October 2018

TechTidbit.com

brought to you by Tech Experts

# October Is National Cybersecurity Awareness Month

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

Online security is something that should get everyone's attention. Threats exist all around us: ransomware, viruses, spyware, social engineering attacks and more. There's so much you need to know to keep your personal and business information safe.

But where do you start?

As trusted cybersecurity professionals, we want to help you get educated and stay informed.

That's why during National Cybersecurity Awareness Month our goal is to give you all the information you need to stay secure.

How can we help? We'll be sharing valuable and timely information on cybersecurity in blogs, in our newsletter, and on all of your favorite social media sites.

## What should you do?

You can also give us a call for personalized solutions by subscribing to our exclusive mailing list.

Being cybersecurity aware means that you understand what the threats are and take precautions to prevent them. Here are some important reminders:

- Never give out your password. Don't share it over the phone either. You never know who's listening.
- Don't click on links that are sent to you via unsolicited emails or from someone you don't know.
- Use complex passwords that are difficult to guess and use different ones for different programs and computer devices.
- Don't reveal your personal, business or financial information in emails.
- Don't respond to email solicitations.
- Keep software, browsers and operating systems up to date, so they stay free of vulnerabilities.
- Encrypt your files to ensure unauthorized people can't access them.
- Be careful when using public Wi-Fi networks – don't conduct sensitive activities like banking or shopping with credit cards on public Wi-Fi.
- Remember your physical surroundings and don't leave your computer devices unattended in public or easy-to-access areas.
- Only use websites that begin with "https://" when visiting online shopping, banking or other sites where you will be entering your private information.
- Keep your online presence private. Don't publish your email address online in social network sites.

## What to do if you become a victim of cybercrime?

First, document everything related to the breach. Save copies of emails, screen shots of websites, and take pictures with your phone if it will help document the situation.

Report it to the appropriate people in your organization, including your network administrator or IT service company.

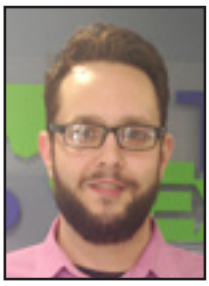
If you think your financial account was compromised, contact your financial institution immediately - you may want to close your account and open a new one.

Watch for any unauthorized charges in your bank or credit card accounts for several months after a suspected breach.

Threats exist all around us: ransomware, viruses, spyware, social engineering attacks and more. There's so much you need to know to keep your personal and business information safe.

# Browser Battle: Why Chrome Continues To Take Over

*"Google also made sure that the mobile integration for Chrome is second to none. Just make sure you are signed in on your computer and your phone to keep all of your bookmarks and browsing synced."*



***Jason Cooley is Support Services Manager at Tech Experts.***

Every day I see different browsers on different computers. There's Chrome, Internet Explorer, Firefox, Vivaldi, Opera, and Apple's Safari browser. Some people like to stick with what they know, and they use Internet Explorer or even Microsoft Edge on Windows 10.

There are those people that really love Mozilla's Firefox browser and are loyal and comfortable using that. Apple users tend to stick with Safari, like how Windows users use Internet Explorer and Edge, because it's the default they've used for years.

I made the switch to Google Chrome for good about 5 or 6 years ago, and I continue to use it as my browser of choice.

There are preference issues and everyone likes what they like, but there is definitely more to why I use Google Chrome over the other browsers. There are even reasons why I think you should probably use Chrome too.

Let's start by acknowledging that there are certain websites that only have full functionality in a certain browser and that's OK. Maybe you need to use Internet Explorer for something. Use what you need to for certain tasks. When you have a choice, use Chrome.

Chrome is celebrating its 10th birthday with a nice updated look, but that's just the surface. It continues to add features that not only improve your user experience, but also help make things a little more secure.

Chrome now will auto-generate and suggest strong passwords for new accounts created, keeping them unique and therefore significantly more secure.


Google also made sure that the mobile integration for Chrome is second to none. Just make sure you are signed in on your computer and your phone to keep all of your bookmarks and browsing synced.

While a browser like Firefox may meet some of the standards set by Google, there are areas other browsers just can't stack up.

Mozilla has updated and launched a new and improved mobile app. It is now faster than it was ever before. Want to sync your data between your phone and computer browser with Mozilla? Sure, just create a completely separate account, link them, and hope for the best. Mozilla's ability to share bookmarks is fair, but it can't keep the settings streamlined.

These are the areas that Google Chrome excels in, making your browsing experience seamless.

The password manager will also make using your account on multiple devices much easier, as you can use the manager to store passwords and use them on any device you are signed in to.

If you own an Android phone or use the Google Play store but don't use Chrome, you are missing out on great app integration.

Another reason Chrome pulls ahead in the battle is because of its amazing app library and easy integration and updates. Other browsers can't begin to offer the things that Google does.

If you need more reason, consider that most of the major browsers use Google's safe browsing programming to detect potentially dangerous sites.

Consider that these companies are using someone else's programming to keep you safe… and that programming is from the clear leader in the browser battle: Google Chrome.

# Replace Your PC Every 4 To 5 Years To Save Thousands Of Dollars

*Chris Myers is a field service technician at Tech Experts.*

When it comes to replacing computers, many consumers and businesses wait as long as possible before committing to an upgrade. However, those businesses would actually be better off in almost every way if they replaced their computers as part of a standard process based on the hardware age.

