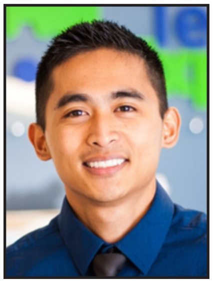
June 2016

TechTidbit.com

brought to you by Tech Experts

Technology Considerations When Moving To A New Office



Michael Menor is Vice President of Support Services for Tech Experts.

Moving your office is never an easy task. You have to move furniture, personal objects, and above all else, your technology infrastructure. There's nothing simple about moving your office's technology, but it's still nothing to get worried about. That's why we're here to help - from suggesting the optimal network cabling, to the proper deployment of new and improved technology solutions.

For example, let's take a look at your office. You have a certain number of workstations, one for each of your employees. These workstations need to be connected via cable to your business's network. Otherwise, your team could go without required software, data, and other important resources. Your cabling infrastructure could quickly grow to be uncontrollable, especially if you don't approach your cabling procedures correctly.

Another issue that you might encounter comes from equipping everyone with the right communications solutions. The most notable problem is setting up phone lines for everyone who needs them. Adding new lines is far from a simple task and it can quickly exceed your budget if it's not planned out in advance. Adjusting for growth is also much more difficult, considering you have to add and/or remove lines as needed, making for an expensive investment.

How about your physical files? Chances are that you would much rather make the move without lugging unnecessary items, such as file cabinets. The problem is that your organization might be torn between keeping the files and getting rid of them. It makes sense to take inventory before committing to such a move, especially if you have files you're required to keep.

Tech Experts offers several services that are designed to help your business make its move much easier. In fact, our services aren't just convenient for businesses that are relocating; they're great for most any business that wants to maximize productivity.

Cloud storage and virtualization

If you're having trouble providing information to your entire infrastructure, you can use cloud computing and cloud storage to provide access to applications, software, and data required by your employees throughout the workday. Doing this helps you avoid unnecessary cabling and allows for similar data access capabilities. As long as your employees have an Internet connection (say, through a WiFi signal), they'll be able to connect to the cloud and access information. In other words, they can work from anywhere, leading to more productivity.

Voice over Internet Protocol (VoIP)

With a VoIP solution, your business can take advantage of your Internet connection to make and receive phone calls. Since the only connection you need is to your Internet, you can skip out on the complex cabling required of traditional telephone systems. You still need to keep an eye on your bandwidth, but if you use a Tech Experts-provided solution, we'll help you ensure that you get the most out of VoIP with minimal incident.

Electronic records storage

If your organization is having trouble with file storage, Tech Experts can equip your business with a solution that's designed to help you eliminate unnecessary physical file storage systems. Instead, you can store your files in a digital, compliant space that's optimized for security. Since your files will be stored digitally and protected with data backup, you'll be able to quickly get back up to speed.

A new office means a second chance to start over, so why not do your IT the right way? For more information about how we can help your office relocation progress more smoothly, give Tech Experts a call at (734) 457-5000.

> A new office means a second chance to start over, so why not do your IT the right way?

We're proud to partner with the computer industry's leading companies:

Microsoft Partner

Microsoft Small Business Specialist

Business Partner IBM

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.

Do You Have Internet Privacy At Work?

> *"...if someone at the office is using the work Internet, it is more than possible that every website visited is being kept track of in one way or another."*

Luke Gruden is a Help Desk Specialist at Tech Experts.

Sometimes, when there's a break or the work day is slow, it can be tempting to check on a couple different websites. In doing this, would anyone know what websites were visited? Other than the people around, who else would know what sites might have been visited? It may come at a surprise that there could be many different people later on - or even immediately - that find out about the websites that were visited.

It is common for workplaces to have a firewall that prevents certain websites from being visited. Along with blocking certain websites, firewalls usually keep track of all the different websites that have been visited and by who.

Any time a website is visited that has been blacklisted (blocked), this usually triggers an alert to the IT department or management, so they can look over who tried to connect to a blacklisted site. From there, if IT or management feel it is necessary, they could look over the entire history of websites that were visited by a user or a group of users.

