April 2018

TechTidbit.com

brought to you by Tech Experts

Watch Out For This Overlooked Threat In Your Business

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

With the risk of being hit by hacking, malware, and other forms of cyber-crime so high, most organizations go to great lengths (and expense) to protect their networks and infrastructure.

However, one major security risk that's being overlooked is the printer!

All too often, print falls beyond IT teams' field of view and is left hanging in an abyss ready and waiting for hackers to take advantage.

Here are some interesting statistics: According to research that was conducted by the Ponemon Institute, 64 percent of IT managers are suspicious that their printers have been infected with some form of malware; however, just 54% of organizations include printers in their security strategy.

With organizations placing all eyes firmly on network security, the major threats that are posed by printing devices that are directly connected to these networks are all too often completely overlooked.

So, what actions can you take to reduce the risk of print-related breaches?

Monitor your print devices

Regardless of how many printers are connected to the network, keep tabs on every single one. You can make this job easier by using remote management software.

Utilize pull printing

Also known as "follow-me printing," this security technique holds a print job on the server until the person who executed the print command is physically present at the printer and authenticates themselves using a card or code.

This reduces the risk of sensitive documents being left unattended in the print room.

Encrypt data

Did you know that most printers and multi-function devices contain a hard drive where your print jobs and copies are stored?

In many cases, years of images and print jobs are retained on this drive, and can easily be read by hackers or criminals when the machine is removed from service.

You need to protect your documents and ensure they are always stored on secure hard drives. Consider fitting your printers with hard drive encryption functionality to prevent data from being stolen.

Include print in the overall security strategy

As printers are connected to your network, they should form an integral part of your security strategy. Ensure they are protected in the same way you would protect any other device on the network.

Follow data protection mandates

When it comes to printers, user behavior represents a critical threat. Develop a clear security policy and ensure it is followed across the organization.

According to research that was conducted by the Ponemon Institute, 64 percent of IT managers are suspicious that their printers have been infected with some form of malware; however, just 54% of organizations include printers in their security strategy.

Stopping Power Surges Before They Reach Your Equipment

"The one thing you have to keep in mind is if you are not protecting your computers, printers, and display devices from power surges, then you are taking the risk of losing valuable data on your storage devices."

Ron Cochran is Help Desk Supervisor at Tech Experts.

We all have some sort of electronic device that we plug into the wall, either to charge the battery or power the device. While these devices are connected to the power source in your home or office, they are being subjected to power surges on a regular basis. Some of these surges can damage your electronic devices.

The main source of a power surge is inclement weather. A surge protector or suppressor will keep your devices safe from inconsistencies in power delivery.

Most people will use power strips to connect more than one device to an outlet and these are OK to use, but they do not offer any surge suppression attributes.

A legitimate surge protector or suppressor will have a rating that is measured in joules, which represents how much of a power surge it can mitigate without damaging your electronic devices. There are several manufacturers of surge protectors for home use, whole-home use, and even industrial applications.

Depending on your needs and budget, you could install a whole-home surge protection system which would protect all of the devices in your house from a surge.

If you are budget-minded, then picking up a couple brand-name, surge-protecting power strips for your entertainment system or electronics charging station would be sufficient.

The one thing you have to keep in mind is if you are not protecting your computers, printers, and display devices from power surges, then you are taking the risk of losing valuable data on your storage devices.

You are also opening yourself up to the potential need to replace faulty equipment due to the power surge. These repairs are not cheap and the data that you lost due to the power surge is most likely irreplaceable, unless you have a backup solution implemented.

Now, once you have decided to purchase a surge protector, you will need to decide how many and what devices you want plugged into it, keeping in mind the total power draw of all of the devices.

You do not want to use a lot of high-power equipment on one single surge protector because they are rated for a certain power draw; if you are consuming more power than they are rated for, they might not be able to do their job properly.

On top of an overloaded surge protector having issues operating and protecting your devices, it poses a fire hazard due to wires being overheated.

