July 2021

TechTidbit.com

brought to you by Tech Experts

Your Business Is Already Under Attack

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

Ransomware is big business. It's one of the fastest growing online crimes. Cyber criminals are targeting small and medium sized companies as well as non-profits and government agencies.

It's the computer crime where your data is encrypted so you can't access it unless you pay the ransom fee.

The really scary part is that it's unlikely you'd realize you were under attack from ransomware until it was too late.

Cyber criminals hide in your network for between 60 to 100 days before they strike. During that time they're checking out your network, identifying vulnerabilities, and preparing what they need to hit you with the attack.

And they do all of this without leaving much of a footprint for you to discover.

Fortunately, there are a number of signs you can be on the lookout for to identify an attack and stop it in its tracks. This is the most technical thing you will ever read from us, but it's important you know what to look out for.

Open RDP links

What's an RDP link? How do you open or close one?

RDP - or Remote Desk Protocol - is Microsoft tech that allows a local PC to connect to a remote device. You'd use it if you've worked from home.

And many people neglect to close their open RDP links when they've finished with the connection, allowing cyber criminals easy access.

Scan for open ports regularly and start using multi-factor authentication (where you generate a login code on another device) if you don't already.

Unfamiliar software

Noticed new software on your device lately? It's probably not an update.

Hackers typically gain access to one device, and then use particular software tools to access the entire network. Look out for anything you haven't noticed before, but particularly apps called Angry IP, Advanced Port Scanner, and Microsoft Process Explorer.

New administrators

Noticed a new admin on your system? It's worth double checking that your IT team hasn't added the new person.

Cyber criminals will set themselves up as administrators so that they can download the tools they need to carry out their attack of your network. And to do this, as well as the software mentioned above, they may also use other software called Process Hacker, IOBitUninstaller, or PCHunter.

These are all pieces of software that your business may legitimately use, but they can be used to uninstall security software and your anti-virus application.

Disabled software

Of course, to carry out the perfect attack, your security software needs to be disabled. Some things called Active Controller and domain controllers will be disabled when the attack is imminent, and it's likely that your back-up will be corrupted too.

Ensure that someone is regularly checking that software is active, and your backup is working as it should be.

Remember, ransomware attacks are usually slow, so these things won't all appear at once. Vigilance is key here. Keep an eye out for anything unusual, and if you do spot something, no matter how minor, report it right away. It could help stop a huge, costly attack on your business.

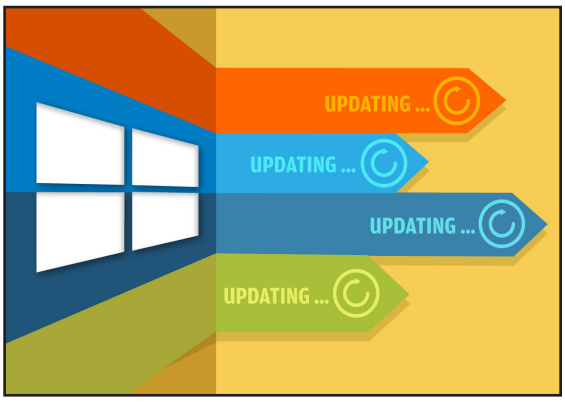
Cyber criminals hide in your network for between 60 to 100 days before they strike. During that time they're checking out your network, identifying vulnerabilities, and preparing what they need to hit you with the attack.

Windows 10: Don't Skip Your Automatic Updates

"Microsoft deploys small updates as well as large feature updates, so if you put it off for too long, you won't only be behind on updates but possibly entire versions."

Mark Funchion is a network technician at Tech Experts.

Windows Automatic Updates: a simple feature with a name that puts you at ease. Windows is the operating system installed on most of our home and business PCs, and as we often mention, malicious individuals try to make our lives miserable by attacking those systems.



Windows, by default, is set to automatically update and protect itself from new viruses and exploits, which is a great feature.

Granted, some updates may be flawed and may need to be removed, but you can prevent those updates from installing. What's more important than the errant glitch or bug is keeping your PC up-to-date.

However, how many of you have come in the morning and been greeted with a message that your update failed and changes were being undone?

Then, after a lengthy wait, your system restarts and says it will try again later. Most of us ignore that message. Sometimes, repeatedly.

Microsoft deploys small updates as well as large feature updates, so if you put it off for too long, you won't only be behind on updates but possibly entire versions. Windows 10 has had ten major updates total since 2015, and there are usually two feature updates released per year.

The four most recent versions are 1909, 2004, 20H2, and now 21H1 – and we've seen some computers get stuck as far back as Versions 1903 or 2004.

Version 1903 was released in May 2019 and Version 2004 was released in May 2020; if your updates are that far behind, that's a lot of time spent vulnerable.

That long of a timeframe means the smaller updates that often work, even when the larger versions fail, are no longer produced. Over time, we have seen systems not only stop operating completely, but left in a state unable to perform certain tasks.

One example we've encountered is a problem where users on old Windows versions are no longer able to connect to Office 365 with Outlook.

That means having to use the web-based version, which many do not prefer, or trying to fix the update installation errors.

This is where having a managed service provider such as Tech Experts can help. We follow and encounter these issues and know that simple things such as a particular audio driver or a permissions error can cause these update problems.

We manage your updates and take a proactive approach to resolving them before they impact your daily work. When an update needs some manual tweaking, we can schedule a time convenient to you to resolve these issues, often before you're even aware of them.

Our service extends beyond just these updates, but like a house, if the foundation of your PC (the operating system) is not strong, then every other part is weakened.

