October 2026

TechTidbit.com

brought to you by Tech Experts

Why AI Training Is A Business Essential



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

There is a good chance someone in your business is already using AI.

They might be using it to draft emails, summarize notes, organize information, research ideas, or even to help with presentations and reports.

AI has arrived long before any formal plan for using it.

The conversation around workplace AI usually focuses on the technology. Which tools should we use? Which platform is best? How quickly should we adopt it?

But the more important question is simpler: Do people know how to use it properly?

Like any workplace tool, AI delivers the best results when people understand both its strengths and its limitations.

Used well, it can save time, remove repetitive admin, and help people focus on higher-value work.

Used poorly, it can create confusion, introduce errors, and increase the chances of sensitive information ending up in places it should not.

The challenge for businesses is that employees are often learning about AI from social media, online videos, articles, and conversations with colleagues rather than from their employer.

That means people inside the same business can develop different habits and expectations around the technology.

Some become confident users very quickly.

Others avoid it altogether because they worry about getting something wrong.

Good AI training helps employees understand where AI adds value, where human judgment is vital, what information should never be shared, and how to spot when an answer needs checking rather than trusting automatically.

Importantly, that training should reflect the work people do.

The way a finance team uses AI will look different from marketing, operations, customer service, or leadership teams.

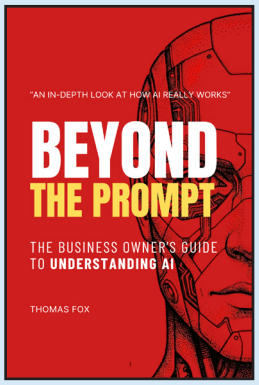
A one-size-fits-all approach probably won't cut it.

Invest in practical guidance now and you're likely to find adoption becomes more consistent, confidence grows more quickly, and security concerns become easier to manage.

Because whether you actively encourage AI use or not, the technology is already finding its way into the workplace.

Training helps make sure it arrives in a way that benefits the business as much as the people using it.

If you need help with training your team, get in touch. Give us a call at (734) 457-5000, or email us at info@mytechexperts.com.



AI Book For You

AI can save time, improve productivity, and make everyday work easier - but only if you know where the risks are. Beyond the Prompt is a practical, plain-English guide to using AI wisely in your business.

www.MyTechExperts.com/aibook

Tech Experts®
Information Technology Professionals

Empowering clients to do more with technology.
We support, manage, and optimize business IT.

Need Help? Email support@MyTechExperts.com, or call (734) 240-0200

Why Employees Shouldn't Have Administrator Access To Their PCs

"For email, web browsing, documents, meetings, and most business applications, employees should use standard accounts. Administrator access should be reserved for approved IT work."

Administrator access often starts with a reasonable request.

Someone needs to install a printer, update a program, or change a setting, so they're made an administrator on their computer. The task gets done, but the access stays.

From then on, that employee can approve software installations and make changes that normally require help from IT.

If they download a fake installer or approve a harmful program, it may be able to install system components, change security settings, or affect other information on the computer.

For email, web browsing, documents, meetings, and most business applications, employees should use standard accounts. **Administrator access should be reserved for approved IT work.**

What administrator access allows

On Windows, members of the local Administrators group have broad control over that computer.

They may be able to install software, add drivers, manage other local users, and change system settings or file permissions.

Why standard accounts are safer

Programs normally start with the permissions available to the person who launches them. If an employee can approve an administrator request on their own, harmful software may receive the same level of access.

Windows uses User Account Control to ask before many important changes. An employee using an administrator account can approve that request.

A standard user is normally asked for administrator credentials, which gives IT an opportunity to check the program and where it came from.

Standard accounts still support normal work. Employees can use email, browsers, Microsoft 365 or Google Workspace, meetings, approved software, printers, and shared files.

How to handle software installations

Employees can still get software installed without keeping administrator access. Your IT team can install it remotely, approve a request when it is needed, or deploy updates to several computers at once.

Test specialist or older software before changing permissions across the business.

If a program expects the user to be an administrator, your IT provider may be able to change its setup or find a supported alternative.

Keep a separate administrator account for approved technical work. Do not use it for email, web browsing, or everyday tasks. Protect it with multifactor authentication where the system supports it.

Check who has access now

Ask your IT provider to review the administrator accounts on every company computer, including former employees, shared logins, vendor accounts, and accounts created during the original setup.

Before removing access, confirm that IT still has a tested way to perform administrator tasks on every device.

Standard accounts let employees do their jobs without giving them or the software they run more control than normal work requires.



We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Should Your Team Use Personal Devices For Work?

Allowing employees to use personal phones or computers can be convenient. They already know the device, and they can check email or join a meeting without carrying another piece of equipment.

But the business still needs to decide what work is allowed, which applications employees may use, and what happens to company information if a device is lost or an employee leaves.