Now, let's say for some odd reason that the business does not have a firewall or other device that keeps records of websites visited - could websites that were visited still be discovered?

Well, the computer someone uses also keeps records of websites that they have been visiting, which can be accessed by IT.

Some clever users might be able to remove their footprints from their workstation computer, but they may not have access to something like that.

There is another way that websites visited from a workplace can be tracked without a firewall or looking into the computer files.

If the websites visited warrant any legal action or an investigation is happening at the company, the ISP (Internet Service Provider) can release any and all records of websites visited and exact information of what was done. There is no way to get around this as you need an ISP to use the internet.

There are even more ways to find out what websites are being visited than what was mentioned here. In short, if someone at the office is using the work Internet, it is more than possible that every website visited is being kept track of in one way or another.

If you follow the rules of your workplace and visit only the type of websites allowed by the work place, you shouldn't have much to worry about. As a rule of thumb, you should only visit sites and do things that you don't mind the public or workplace knowing about. If you ever see "NSFW" (Not Safe for Work), do not visit or have anything to do with it while on the work Internet.

Only surf the Internet when you are allowed to surf the internet. Don't visit websites or open emails where the main site or email sender is unknown. With these tips in mind and a better awareness of how a person can be tracked on a business network, you can make better choices while on the company's Internet.

Why Do I Keep Seeing The Same Ads On Multiple Websites?

This is the result of an online advertising approach known as site retargeting which tracks your online behavior to offer you targeted advertising. At first glance, this may seem like it is posing a security threat, but there are assurances that tracking is done anonymously.

Site retargeting is based on a pretty simple concept. Whenever you visit a website that may want to show you an advertisement, it puts a digital tag called a cookie on your browser. Then, when you visit another site with an area to display paid advertising, the information on that particular and other tags is used to choose an advertisement you would likely be amenable to click or watch. The hope is that, while you may have missed an opportunity to purchase an item once, you may be more inclined to complete a purchase at a later date.

If you don't appreciate being such a target for advertisers, there are ways to block and delete cookies and to stop ads from reappearing. To delete existing cookies on your browser, choose the option to delete cookies under the settings. Also, if you see an icon that says AdChoices next to recurring advertisement, you can click that icon to stop the reappearance of that particular ad. Most browsers also have a Do Not Track option in their settings, which prevents your browser from being tagged in the first place, but that also means you can't save passwords or use other tools that are also dependent on cookies. You could also surf the web in private browsing mode (accessible through your browser's settings) or use an ad-blocking service like Ghostery or AdBlock Plus.

Windows 10 Goes Back On The Shelf

Brian Bronikowski is Field Network Engineer at Tech Experts.

While it was broadcast everywhere during the launch of the newest operating system from Microsoft, users of Windows 7 and 8.1 are nearing the end of the free upgrade period. The infamous “Get Windows 10” app has been hounding users for quite some time now and most will be happy to hear that it will be gone nearing the end of July.

That, however, is only after Microsoft ups the ante attempting to reach their goal of one billion Windows 10 devices within 2-3 years of launch. The question many users should be asking themselves is simple: what does this mean for me?

First and foremost is price. After July 29th, there will be no opportunity to obtain a free upgrade. Instead, home users will need to purchase a license for the new system that would run them $119.00. Businesses and those in need of a professional Windows license would look at a price tag of $199.00.

Neither of these seem like friendly numbers to your average user or business owner. Those who have upgraded and switched back to their previous operating system are in luck, however. Once upgraded, you obtain the Windows 10 key indefinitely. In the future, a fresh install of Windows 10 will automatically activate and update as per usual.

Before we get there however, we have one last hang-up from the software giant. It would seem that Microsoft wants to get as many free upgrades in the world as possible.

This is quite a feat when just over half of Windows-based computers are still running Windows 7. How do they plan access that user base?

Automatic upgrades seem to be their answer.

While many have claimed to have experienced Windows 10 upgrading by itself, it seems to be a reality in the very near future. The actual update for Windows 10 comes through as any other update you may be familiar with.