Winter is over and we are entering the stormy season of spring. Power surges will be happening in our area before you know it.

If you are concerned about protecting your home or office equipment from a power surge, then now is the time to evaluate your needs for a surge protector.

We'd be more than happy to conduct a site survey, then recommend and install surge protectors for your business needs.

Protect Yourself Against The Phone "Port-Out" Scam

Chances are that you probably haven't heard of the port-out scam. However, just because it is something that has yet to attract widespread attention doesn't mean it's not a threat you should take seriously. Let's take a look at why.

What Is a Port-Out Scam?

It's very common for people to take their existing phone numbers with them when they switch mobile provider. Recently, unscrupulous individuals have been taking advantage of the ease with which this can be done by porting other people's numbers and essentially taking control of them.

Here's how it works: Someone calls your carrier or visits the store and pretends to be you. They then instruct the provider to port your number to a new carrier. Without warning, you find your cellphone service has been cut off, and some stranger has complete control of your number. A variation of this is SIM hijacking, which operates in a similar way but the attacker orders a new SIM.

Why Should You Care?

Losing the ability to use your phone is the least of your worries. Once the attacker has control of your phone, they will receive all your messages. If you have set up banking security measures that involve SMS authentication, the hijacker can potentially access your bank account and many other sources of highly sensitive information.

How To Protect Yourself

Fortunately, it's really easy to avoid the port-out scam. All you need to do is add a security PIN to your account. From that point onward, people will not be able to make any type of change to your account without citing the PIN. As such, you are protected against both the port-out and SIM hijacking scams. Most carriers will let you set a PIN quickly and easily online or via the phone.

What Are The Seven Basic Parts Of A Computer?

Chris Myers is a field service technician at Tech Experts.

People usually notice performance issues in their computers after five to six years. When that starts to be the case, a hardware upgrade can be a real boost to both performance and the computer's lifespan. Where do you even begin when upgrading a computer, though?

Even though their inner workings can seem complicated, computers are actually made up of a few key parts.

Core Upgradable Components - RAM

Random-access memory comes in small removable cards (or "sticks") that are inserted into the computer's motherboard. RAM modules usually come between two and four gigabytes each, used in sets of two.

In a computer, RAM holds the code and data actively used by the CPU. Every program you have open takes up a certain amount of space in RAM. For example, using an Internet browser with 8 tabs open takes about 1 gigabyte of RAM.

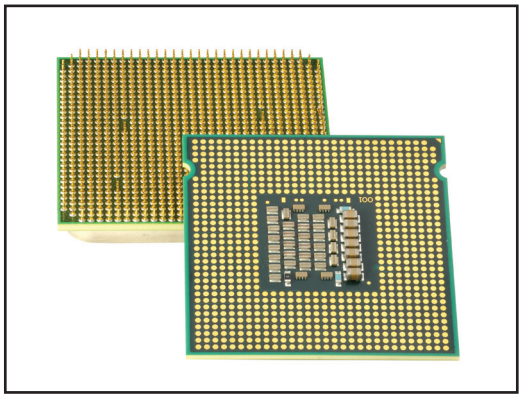
Using up 95-100% of RAM capacity will usually cause the computer to crash, so it's something you want to avoid. Adding more RAM to a computer will allow the user to have more programs running at once.

Hard Drive

The hard disk drive (HDD) stores the operating system and all user files on several small disks, called platters, stacked on top of each other. They are read by a mobile arm, much like record players.

Hard drive performance is determined by how much data the manufacturer is able to fit on each platter (areal density) and how fast the platters spin (RPM). Usually, the only public number is the RPM, either 5400 or 7200. A 7200 RPM hard drive is about 30% faster than a 5400 RPM one.

If you want real performance though, you need a solid state drive (SSD). Solid state drives are five times faster than 7200 RPM hard drives. They just have a little less storage capacity and can be more expensive.



