November 2022

TechTidbit.com

brought to you by Tech Experts

Guide For Better Endpoint Protection

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

Endpoints are the collection of computers, mobile devices, servers, and smart gadgets that make up your company's network and IT infrastructure. Each of those devices is a chance for a hacker to penetrate a company's defenses. 64% of organizations have experienced one or more compromising endpoint attacks.

The following solutions are focused on the protection of endpoint devices.

Address Password Vulnerabilities

Passwords are one of the biggest vulnerabilities when it comes to endpoints.

Poor password security and breaches make credential theft one of the biggest dangers to cybersecurity.

Address password vulnerabilities in your endpoints by:

• Training employees on proper password creation and handling
• Look for passwordless solutions, like biometrics
• Install multi-factor authentication (MFA) on all accounts

Stop Malware Infection Before OS Boot

USB drives (also known as flash drives) are a popular giveaway item at trade shows. But an innocent-looking USB can actually cause a breach.

Hackers can use them to gain access to a computer by booting from a USB device containing malicious code.

There are certain precautions you can take to prevent this from happening. One of these is ensuring you're using firmware protection that covers two areas: Trusted Platform Module (TPM) and Unified Extensible Firmware Interface (UEFI) Security.

TPM is resistant to physical tampering and tampering via malware. It looks at whether the boot process is occurring properly and also monitors for the presence of anomalous behavior.

Additionally, seek devices and security solutions that allow you to disable USB boots.

Update All Endpoint Security Solutions

You should regularly update your endpoint security solutions. It's best to automate software updates if possible so they aren't left to chance.

Firmware updates are often forgotten about. But they are just as important for ensuring your devices remain secure and protected.

Use Modern Device & User Authentication

How are you authenticating users to access your network, business apps, and data? If you are using only a username and password, then your company is at high risk of a breach.

Use two modern methods for authentication:
• Contextual authentication
• Zero Trust approach (Trust but Verify)

Apply Security Policies Throughout the Device Lifecycle

From the time a device is first purchased to the time it retires, you need to have security protocols in place.

Examples of device lifecycle security include when a device is first issued to a user. This is when you should remove unnecessary privileges.

When a device moves from one user to another, it needs to be properly cleaned of old data and reconfigured for the new user. When you retire a device, it should be properly scrubbed.

Prepare for Device Loss or Theft

Unfortunately, mobile devices and laptops get lost or stolen. When that happens, you should have a sequence of events that can take place immediately. This prevents company risk of data and exposed business accounts.

What Does 'Zero Trust' Actually Mean?

It's nothing to do with the fear that your teenage children will hold a party when you go away for the weekend.

Zero trust is actually about technology security. It's one of the most secure ways to set up your network, although it can have a very negative effect on productivity.

Most networks take a 'trust but verify' approach. They assume every device that connects is supposed to be there. Access the network once and you can go anywhere.

Imagine you're using a security pass to access a building… and once inside there are no further security checks, so you can get into every single room.

Cyber criminals love this approach, for obvious reasons.

Zero trust is the opposite approach. Every login and device is treated as a potential threat until it's authenticated, validated, and authorized.

Once in, you can't access other parts of the network without going through this process again.

Back to the building analogy – once inside the building you are surrounded by security doors and must use your security pass to get through each one. If your pass isn't valid, you're limited where you can go.

Zero trust has its uses, especially with so many people working remotely these days. But it can have a negative effect on your workflow and can slow down your team.

If you want to talk through whether it's right for your business, get in touch.

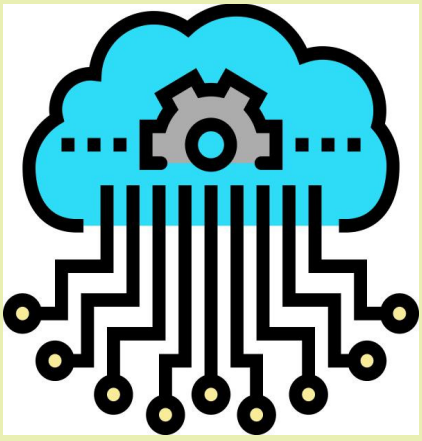
MEET MICROSOFT VIVA SALES

Data entry can be a real drag for salespeople. The time they spend on administrative tasks is time away from customer interactions. But that data is vital.

It's important to capture customer orders, quotes, needs, and more. Lead and sales reporting help sales managers know where to direct their attention.

Analytics also help drive more efficient ways of closing the deal.

Microsoft has taken up the mantle of this challenge. It is about to launch a new digital experience for sales teams. Microsoft Viva Sales is part of the "Viva" line of applications. It is a "CRM helper" application, but not designed to replace your current CRM.



Microsoft Viva Basics

- Eliminate Forms
- Powerful Data Leveraging
- AI-Driven Help
- Interconnected Interface

Tag to Capture Sales Interactions

Salespeople can use the familiar tagging function to capture data from another M365 application for a prospect or customer.

Collaborate

Viva Sales makes it easier than ever to collaborate with your team.

Call Summaries & Integrated Data

Viva Sales brings all that customer engagement data together into a single view.

This allows the salesperson to see call summaries and capture call action items.

Download & Customize

Download lead and customer lists. Customize the application per the organization's needs.

Take Advantage of Microsoft Viva Automation

Microsoft built the Viva suite of digital experience apps for productivity. These apps help employees find information faster, feel more connected, and work more productively.

The Rising Threat of BEC Attacks: Don't Let Your Business Fall Victim

Business email compromise (BEC) attacks are becoming widespread and present a significant risk to businesses of all sizes.