We also inspect the rest of your system on a regular basis to keep you protected. Tech Experts can stay on top of these things – from updates to exploits and bugs to enhanced security measures – and guide you in the right direction as a more informed user.

When Was Your Last Permissions Review?

When was the last time you reviewed who in your business has access to which documents?

Do you know who has access to your documents? Or can everyone access everything?

You may need to make some changes. You see, the more people that have access to your business documents, the less secure they are.

Let's imagine for a moment that one of your people opens a very convincing email, supposedly from a supplier.

The email contains a document to download, which they do, because it's from a supplier, right? They can trust it.

What your employee didn't notice was that the email signature was missing or that the email address wasn't the same as it usually is.

And the document they downloaded has now installed malware on their device.

They don't notice the malware because it all looked legit and nothing obvious has happened. They continue their working day unaware.

While they're working, the malware is working too, in the background. It's accessing and copying all of the data that your employee has access to.

You might get lucky and stop this malware before it enters your network and takes everything, but if your employee already has access to everything, well, it's gone. Although this isn't a malicious act on behalf of the employee, they've essentially caused a huge data breach that could kill your business.

And this scenario doesn't even need the malware to become a reality. One day, a member of your team might decide they'd like to make a little money by stealing your valuable data.

By giving everyone access to everything, you're making it too easy - and too tempting - for them.

So, if you haven't already done this, I suggest that this week you make it a priority to sit down and work out who needs access to which files and documents and restrict access to absolutely everything.

Keep your own document detailing who has access to what. And update it whenever anyone joins the business or changes roles.

This is also a great way of protecting your data when somebody leaves, because you can see exactly what you need to revoke access to.

If you already restrict access, when was the last time you reviewed it?

Are people able to access files they no longer need? And are there people who could benefit from access to more documents to complete their role?

Yes, that's a lot to think about. But once you have a detailed document to work from, regular reviews are pretty simple and definitely worth your time.

Please give us a call if you'd like to go over the shares and permissions on your network.

"Keep your own document detailing who has access to what. And update it whenever anyone joins the business or changes roles."

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

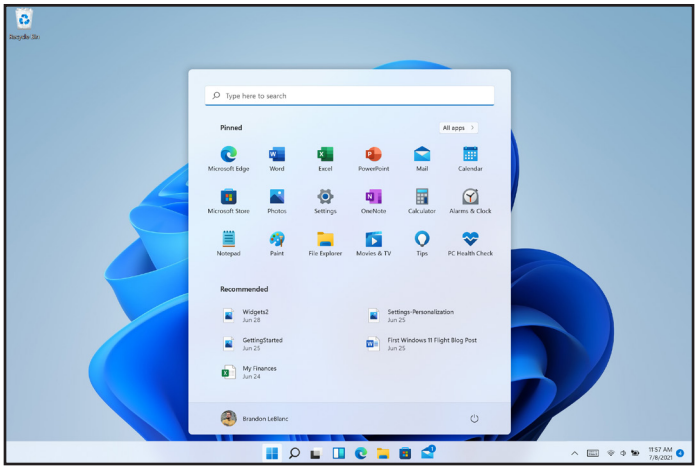
15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Microsoft Is Working On Windows 11 Update Release

Later this year, the Windows 10 era will officially come to an end with the release of Windows 11.

The latest version of the OS promises a raft of new features that will offer a "Next Gen" experience.

Here's a quick overview of what you can expect to see in Windows 11 when it is rolled out:



A totally redesigned Start Menu & taskbar

Unlike all prior versions of Windows, Windows 11 will feature a centered Start Menu and taskbar, making it aesthetically similar to ChromeOS. In addition to that, the Start Menu on the new OS won't come with the live tiles you're accustomed to. Instead, it will use static icons for all Microsoft Store apps.

If you decide you don't want your Start Menu centered, you can revert to more traditional Windows Left Aligned menu quickly and easily, and you'll also be able to choose from among three different Start Menu sizes.

Explorer improvements

Windows 11 will include the same File Explorer that you're used to, but it's getting a much needed facelift and a variety of improvements. Most of these are aesthetic in nature and designed to give File Explorer a sleeker and more modern look, with new icons and rounded corners.

Snap and widgets

Windows 11 sports four different Snap layouts, allowing you to choose between them, or switch from one to another at will. In addition to that, Microsoft is also introducing Widgets, which appears to be the successor to Window's 10's "News and Interests" feature. It utilizes your browsing history to create a custom news feed that updates constantly.

In addition to those things, you'll find virtual desktop support, HDR support for color-managed, apps, a modernized, redesigned device manager, and a whole lot more.

Although there are bound to be kinks and growing pains when Windows 11 is initially released, we're looking forward to seeing all this in action. Change is coming.

Q&A

I know I just saved a document, but I can't find where it went

This is more common than you think. You click 'save' and when you try and reopen your file, it's not in the folder you thought you'd saved it to. Don't worry, simply open up a folder, click on 'recents' and your document should be there. Look at the file information and it will show you where you've saved it.

I clicked a link in a phishing email. What do I do?

First, do not enter any data. Disconnect your device from the Internet. If you've got malware, this will stop it from spreading. Run a full malware scan. And then consult an IT expert. They'll advise how safe your backups are and whether you need to change any passwords.

My apps keep crashing, what's wrong?

In true IT support style: have you tried turning your device off and on again? If it's still happening, you can try deleting the app and reinstalling it. If the trouble is with an Office application, Windows updates can often help with the trouble.