The catch with 10 is that it was previously an optional update, yet Microsoft will be putting it in the “Recommended Updates” category. As such, many users will install the update files without their knowledge. In the meantime, the pre-mentioned “Get Windows 10” app will schedule the upgrade for them in a suspicious window. It looks similar to the previous screen but instead of having a cancel button, they have replaced it only with “OK”.

But what does a single button really cause? For some fast-paced users, they may misunderstand and click the new button thinking that it’s putting off the update.

Little do they know that within a day or two, they’ll find themselves mid-upgrade. There is one way around this once the update is scheduled: a link will appear on the same screen that will allow you to stop the automatic upgrade.

Microsoft leaves it to you to navigate to the link and pages beyond to stop your free upgrade. Luckily, the IT guys at Tech Experts are able to get past this or downgrade those that have recently updated against their will.

The lesson here is a plain one. Users need to keep a look out and understand what is happening to their PC if they hope to retain any control over it. Microsoft’s newest operating system does have many benefits and features that make it very appealing.

However, it isn’t for everyone. If you’re accustomed to what you’re using, the upgrade isn’t a necessity. That said, you should keep in mind that Windows 7 will experience end of life in 2020.

> *“While many have claimed to have experienced Windows 10 upgrading by itself, it seems to be a reality in the very near future.”*

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

Another Major Ransomware On The Loose: Locky

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

Ransomware, a virus that essentially holds a computer user's data hostage for a monetary reward, isn't a new threat. It is in fact, becoming more prevalent with an estimated 35% increase of attacks in the past year alone.

One of the newest forms of this virus is known as Locky, which finds its way onto unsuspecting users' devices through vulnerabilities in the Adobe Flash Player. This ransomware was detected by Trend Micro, and the type of operating system used seems to have little effect on risk. Locky has infiltrated systems through Windows, Mac, Chrome, and Linux.

Many of the Locky attacks, however, have affected Windows 10 users who are unknowingly using outdated versions of the Adobe Flash Player. Anyone running the 20.0.0.306 or earlier versions of Flash is at risk of Locky taking over data and holding it hostage for payment.

Therefore, the simplest way for people to protect themselves from this new ransomware is to ensure they are running the most recent version of Flash.

To do this, access Flash content within your browser and right click on it. Then, choose "About Adobe Flash Player" to view which version is being used. Alternatively, users can visit the Adobe website, which can automatically detect the installed version and also offer the option to upgrade to the most current one.

Locky ransomware isn't just spread through Adobe Flash. It also can find its way onto systems through attachments in spam emails. In this case, the emails have most frequently been distributed through the same botnet responsible for sending out the online banking malware Dridex.

While actual numbers for how many people have fallen prey to Locky infections are not public, security companies have revealed that the majority of the ransomware attacks have taken place in the United States, Japan, and France.

The amount demanded to remove Locky from affected devices is usually around $100, but security experts suggest not giving in to such demands. Instead, victims are advised to create a backup of files and seek help from your IT provider.

The best defense against such attacks, however, is in prevention. Regularly update your operating system and frequently used programs, never open suspicious emails, and only log in as an administrator on your computer system when and as long as you absolutely must to prevent hackers from intercepting your login credentials.

Major Password Breach Uncovered

Some people collect antique trinkets while others collect more abstract things like adventures. There's someone out there, however, collecting passwords to email accounts, and yours just might be part of that collection. To date, it has been estimated that over 273 million email account passwords have been stolen by a person or entity now called "The Collector." This criminal feat is one of the largest security breaches ever, and the passwords have been amassed from popular email services, including Gmail, Yahoo!, and AOL.

It is unclear exactly why "The Collector" has procured so many email passwords, aside from the fact that the individual is trying to sell them on the dark web. The puzzling part of this, however, is that the asking price is just $1. So, the hacker may only be seeking fame for achieving such a large-scale feat.

The email account credentials may have more value in being used in an email phishing scam, but it's impossible to know the cybercriminal's intentions as this point. While potentially having your email hacked doesn't sound like that big of a threat, there are multiple ways in which this information could be used for harm.

The most notable risk is that the login information may be used to access other accounts; many people use the same username and password for their emails accounts as other ones, such as for online banking. So, there is far more value in this large collection than just the asking price of $1. To protect yourself, security experts advise you change your password immediately.