October 2020

TechTidbit.com

brought to you by Tech Experts

Could One Well-intended Click Take Down Your Business... From The Inside?

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

Not many owners and managers realize this… but the biggest data security risk to your business is actually your team.

We're not talking malicious damage. But rather, them being caught out by cyber criminals.

It only takes one click on one bad website, and your business can be compromised. It really can be that simple.

Hackers target staff to try to install malware on your devices. Then they can try to extort money, corrupt files, or steal your sensitive business data.

In some cases, this can cause such extreme damage to your business that it makes genuine recovery very hard. Trust us when we say you want to avoid it at all costs.

Fortunately, there are a few things you can do to help protect your business from this kind of attack. And you're probably already doing some of them.

For example, installing antivirus software across your network, and making sure it's always 100% up-to-date.

And of course keeping a daily, verified backup of all data.

However, there's one protective tool that many businesses miss. And it could reduce your risk of cyber-attack by up to 72%.

What is it?

Cyber security training for all your people – from CEO to administrator.

Don't dismiss such a simple thing. It's one of the most powerful preventive tools at your disposal.

With cyber criminals changing the game so frequently, you'd be forgiven for quickly falling behind on the latest scams to watch out for.

Regular training can arm you and your people with the tools you need to recognize a scam email or a fake website. And keep your business more protected from attack.

We have access to the very latest training. It's our job to keep on top of everything related to cyber security, and we want to help keep your business safe.

Can we review your cyber security situation and suggest a training plan for you?

Before we carry out the review, we'll need to have a quick video call (no more than 15 minutes) to discuss your current security, your business, and to answer any questions you may have.

There's no obligation to go ahead with the training after our chat, and certainly no obligation to buy anything. Ever.

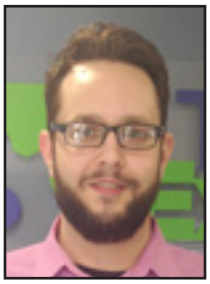
We simply want to show local businesses like yours how they can keep themselves better protected from cyber-attacks and data breaches.

Visit www.MyTechExperts.com/cybertraining to book your video call. You can also give us a call at (734) 457-5000.

Regular training can arm you and your people with the tools you need to recognize a scam email or a fake website. And keep your business more protected from attack.

Zoom In: A Look At The Increase Of Virtual Meetings

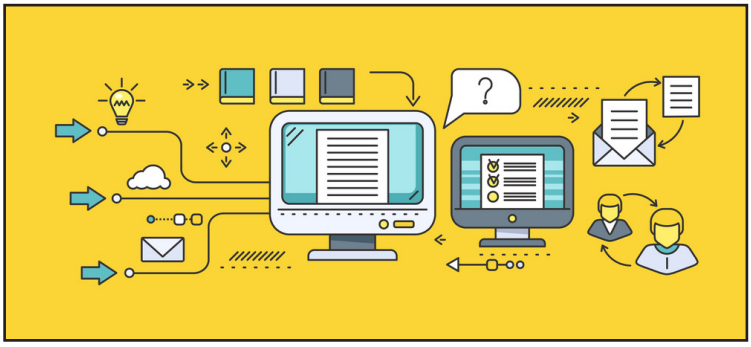
"In December 2019, Zoom reported 10 million daily meetings taking place. Fast forward to March 2020, and Zoom hosted 200 million daily meeting. By the end of April 2020, Zoom reached 300 million daily meetings."



Jason Cooley is Support Services Manager at Tech Experts.

Quarantine as a whole was (and still is) a strange thing to see happen in the United States. With state-by-state protocols varying and dates in which states began to open back up done on a per-state basis, months were lost.

Schools shut down and businesses closed, some permanently. The businesses deemed "essential" stayed open with new restrictions in place.



Travel was restricted domestically and halted internationally. Anyone that could work remotely was reassigned to work from home.

With travel bans and remote work orders in place, Zoom saw huge increases in usage.

Zoom is meeting software, allowing users to do video or audio conferences as a group. There is a very good free tier for users to join unlimited calls, to host calls with up to 100 participants for up to 40 minutes, and unlimited one-to-one calls.

Among other similar solutions, Zoom has seen skyrocketing numbers since the pandemic started.

In December 2019, Zoom reported 10 million daily meetings taking place. Fast forward to March 2020, and Zoom hosted 200 million daily meeting. By the end of April 2020, Zoom reached 300 million daily meetings.

Zoom users vary from friends chatting, students collaborating, businesses meeting, conferences, and even the British members of Parliament.

Video conferencing has been used to keep gatherings to a minimum, teach students, conduct business meetings, and more.

While there may be a time that the number of video conferences may drop down, I believe the way we do business and operate as people has changed in some ways that will continue the prevalence of video conferencing.

Many schools across the US closed early late last year due to the pandemic. In Michigan, students in K-12 have a few different options when it comes to how they proceed with their learning now. Students can work remote or virtually.

Remote learning has two options itself, in-person learning with remote or just remote. The in-person learning involves a limited school day and less days in attendance per week. Or a class will be entirely remote.

Virtual school will remain that way all year. This is an existing system in place, and students will remain home doing virtual learning even when restrictions ease. Students may have already been using this system prior to the pandemic.

In both cases, students are typically using Google Classroom and Zoom. Remote learning with Zoom sees students join a conference with an instructor. They may have a lecture or another type of lesson that is done over the video conferencing. Virtual school's lectures can vary based on the program itself.

When restrictions are lifted in Michigan for schools, those who are doing remote learning with attendance will attend school on a more regular schedule, but will still see some use of Zoom as a way to reduce traffic and students in different classrooms. Those doing just remote learning will stay home after restrictions are lifted and continue to attend video conferences as classes.

