December 2020

TechTidbit.com

brought to you by Tech Experts

Three Big Ways To Improve Your IT Next Year

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

As we head into 2021, are your IT system due for an upgrade?

Here are three key things you can do to improve your IT and keep your business running smoothly into the years ahead.

Move applications to the cloud

The benefits of moving your business to the cloud are clear.

It will reduce your IT costs, improve the level of security, and give you the ability to quickly scale up your IT resources as needed.

You may currently work with a hybrid setup with bits and pieces of your IT in the cloud and other parts of your business still running locally.

With the right IT support team helping you, moving fully to the cloud is smooth and effective.

Take security seriously

It's hard to read any technology news without reading about the damage cybercrime can do.

Cybersecurity issues can impact all devices connected to the Internet, and businesses are prime targets for hackers looking for an easy payday.

Fall victim and your business could grind to a halt. And your reputation can take a real battering.

Investing in help from a proactive IT support partner who knows what they're doing is key to keeping your business safe.

Treat your team to new computers

Upgrading your computers is an investment worth making.

You'll get a happier and more productive team for sure.

New computers will also reduce the amount of time your staff spend fighting with technology that's slowing them down. The mental boost this can provide is huge, as are the productivity gains your company will see.

You may currently work with a hybrid setup with bits and pieces of your IT in the cloud and other parts of your business still running locally. With the right IT support team helping you, moving fully to the cloud is smooth and effective.

Would Your Business Survive The 4 Beer Test This Christmas?

So, it's unlikely you'll be having a traditional office Christmas party this year. Thank COVID, you party-pooper.

But I'm sure at least some of your team will find a way to celebrate together over a few beers after work one day.

And that's why it's worth asking if your business can pass **the four beer test.**

What's that? Four beers is about the stage where people start to "relax" so much, they start to forget the important stuff.

Like picking up their laptop bag when they leave the bar or restaurant.

Laptops and mobile devices get left in bars and restuarants all the time, especially on dark winter nights like these.

Thing is – depending on your IT setup, a lost laptop can either be a minor inconvenience. Or a complete disaster.

How can you tell which? By asking these 3 questions:

• Is it encrypted?

• Is it password protected?

• Can the data be wiped remotely?

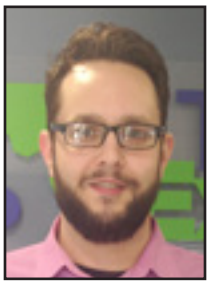
If it's a "yes" to all three, you can relax. It's annoying you've lost your device… but your business's data is safe. No one can access it.

And if you can't positively answer all three, there's a problem. These days, the loss of data is a much bigger deal than the loss of a device.

If you're not 100% sure you can answer all 3 questions with a big fat YES… then give us a call. We can check for you.

Pandemic Continues To Affect Business Models (Even Microsoft's)

"If a giant like Microsoft is adjusting their business models and plans, the impact is sure to reach the little guys. Although a majority of businesses rely on technology and computers in some capacity, not everyone has the capability or the support needed to move to a completely remote business model, even temporarily."



Jason Cooley is Support Services Manager at Tech Experts.

The global pandemic continues on, and here in the United States, we are once again seeing numbers surge after a few months on the decline.

With the holiday season approaching, many are changing and cancelling their usual plans. Many employees are still working from home when possible. Everyone – from tech giants to a small mom-and-pop business on the corner – have been affected in some way.

So, with a reduced workforce, what does that mean for a company like Microsoft? For starters, they are pushing back end-of-support dates. One of which is Windows 10 1803, which had its support extended by six months.

This is partly due to the impact the pandemic has had on Microsoft, but beyond that, it is because many businesses cannot operate normally right now. This is obviously problematic on many levels. The last thing a business owner or company needs is to push out updates without the proper support in place.

Productivity may be down in some cases as people adjust to workflow changes and remote working, but many have become more comfortable with their new normal. They have hit their stride, if they missed a step at all, and Microsoft has opted not to disrupt that.

