system, workplace computers, home computers and multimedia devices.

It would be wonderful if all of these electronics used the same power adapter and charge time. Unfortunately for you, the consumer, it does not work that way.

Most electronic manufacturers have their own proprietary cords, batteries and charger adapters. You can blame costly patents, industry rivalries, or just the desire to be different as the culprit behind all these seemingly trivial decisions.

Regardless of the reasons, knowing how much power each device draws or requires for charging quickly will empower you as well as save you some money on your electric bill.

Belkin has created the Conserve Insight to provide you with the data needed to monitor the watts you're using, how your carbon footprint is affected and how much money you're giving to the power company.

Setting up the Insight is pretty simple and straight forward. Simply plug the Insight into your outlet, then plug in your device and start to monitor your device power usage.

Hit the $ button, and it will switch back between how many watts your currently using as well as how much it will cost you on a monthly basis.

It will even keep track of the carbon dioxide produced in order to power that device.

Another cool feature is the averaging mode option that activates after 45 minutes and projects the carbon dioxide and dollar amount cost for the entire year.

This does not work in watt display mode that only shows you real time usage updates.

The five foot cord that connects the display unit to the outlet adapter is a great improvement over similar products, as you no longer have to crawl around under desks and tables in order to see the read-out.

A bit of form-factor goes the extra mile and makes the Insight look stylish and at home on your desk or workspace.

The best feature by far is the conserve option that allows you to set a time limit for how long the device will draw power.

There's a switch on the side that allows you to choose from one of three time increments, 30 minutes, 3 hours or 6 hours are your only choices, but most devices today will never take more than six hours to charge.

The Insight will power itself off after the time has elapsed, saving you the hassle of unplugging each device after they're fully charged.

Belkin has taken the steps to innovate a product that has plenty of market share, and will most likely win over consumers for its ease of use and reliability.

Using technology to better manage your high tech devices and power usage, plus you can use it to manage your Christmas lights!

HIPAA Risk Analysis And Assessment, Continued From Page 3

And they must remember these truths:

Risk can only possibly exist if three conditions are met: an asset like a laptop with ePHI, a threat to that asset (e.g., a thief may steal it) and a vulnerability (e.g., it is not encrypted) that may be exploited by that threat.

For any single asset (e.g., a laptop with PHI), there may be many different threats and many different vulnerabilities; therefore, there may be many risks to be identified, assigned a value and prioritized.

Controls may already have been implemented or may be implemented to mitigate the likelihood of a certain threat exploiting a certain vulnerability. Controls come in several forms, often categorized as administrative, physical or technical.

Risk has an impact or harm component.

When it comes to health information risk, the adverse impact or harm may come about if the confidentiality and/or the integrity and/or the availability of that information is compromised.