There have been many changes this year, and some are for the better. There will probably be a decrease in travel, even as bans are lifted. Some things that had previously been done in-person will now be done through video conferencing. Students will continue to be able to attend school from home. Work-from-home positions may offered by more companies.

Things will continue to return to how they were before the pandemic, but video conferences will continue to thrive.

It's Time To Move On From Internet Explorer

Mark Funchion is a network technician at Tech Experts.

For those of us who have been online a long time, we remember the original browser war: Internet Explorer vs Netscape Navigator. In recent years, Internet Explorer has fallen off in security and usefulness. Meanwhile, Chrome, Firefox, and Edge (specifically Chromium-based Edge) have increased in usage and also do a much better job of updating frequently to mitigate security issues.

In 2019, Chris Jackson – who is a Principal Program Manager in the Experiences and Devices Group of Microsoft – wrote https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-perils-of-using-internet-explorer-as-your-default-browser.

In the blog post, he writes that Internet Explorer is a compatibility solution. This means that IE exists now just in case it is needed, such as for a banking site that has not been updated to support modern browsers and does not function otherwise.

To further demonstrate that Microsoft does not want you to use IE, they are ending Internet Explorer's support for MS Teams on November 30th 2020. Next year on August 17th 2021, MS will end IE support for Office 365, Outlook, and OneDrive, among other services.

In this time of remote working, ending support for their own remote collaboration software is a big deal, and to follow that up the following year with products so widely used like Office and Outlook shows that the end of IE is finally upon us.

There are a few challenges as some software (especially financial and medical fields) has been slow to change and still only work with Internet Explorer. Another issue is users who have been using a computer for a long time have grown accustomed to using Internet Explorer and do not want to change what they know.

Also, many users have accumulated a lot of favorites and passwords in Internet Explorer and do not want to give those up.

Many people with saved passwords may not know what some of their logins are because they have had their credentials saved for so long.

Fortunately, these issues can be handled by importing your information into another browser. To handle it manually would be a pain, but your information from Internet Explorer can all be easily transferred into the main modern browsers (Chrome, Firefox, and Edge). Aside from a few clicks from you confirming what you want transferred, it's nearly automatic.

That aside, many browsers follow the same general design, making it easy to recognize icons and fields like your address bar or home page button. They are also customizable, much like adding toolbars on IE, so you can adjust a new one to your liking to match your old familiar layout.

What about those legacy web pages? All three modern browsers also have the ability to use a plugin to emulate Internet Explorer on specific pages. Or, if absolutely necessary, you can keep and use IE only as needed.

Another benefit to the three modern browsers is update frequency. Chrome will update within days, if not hours, of an issue being discovered. Firefox is also on a similar schedule.

Edge had three security updates in August of 2020, so it also updates more frequently than Internet Explorer ever did.

Change is hard, especially for some people when it comes to their computers and software. There was outrage when Microsoft Office introduced the ribbon bar and when Windows updated the start menu.

For some, the change was seamless; for others, it took some time. Either way, these have become the norm and most people are now comfortable with them.

The same is true of browsers. They are all used in generally the same way, and while using Chrome may be a little different in the long run, you are safer and your experience is more secure.

If the company who develops a product feels it is not useful for everyday use, it's time to move on.

"There are a few challenges as some software (especially financial and medical fields) has been slow to change and still only work with Internet Explorer. Another issue is users who have been using a computer for a long time have grown accustomed to using Internet Explorer and do not want to change what they know."

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

Why IT Professional Are Terrified Of Ransomware

If you want to scare someone who works in IT, start talking to them about ransomware.

There are few things as scary for IT professionals as the prospect of their systems locking up with hackers demanding money to return things back to normal.

When discussing it, you may notice them breaking into a sweat and starting fidgeting as they contemplate one of the most terrifying cybersecurity threats computers face.

How does ransomware spread?

There are several ways that ransomware can get into computers.

Email is one of the most common ways in. Hackers will send bad files that can trigger a ransomware infection when opened and quickly spread across your network.

Another favorite way to spread ransomware is to send bad URL links that download ransomware when they're clicked. This 'drive-by downloading' can happen without anybody noticing that anything has happened until it's too late.

These bad files and links are not always easy to spot. Cybercriminals are getting increasingly sophisticated in the ways they try to persuade people to do what they want them to do.

A growing trend is for cybercriminals to pose as trusted people, like a client, a colleague, or a friend. And ask you to do something urgently before you have the time to think things through.

This isn't a modern crime. Ransomware's been around for years

Ransomware dates to the late 1980s when payment was often sent by check through the mail!

Now, modern hackers normally demand payment in cryptocurrencies that make them much more difficult to track.

Here is some information on two of the more infamous ransomware attacks.

WannaCry

The WannaCry ransomware attack took over the news when it spread widely in 2017.

More than 200,000 computers in over 100 countries were left useless. The ransomware exposed weaknesses in critical IT systems, like those in hospitals and factories.

One of the worst-hit victims was the National Health Service (NHS) in the UK. Operating theatre equipment, MRI scanners, and other computers essential for hospitals were left useless and patients suffered.

NotPetya

NotPetya is less well-known than WannaCry but the financial costs are estimated to have been far higher.

Mainly spread among businesses due to the early infection of a major financial software vendor, the cost of this ransomware to small businesses and governments is estimated to have been around $10 billion.

This attack impacted computers around the world. But around 80% of the cases are estimated to have been in Ukraine.

Create new service requests, check ticket status, and review invoices in our client portal: http://www.TechSupportRequest.com