There are many drawbacks to using an old computer that aren't immediately visible. All of these result in costs to the business, whether it is due to lost employee productivity, downtime, or lost data on failed drives.

If any of the above issues are visible to a client, they can also cause loss of business purely on the perception of inadequacy or unreliability.

A major difference overall is the gradually decreasing performance that every computer suffers from as time goes on. This is due to the actual mechanical parts wearing down as well as bloat from applications and files.

Additionally, with each new software update, there is more and more of a chance of business software no longer running on older hardware or operating systems.

Computers have many moving parts that have different expected lifetimes. Past four years, it is likely that different hardware components will start failing one by one every four or five months.

Each of these failures will result in a service call to diagnose the problem and replace the part, while the employee is not working.

Hard drive failures are almost always unrecoverable. If that employee does not have a backup in place, there is little anyone can do to restore the lost data.

However, if the upgrade is done while the PC is still functional, absolutely everything can be copied over to the new computer.

This includes files, but also things that aren't usually backed up, such as applications and user specific settings in their commonly used programs.

On a four-year cycle, each new computer will be at least one major operating system version apart.

Operating systems such as Windows 7 and Windows 10 are the framework of the computer and are therefore much harder to change on a computer already in use.

The service charge and software errors for such an installation would be as much or more than buying a new hardware component.

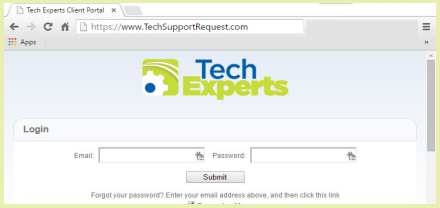
Each new operating system also contains hundreds, if not thousands, of patches to fix security vulnerabilities.

With each passing day, an old computer becomes more and more vulnerable as new holes are found in its programming. Many 5+ year-old operating systems no longer meet the requirements for mandates such as HIPAA.

The price of a new mid-range computer is usually the same as one or two of those service calls. And a new computer would avoid all of the other costs discussed above, usually resulting in savings more than double the price of the new PC.

Enacting a company-wide policy to replace PCs by hardware age also eliminates a great deal of hassle for users, clients, and your IT department.

*"There are many drawbacks to using an old computer that aren't immediately visible. All of these result in costs to the business, whether it is due to lost employee productivity, downtime, or lost data on failed drives."*




**Create new service requests, check ticket status, and review invoices in our client portal:**

**http://TechSupportRequest.com**

**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**



# Is Your Smart TV Spying On You? (Hint: It Is.)

*Frank Deluca is a field service technician at Tech Experts.*

There's a good chance your smart TV is spying on you. Smart TVs often analyze the videos you're watching and report back, whether you're watching live TV, streaming videos on a service like Netflix, or playing local video files. Worse yet, this can be a security problem.

Smart TVs not only usually have bad interfaces, but they spy on what you're watching even when you aren't using their "smarts."

Modern smart TVs often have "features" that inspect what you're watching and report it back to some company's servers.

This data can be sold to marketers or it could be tied to you somehow to create a better ad-targeting profile.

In reality, you are not getting anything out of this as the TV manufacturer just makes some more money on the side by collecting and selling this data.

Smart TVs also have questionable security protections.

For instance, Vizio TVs were discovered to be transmitting tracking data without any encryption, so other people could possibly snoop on the snoopers. They also connect to a server without checking if it's a legitimate server, so a man-in-the-middle attack could send commands back to the TV.

Vizio says it has fixed this problem and TVs will automatically update to a new firmware.

But are those smart TVs even checking to ensure they're downloading legitimate firmware files with correct digital signatures?

Based on TV manufacturers' cavalier attitude towards security in general, I wouldn't bet on it.

To make matters worse, many smart TVs have built-in cameras and microphones. If the security is so shoddy in general, it would theoretically be possible for an attacker to spy on you through your TV.

What can you do to stop your TV from spying on you?

Just don't connect your smart TV to your home network and you'll be protected from whatever built-in analysis features it has and any security vulnerabilities that could be exploited.

If the TV is not connected to the Internet, then it cannot transmit data out.

If you have connected it to the network, go into your smart TV's settings and disconnect it from the Wi-Fi. Don't connect it to the network with an Ethernet cable either.

If you've already connected to the Wi-Fi network, try to get your smart TV to forget the password. If you can't, you may need to reset it to its factory default settings. When you set it up again, don't give it the Wi-Fi password.

This will also prevent your smart TV from embedding extra advertisements into other things you watch — yes, some Samsung smart TVs actually do that!

The best, most secure way to get "smart features" on your TV is by plugging in a streaming box like an Apple TV, Roku, Chromecast, Fire TV, video game console, or one of the many other devices that works better and should be more secure than your smart TV. In which case, that box can be connected to the Internet.

This is part of a larger problem with the "Internet of Things" that society is beginning to grapple with, which envisions modern appliances like your toaster, blender, microware, and fridge becoming "smart" and connecting to the network.

Most devices' manufacturers don't seem capable of (or are apathetic toward) creating software and continually updating it so it remains secure.

Smart appliances are great, but the reality of spying and security holes will be a serious problem.