Personal devices can be suitable for limited work when they meet your security requirements. Company-owned devices are a better choice for sensitive work, administration, or jobs that require large amounts of business data to be stored on the device.

What counts as a personal device used for work?

Bring your own device, often shortened to BYOD, includes reading company email on a personal phone, opening documents in mobile apps, or using a home computer to connect to a business system. Files may remain in the Downloads folder, and accounts can stay signed in after the work is finished.

Decide what employees may do

Set the rules according to the work and the information involved. You might allow employees to read email through an approved mobile app but require a company computer for customer database exports, payroll, system administration, or access



to sensitive client records.

Staff should know which devices and applications are permitted, whether they may download files, and what they must do before selling or replacing the device.

Set minimum security requirements

A personal device should run an operating system that still receives security updates. It should have a screen lock, device encryption where available, current updates, and multifactor authentication on company accounts. A lost or stolen device must be reported quickly.

Keep business information inside approved applications or a managed work profile where possible. Device and app management tools can apply security settings and, on supported platforms, remove company data from managed apps. Tell employees what the business can see or remove before they enroll their device.

Plan for a lost device or departing employee

If a personal device is lost, IT may need to revoke active sessions, reset affected passwords, and remove company information from managed apps.

When an employee leaves, disable their account and active sessions at the agreed time. Remove company data from managed apps, check for downloaded files, and confirm that business information has been returned or deleted.

When to provide a company device

Use a company-owned device when an employee handles sensitive information, needs administrator access, stores a large amount of data locally, or requires specialist software. It is also the better choice when IT needs full control over updates, backups, applications, and security monitoring.

BYOD can work, but only when the rules are clear and the device can meet them. If your business allows personal devices, ask your IT provider to review the policy, access settings, and offboarding process before a lost phone or employee departure puts company data at risk.

"Bring your own device, often shortened to BYOD, includes reading company email on a personal phone, opening documents in mobile apps, or using a home computer to connect to a business system."

Do You Know What Software Is Installed On Your Computers?

Most businesses have a pretty good idea how many computers they own. They may even know who uses each one.

But ask what software is installed on those computers and the answer can be much less certain.

Over time, employees install PDF tools, browser extensions, meeting applications, printer utilities, and other software they need to get something done.

Some of it is useful. Some was installed for a project three years ago and hasn't been opened since. And some probably should never have been installed in the first place.

The problem isn't necessarily that employees are doing anything wrong. Most are simply trying to get their work done. But every piece of software installed on a business PC becomes something that needs to be managed.

Software adds up quickly

Think about a computer that's been in service for several years. Employees may have installed utilities. Before long, that computer can have dozens of programs beyond the applications the business actually uses.

Each one represents another potential maintenance or security issue.

Software needs updates. Older applications may stop receiving them altogether. Some programs install background services that continue running even when nobody uses the application.

A program doesn't have to be malicious to become a problem. It may simply be old, forgotten, and vulnerable.

Free software isn't always free

Employees often search online when they need to perform a task their existing software can't handle.

Need to edit a PDF? Search for a free PDF editor. Need to convert a file? Download a converter.

The employee may solve the immediate problem, but nobody has reviewed the software, its publisher, or what else was included with the installation.

This is one reason administrator access should be limited on company computers. Requiring IT approval before software is installed creates an opportunity to make sure the program is legitimate, supported, and appropriate for business use.

Don't forget the web browser

Not everything employees use appears in the Windows list of installed programs. Browser extensions have become applications of their own. Employees may add extensions for screenshots, grammar checking, productivity, document handling, or dozens of other purposes.

Depending on the permissions granted, an extension may be able to read information displayed in the browser or access information employees enter online.

Many extensions are legitimate and useful. Businesses should still know which ones are being used and remove those that aren't necessary or approved.

Remote access deserves special attention

IT providers and software vendors frequently use remote access tools for legitimate support. Employees may also install their own remote access application so they can reach a work computer from home.

The problem comes when nobody knows those programs are there.

Old remote support applications can remain installed long after a vendor relationship has ended. Your IT provider should know which remote access tools are installed, who uses them, and why they are needed.

Start with an inventory

Modern IT management tools can collect an inventory of installed applications across company computers. That information can then be reviewed for software that is outdated, unnecessary, unauthorized, or no longer supported.

Pay particular attention to remote access programs, old versions of common applications, software from unknown publishers, and applications installed by former employees.

The goal isn't to strip every computer down to the bare essentials. Employees need tools to do their jobs.

The goal is to know what's there.

Once you have an inventory, establish a simple process for approving new software and periodically reviewing what's installed.

Your computers shouldn't accumulate software forever. If nobody knows what a program does, who installed it, or whether it's still needed, that's a good reason to take a closer look.

Ask your IT provider to review the software installed across your company computers. You may be surprised by what's been quietly collecting there.

Contact Information

Tech Experts Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

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

Copyright © 2026 Tech Experts® All Rights Reserved.

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.