If a giant like Microsoft is adjusting their business models and plans, the impact is sure to reach the little guys. Although a majority of businesses rely on technology and computers in some capacity, not everyone has the capability or the support needed to move to a completely remote business model, even temporarily.

For a managed service provider like Tech Experts, managing clients remotely has been our primary focus for years. There will always be times that even we need to physically be somewhere to perform certain tasks, but in a pandemic, even for us, that number has decreased.

Some industries are more reliant on physical presence to be effective, which completely shakes up their operations.

In Monroe, schools have now switched to all online classes. Most students were already primarily remote, and due to surging cases, they have now switch to online.

I sat in on parent teacher conferences last week. During the conferences, I spoke to different teachers, and I gained some perspective on how the pandemic has affected their classes and their interactions with students.

More than one teacher specifically mentioned how, even on Zoom, it feels like they are teaching to an empty room or a black screen. Participation is down, but usually, school work comes in without issue.

Remote capabilities are in place, but it's a very different experience than sitting in classrooms with peers.

Whether you're an IT pro, doctor, lawyer, insurance agent, teacher, or student, your days this year surely look a lot different than they have in the past. We're getting by as well as we can under the circumstances, trying to make things work with what we have.

Even with a vaccine on the way, things may never be exactly the same again. Work-from-home positions may become more popular or widely offered. Traveling for meetings will be less likely as many companies have gotten used to teleconferencing. Some students may flourish in online school and cause the industry to expand.

Changes aren't always easy, but hopefully, the things that can be improved will be. No matter how it has affected you, the pandemic will not be missed.

Happy Holidays: The Season Of Cyberattacks

Mark Funchion is a network technician at Tech Experts.

The year 2020 has, in many ways, been the year of COVID. Whether or not you have had COVID-19, it is a safe bet that your life has in some way been impacted by the pandemic.

As is usually the case, cybercriminals are at the forefront of exploiting every opportunity they can.

A look at Google trends for coronavirus (https://trends.google.com/trends/story/US_cu_4Rjdh3ABAABMHM_en) shows how prevalent the topic is and continues to be.

This desire for information has led to a third of the cyberattacks in the United States (and a quarter of the attacks in the UK) being coronavirus-related. Like most cybersecurity attacks, these are often of the ransomware variety.

These attacks are increasingly targeting heath care facilities, but anyone can be a target. Since these medical facilities are overwhelmed and COVID leads most of the news today, people are on data overload while trying to manage their immediate concerns – and can become complacent when dealing with potential threats.

As we must remain vigilant in keeping ourselves medically safe, we must do the same to keep ourselves technologically safe. A few best practices are:

• Don't open an attachment unless you know who it is from and you are expecting it.

• Use the same level of caution with email messages that instruct you to enable macros before downloading Word or Excel attachments as you would with a live cobra. Don't touch it!

• Use anti-virus software on your machine, and make sure it's kept up-to-date with the latest virus definitions.

• If you receive an attachment from someone you don't know, don't open it. Delete it immediately.

• Learn how to recognize phishing:

- Messages that contain threats to shut your account down

- Requests for personal information such as passwords or Social Security numbers

- Words like "Urgent" – a false sense of urgency will encourage you to act

- Forged email addresses

- Poor writing or bad grammar

• Hover your mouse over links before you click on them to see if the URL looks legitimate.

• Instead of clicking on links, open a new browser session and manually type in the address.

• Don't click the "Unsubscribe" link in a spam email. It would only let the spammer know your address is legitimate, which could lead to you receiving more spam.

• Understand that reputable businesses will never ask for personal information via email.

• Don't send personal information in an email message.

Tech Experts can assist with keeping you safe by providing support, running backups, and ensuring that your devices and software are up-to-date.

However, even with these safeguards in place, it is important that you do your part and do your best to act responsibly and thoughtfully when dealing with technology.

Messages that ask you to click for COVID news, updates, cures, etc. that you are not expecting should be treated as a potential threat. Obtain news from trusted sites.