These attacks involve hackers posing as trusted individuals or organizations via email to request sensitive information or financial transfers.

BEC attacks often target high-level employees, such as executives or financial managers, and can be highly sophisticated.

Attackers may go to great lengths to make their emails appear authentic, including using genuine email addresses and logos. In some cases, they may even gain access to an employee's email account to send BEC emails to other employees or partners.

In BEC attacks, a common technique is the "man-in-the-middle" approach, where the attacker poses as a trusted third party, such as a supplier or vendor, and requests payment or sensitive information.

These attacks can be challenging to detect because the attacker may use genuine email addresses and logos to seem legitimate.

The attacker manipulates the victim into thinking they are communicating with a trusted party, which can lead to them divulging sensitive information or making financial transfers to the attacker.

To safeguard your business from BEC attacks, it is essential to implement strong email security measures and educate your employees on the signs of such an attack.

Two-factor authentication and monitoring for unusual activity can help protect your business.

Employees should also be aware of red flags, such as requests for sensitive information or financial transfers from unknown individuals or organizations, or requests to transfer money to unfamiliar bank accounts.

If you receive a suspicious email, do not click on any links or download any attachments.

Instead, verify the request through a separate, secure channel, such as a phone call to the sender using a number you know to be valid.

Business email compromise attacks are a rapidly growing threat to businesses of all sizes.

By taking proactive steps to secure your email communications and staying vigilant, you can help protect your business from costly and damaging BEC attacks.

What Are The Most Helpful VoIP Features For Small Businesses?

During the pandemic, VoIP and video conferencing have skyrocketed by over 210% due to the move to remote work and hybrid offices.

Sixty-seven percent of surveyed companies say switching to VoIP helps improves call handling.

The technology is much cheaper to use than a traditional landline-based system. Calling plans are also often less expensive, and a company can add new numbers for very little cost.

VoIP has several helpful features for small businesses, but what are the best features to drive efficiency, productivity, and positive caller experience?

1. Automated Attendant
2. Find Me/Follow Me
3. Hold Music
4. Voicemail Transcription to Email
5. Ring Groups
6. Call Reporting
7. Local Support

6 Things To Consider When Getting A New Computer

Have you ever bought a new computer and then had buyer's remorse a few months later? Maybe you didn't pay attention to the storage capacity and ran out of space. Or you may have glossed over memory and experienced constant freeze-ups.

An investment in a new PC isn't something you want to do lightly. Doing your research ahead of time and consulting with a trusted friend or IT shop can help. It will keep you from making major mistakes that could come back to haunt you later.

Here are several things to consider before you put down your hard-earned money on a new computer.

The Amount of Memory (RAM)

One of the big mistakes that people make when looking for a new computer is to ignore the RAM. Random access memory may be called RAM on the specification or "memory." If your system has low memory, you run into all sorts of problems.

These issues can include:
- Browser freezing up when you have too many tabs open
- Issues watching videos
- Some software not working properly
- Sluggish behavior
- Inability to open multiple applications
- Constant freezes

Memory is the "thought process" of the PC. If there isn't enough, it can't take on another task until it completes the current processing tasks. This can cause frustration and ruin your productivity.

People often go for those low-priced computer deals when looking for a new device. But these can include only 4GB of RAM. That's not a lot if you do much more than staying in a single application or just a few browser tabs.

The higher the RAM, the more responsive the system performance. So, look for PCs with at least 8GB of RAM. Or higher if you do any graphics/video or other processing-intensive activities.

User Reviews for Longevity

Buying a new computer is an investment. So, it's natural to want that investment to last as long as possible. You don't want to spend $700 on a new computer, only to begin experiencing problems when it's just two years old.

Take your time to research user reviews on the specific models you're considering. You'll begin to see patterns emerging. Steer clear of models that have consistent complaints about breakdowns sooner than expected.

You may have to pay a little more for a system that has a better track record of performance. But it will save you in the long run when you have more years of usable life before that device needs replacement.

Whether the PC is for Personal or Business Use

If you have a small business or are a freelancer, you may try to save money by buying a consumer PC. But this could end up costing you more in the long run.

Consumer PCs aren't designed for continuous "9-to-5" use. They also often lack certain types of firmware security present in business-use models. The price gap has also shortened between good consumer computers and business versions. If you're not looking at the cheap systems, you'll find that it's not that much more to get a business-grade device.

The Processor Used

It can be confusing to read through the processor specifications on a computer. How do you know if Intel Core i7 or i3 is best for your needs? What's the performance difference between AMD and Intel processors?

If you don't want to do the research yourself, you could call up your local IT shop.

We will be happy to steer you in the right direction. We'll explain in layman's terms the differences. As well as which processor makes the most sense for your intended use.

For Laptops: The Case Type

If you're looking for a laptop computer, it's important that it is durable. Laptops have some unique characteristics that differ from desktops. For example, the screen is often folded down one or more times per day. Additionally, the keyboard is part of the case and is not easily replaced by the user.

If you get a laptop with a cheap plastic case, it's bound to break during normal use. Keys could also easily pop off the keyboard, requiring a trip to a computer repair shop.

You want to consider the materials used for the case. Paying an extra $20-$30 upcharge for a better casing is definitely worth it. It can help you avoid unneeded headaches.

Storage Capacity

Storage capacity can be a pain point that you experience after the fact. If you buy a computer without paying attention to hard drive space, you could regret it. You may not be able to transfer over all your "stuff" from the old system.

But storage capacity can also be an area where you can save some money. If you store most of your files in the cloud, then you may not need a lot of hard drive space. The less space you need, the lower the price.

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