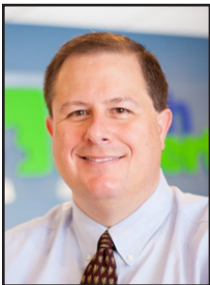# Your Remote Workers Aren't Using Computers That Look Like This, Are They?

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

When did you last check everything was OK with the devices your team uses when they work remotely?

That might sound like a strange question. But a recent survey discovered that 67% of remote workers are using faulty devices to work from home. And the reason?

They've likely damaged the device themselves and are too scared to tell you!

Laptops, keyboards, and monitors are most likely to be damaged (in that order). And it's usually because of food or drink spills… though some people blame their partners, children, and even their pets!

We've all watched in horror as a cat rubs itself against a full glass of water next to a laptop…

Using a device that doesn't work properly is a problem, of course.

First, it's going to damage your team's productivity. Tasks might take longer or be more difficult to complete. If they try to fix the problem themselves, they risk causing further damage or making the device completely unusable.

No, a fork isn't a clever way to get bits of cake out of your keyboard, and duct tape isn't the solution for a cracked or damaged laptop case.

But the other issue, of course, is that of security.

In some cases, your people will stop using their damaged company-issued device, and use a personal device instead. Which puts your data at risk.

That's because their personal devices won't have the same level of protection as your managed and monitored business devices.

It also means that if they're connecting to your network, it might not be a safe connection, potentially leaving the door open for cyber criminals, viruses, or an encrypting trojan.

And because your IT partner isn't monitoring personal devices, it's possible they won't spot an intrusion until it's too late.

Our advice? Make it a regular routine to check that everyone's happy with their devices and that there isn't any damage that needs repaired. It is also a good idea to have a policy that team members won't get in trouble for accidental damage, so long as it's reported immediately.

If you need help replacing any damaged devices, just give us a call.

Our advice? Make it a regular routine to check that everyone's happy with their devices and that there isn't any damage that needs repaired. It is also a good idea to have a policy that team members won't get in trouble for accidental damage, so long as it's reported immediately.

Top 5 Cybersecurity Mistakes That Leave Your Data At Risk

> *"Phishing also overwhelmingly uses links these days rather than file attachments to send users to malicious sites. Those links won't get caught by simple antivirus solutions."*

The global damage of cybercrime has risen to an average of $11 million USD per minute, which is a cost of $190,000 each second.

Sixty percent of small and mid-sized companies that have a data breach end up closing their doors within six months because they can't afford the costs.

The costs of falling victim to a cyberattack can include loss of business, downtime/productivity losses, reparation costs for customers that have had data stolen, and more.

Many of the most damaging breaches are due to common cybersecurity mistakes that companies and their employees make.

Here are several of the most common missteps when it comes to basic IT security best practices.

Not implementing multi-factor authentication (MFA)

Credential theft has become the top cause of data breaches around the world, according to IBM Security.

MFA reduces fraudulent sign-in attempts by a staggering 99.9%.

Ignoring the use of shadow IT

Shadow IT is the use of cloud applications by employees for business data that haven't been approved and may not even be known about by a company.

Shadow IT use leaves companies at risk for several reasons:

- Data may be used in a non-secure application
- Data isn't included in company backup strategies
- If the employee leaves, the data could be lost
- The app being used might not meet company compliance requirements

It's important to have cloud use policies in place that spell out for employees the applications that can

and cannot be used for work.

Thinking you're fine with only an antivirus

No matter how small your business is, a simple antivirus application is not enough to keep you protected. In fact, many of today's threats don't use a malicious file at all.

Phishing emails will contain commands sent to legitimate PC systems that aren't flagged as a virus or malware.

Phishing also overwhelmingly uses links these days rather than file attachments to send users to malicious sites. Those links won't get caught by simple antivirus solutions.

You need to have a multi-layered

strategy in place that includes things like:

- Next-gen anti-malware (uses AI and machine learning)
- Next-gen firewall
- Email filtering
- DNS filtering
- Automated application and cloud security policies
- Cloud access monitoring

Not having device management in place

A majority of companies around the world have had employees working remotely from home since the pandemic. However, device management for those remote employee devices as well as smartphones used for business hasn't always been put in place.

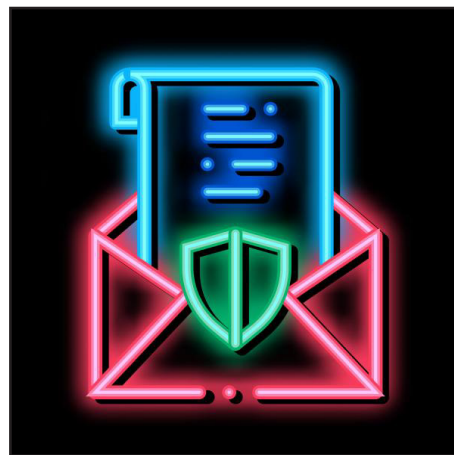A device management application in place, like Intune in Microsoft 365 can help manage this.

Not providing adequate training to employees

An astonishing 95% of cybersecurity breaches are caused by human error.

Employee IT security awareness training should be done throughout the year, not just annually or during an onboarding process.

Some ways to infuse cybersecurity training into your company culture include:

- Short training videos
- IT security posters
- Webinars
- Team training sessions
- Cybersecurity tips in company newsletters

Is Unified Communications Right For Your Business?

Unified Communications (UC) is a ready-to-use system that allows for seamless communication in numerous ways such as phone, video, screen sharing, chat and file management.

The system operates as a cloud service, making it easily accessible to all team members with access to the Internet. But why should anyone consider switching to unified communications?