While our interest in COVID is high, that is what makes it such an effective method of lowering people's guards. Relatedly, as we head into the holiday season, watch out for "There is a problem with your delivery – click here" emails and other similar traps.

If cybercriminals, hackers, and spammers can find an opportunity, they'll take advantage of it regardless of a global pandemic or the holidays. You've got enough on your plate; staying vigilant will go a long way in preventing the headaches of cyberattacks or identity theft.

"These attacks are increasingly targeting heath care facilities, but anyone can be a target. Since these medical facilities are overwhelmed and COVID leads most of the news today, people are on data overload while trying to manage their immediate concerns – and can become complacent when dealing with potential threats."

Four Signs You're Under Attack From Ransomware

You've probably heard a lot about ransomware recently. This is the computer attack where a hacker locks you out of your systems and data. And you must pay a ransom, typically in Bitcoin, to get access again.

While it's not a new crime, it's one of the fastest growing crimes online because it's so lucrative to criminals. Thanks to COVID and work-from-home, more and more businesses are unintentionally opening themselves up to the threat.

In fact, it's estimated there are more than a hundred calls to insurers every day relating to problems caused by ransomware. Unless you take necessary precautions, your business could fall victim.

But how do you know you're not already under attack? Because here's something most people don't realize about ransomware. If a hacker gets access to your systems today, they won't launch the attack right away. It can take around 60 to 100 days - if not longer - from the time you're breached, to the delivery of ransomware.

You might be wondering why these cybercriminals spend such a long time launching their attack. They spend weeks or more just skulking around, investigating your network for weaknesses, and waiting for just the right time to maximise their profit.

So how do you know if you're under attack? And what do you do if you are? Here are four of the best ways for you to check that your network is safe and secure.

Check for open RDP links

What's an RDP link and how do you open or close it? We don't want to get too techy here, so put simply, an RDP (or Remote Desktop Protocol) is Microsoft technology that allows a local computer to connect to and control a remote PC over a network or the Internet.

You're probably utilizing this kind of thing if you've had any of your people working from home this year, as it makes remote access a lot easier. But RDP links left open to the Internet are a very common route for cybercriminals to enter your network.

Look for unexpected software

One of the methods ransomware gangs use to take control of your system is certain software tools. It's important that you use a network scanner to check exactly what's running and who's running it.

Often, cybercriminals will take control of just one PC first, perhaps using a phishing email to persuade someone to click on a bad link without realizing it. Once they have control of one PC, they can then target the entire network.

Criminals also utilize tools to steal your passwords and log-in credentials. If you spot anything unfamiliar anywhere in your system, contact your IT support partner, who can investigate further.

Monitor your administrators

Your network administrators typically have the authority over which applications are downloaded to your network. So what's the best way for hackers to download the applications they need? They create a new administrator account for themselves.

Then they can download whichever tools they need to compromise your network.

Check for disabled tools and software

Once the cybercriminals have administrator rights, they can locate and disable your security software. You can tell that an attack is close to being launched if something called Active Directory and your domain controllers are disabled.

Next, any backup data the criminals have found will be corrupted. And any systems that automatically deploy software will also be disabled to stop your attempts to update your computers after an attack.

It's worth remembering that this will all be done slowly. Your hackers will take their time because that makes it much harder to detect them.

Once an attack has been launched and your data held to ransom, most of the time there's little you can do other than attempt to restore backups. Or pay the ransom.

The hackers have normally been so thorough with their preparation that even the best IT security specialists have few options open to them.

So, once you've detected that something might be wrong, what can you do to stop an attack from being launched?

You can force a password change across your core systems, which many times will also throw your attackers out.

Monitor your administrator accounts. This may sound like a simple step, but you'd be surprised at how often it's neglected.

Keep all of your software and security patched and updated. It's very tempting to click 'later' on updates. But saving a little time now is not worth the huge amount of time and money that you'll lose should you become the victim of a ransomware attack.

Implement multi-factor authentication across all of your applications, if you haven't already. This adds another level of security for your network and helps to prevent unauthorized access.

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