Graphics Card

The graphics processing unit (GPU) handles graphics and image processing. Most business computers don't have one since they just use database or word-processing applications. However, if you use any graphics intensive programs like computer-aided design (CAD), computer-generated imagery (CGI), or digital content creation (DCC), you will see a massive performance boost after installing a graphics card.

Other Parts In A Computer - CPU

The Central Processing Unit is the core of the computer. Every action taken by the user or a program is processed one-by-one in a CPU thread. Modern CPUs have multiple cores so that it can have more threads running at once. Four cores are the standard amount now.

CPUs are the main source of low performance on older PCs, especially if they were bought for a fairly low price to begin with. However, changing a CPU often requires changing the motherboard as well. Therefore, it is not a cost effective solution versus buying a new computer.

Motherboard

The motherboard is a large circuit board that all other PC components connect to. It is basically the framework that turns all of those pieces into a working computer.

Case

The case refers to the outer shell around all of the components. Most cases come with several cooling fans installed. The main thing to remember about cases is that the smaller the case, the hotter the computer will be.

Power Supply

A small box with its own fan that runs power cables to all of the other parts. More expensive computers usually come with better power supplies, which is a good thing considering the severe damage that can occur when a power supply fails.

"Even though their inner workings can seem complicated, computers are actually made up of a few key parts."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(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) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Windows Fall Creator's Update: Breaking More Than It's Fixing

Jason Cooley is Support Services Manager at Tech Experts.

Microsoft dominates the world of operating systems. Windows has been a part of our lives for years and some of us can't remember a world without it.

Each time Microsoft rolls out a new operating system, it is updated and patched for years for various reasons.

Over the lifespan of a Windows operating system, there are various security updates perhaps more than any other type of update.

There are fixes for issues, whether that's problems with Windows itself or interaction with other hardware and software.

Then there are the outliers: Windows feature updates. These updates typically introduce new features or changes to the core function of the operating system. Feature updates can improve the user experience for many people.

Windows 10 launched in 2015 and, like all of its predecessors, did not launch with perfection. There have been numerous updates of all kinds since its launch. Those security patches, hotfixes, and even a handful of feature updates had rolled out by October of 2017.

That is when Microsoft released the Window's Fall Creator update. This update was going to create a better user experience. Personal connections were going to be easier to make.

A new application allowing you to resume work or browsing started on a mobile device like a smartphone on your computer was introduced as well. There were a few security updates as well.

All in all, the Fall Creators Update was going to fix a few bugs and introduce some quality-of-life improvements.

In previous versions of Windows, the updates were able to be shut off and postponed.

Large scale feature updates are known to have some complications when rolled out.

That is why these updates are not "pushed" when initially launched, but available to download as an optional update at first.

Upon this introduction window, there were, as expected, reports of problems coming in. What was not expected was the range of issues and the severity of some.

The first issue arising from the release of Windows 1709, the Fall Creators Update, was the update failing to install.

Many people reported issues of an error when attempting to install the update. The initial portion would install, but the finalizing of the updates upon a restart would fail.

If that wasn't frustrating enough, if the update did manage to install, it was reported that the applying updates portion could take two hours (and in some cases as many as ten hours).

Then, let's assume you got that far. Maybe you want to use Microsoft Edge, the Microsoft browser of choice. With the 1709 update, many users found that Edge was essentially broken. It would crash repeatedly.

Then, bring in the numerous broken drivers. Imagine an update breaking your Ethernet adapter. It happened. Applications disappeared, began opening on their own, and in some cases just didn't work. The problems continued to roll in.

Many of these issues were resolved in a timely fashion and some were not. In mid-January, Microsoft declared the Fall Creators Update ready for business. This means that the update would be pushed out to anyone that was not already using it.

After 3 months, many issues were still present and others would soon be discovered.

Many users of corporate software and other specialty software were surprised by software that no longer worked. In some cases, the suggested fix was to roll back the update, which will force itself to reinstall shortly after.

There have been some big patches to fix these issues since January and I'm hoping that in another three months Microsoft will have all of these issues resolved.