There are several reasons, but this is the most crucial: Business leaders who adopt UC would be able to impact their business every day and make it seamless for employees to interact with each other.

That said, we'll list 5 of the key features of this concept to help you better understand how it can help you scale your business.

Mobility

When connected to unified communications, all employees can stay connected at all times and from all locations.

It doesn't matter whether they're working from home, vacationing on a remote island, or sitting in the office. They'll still be able to chat, receive calls, and more.

Unified messaging

This allows employees to handle different message types using a single tool. They can easily switch communication modes, depending on their needs.

Conferencing

Whenever you need conferencing tools, you'll have them in the palm of your hand.

You can allow a group of team-mates or customers from outside your organization to connect and speak via video or audio from different locations.

Fax support

Faxes received through unified communications appear as email attachments. This way, users can also receive faxes on their desktops and smartphones.

Presence

This feature lets other users know each other's status. That means you'll be able to see when someone is online (Active), busy (Do Not Disturb), or away (Out of the Office).

"There are several reasons, but this is the most crucial: Business leaders who adopt UC would be able to impact their business every day and make it seamless for employees to interact with each other."

Malware Is Becoming Harder To Spot

According to new research, four in five malware attacks delivered by encrypted connections evade detection. And since two-thirds of malware is now arriving this way, it has the potential to be a big problem for your business.

This type of threat has already hit record levels and continues to grow. So, if you don't yet have a response and recovery plan in place, now's the time to create one.

It sits alongside your cyber security software protection and regular staff training. The plan details what you do in the event of a cyber-attack.

Having the right plan in place means all your people will know how to sound the alarm if something is wrong. It ensures downtime and damage are kept to an absolute minimum.

The faster you respond to an attack, the less data you should lose, the less it should cost you to put things right, and the faster you get back to work.

Of course, you should also follow the usual security guidelines of making sure that updates and patches are installed immediately, and regularly checking your backup is working and verified.

Businesses that don't place a high importance on their own cyber security planning are the ones hit hardest by such an attack.

Can we help you create your response and recovery plan? Call us.

What Are The Best Ways To Give An Older PC New Life?

Purchasing a new computer is a big investment. Many small businesses and home PC owners end up struggling with older systems because they want to get as many years out of them as possible.

Have you found yourself banging on your keyboard in frustration? Have you tried every tip and trick you found online, only to still struggle with a slow PC?

There are some promising upgrades you can do that will cost much less than the price of a new computer, while making your PC feel like new again. Here are some of the options you can try to improve the performance of an older computer.

Upgrade to a solid state hard drive (SSD)

Prices for solid-state drives have come down quite a bit in the past few years, making them an affordable upgrade that can breathe life back into an older PC that might be slowing down.

Unlike hard disk drives (HDDs), SSDs do not have any moving parts and use a flash memory that allows for a quicker response time. You can improve your time to boot and your experience when searching files, opening applications, and other activities.

Some of the advantages of upgrading your computer's hard drive to SSD include:

- SSD read/write speeds up to 2500 MB/second compared to HDD at up to 200 MB/second
- SSD access time of 0.1ms as compared to HDD at 5.5-8.0ms
- SSDs use between 2-5 watts of energy compared to HDD at 6-15 watts

Increase the memory

One upgrade that is very low-cost and can mean a significant increase in performance is a memory upgrade. If your PC was one of the cheaper ones that only had 4GB of RAM when you bought it, you likely have trouble opening too many tabs in your browser or using any graphics-heavy program.

Upgrading your RAM, if your PC has available memory slots, to 8GB or 12GB can make it seem like you have an entirely new computer due to the big increase in speed.

Upgrade the graphics card

If you play computer games or work in any type of video, imaging, or 3D software, an outdated graphics card can ruin your experience.

Instead of replacing your entire computer, just upgrading the graphics card to a more robust model can improve your PC's performance and give you several more useful years from it.

Replace your PCs cooling system

Heat is an enemy of your computer's internal parts. If your cooling system is getting worn out and not working the way it should be, then excess heat can be building up inside your device.

When this happens things can get strange, with programs crashing or your system rebooting on its own.

If you suspect excess heat may be an issue, have your computer's fan and cooling system checked out to see if it needs replacing.

Connect an external monitor to a laptop

If you're working on a laptop and having a hard time multi-tasking due to limited screen real estate, consider getting an external monitor rather than replacing your entire PC.

Monitors are just a fraction of the cost of computers and having a screen twice the size of the one on your laptop can make all the difference in the world and improve productivity due to the additional screen space.

Replace your keyboard

Older keyboards can stick, lose keys, and have the writing rubbed off the keys, making it more difficult to tell a "prt screen" from a "delete" button. If the performance of your PC is hampered by a frustrating keyboard, an upgrade can be a very inexpensive way to improve your equipment.

Get an external hard drive

Computers can slow down and be more difficult to use when the hard drive fills up with data. Over the years, files build up, and many users never take the time to go through and delete those that are unnecessary.

Buying an external hard drive can allow you to offload files that may be slowing you down while still keeping them easily accessible.

Another benefit of an external hard drive is that it's portable and can easily be carried between home and work and used in both places.

Get a processional PC tune-up

Those free PC cleaner tools you find online aren't going to give you the type of tune-up that a professional IT provider can give.

We will go through things like the Windows Registry, duplicate system files, internal errors, and more to clean up your system and remove all the "junk" that has built up over the years.

We can also do a maintenance check for things like failing parts, and provide expert guidance on your most impactful upgrade options.

Don't struggle with an older PC! We can help you with cost-effective upgrade options that will fit your system and budget perfectly.