VOLUME 7, ISSUE 3

OCTOBER 2024

MTC TECH TALK

For Humans Not Geeks!

Your resource for the latest technology updates and opportunities for your success.

Building Trust in AI: A Guide to AI Adoption in the Workplace

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

AI is the buzzword of the decade. Everyone's talking about how it can revolutionize business, from streamlining operations to making data-driven decisions faster than ever before. And you might be thinking, "How can I get in on this?" But here's the thing: while you're pumped about the potential, your team may not share your excitement just yet.

And that's totally normal! A recent survey found a clear disconnect when it comes to AI in the workplace. Business owners like you see it as a golden opportunity. But your employees? Some of them are a little skeptical, maybe even worried about what AI means for their future.

So, what exactly is going on here? Let's break down some of the numbers:

- **62% of C-suite executives** are all-in on AI, while only **52% of employees** feel the same.
- **23% of employee**s are concerned about whether their company really has their best interests in mind when rolling out AI.
- But wait—**70% of business leaders** agree that AI should involve human oversight, meaning they don't see AI as a job-snatcher but more like an extra set of hands.

In short, leadership is excited, but employees might not be ready to throw a party for their new AI coworkers just yet. So, how do you bridge that gap? How do you get everyone on board and ensure that AI doesn't feel like a looming threat but a golden opportunity for growth?

Start with Open Conversations
It might sound simple, but one of the most effective ways to ease concerns about AI is to have an honest, open conversation. Think of it as AI 101—explain what AI really is, what it's not, and how it's going to make the company (and everyone's jobs) better.

Transparency is your secret weapon here. Encourage your team to ask questions, share their concerns, and get involved in the process. When employees understand that AI is a tool to make work more meaningful (hello, creative and strategic thinking!), they'll be more likely to see the upside.

Use this time to highlight that AI isn't about replacing people—it's about removing the boring stuff so everyone can focus on the parts of their jobs that actually matter.

AI: Your New Assistant, Not Your Replacement

Let's address the elephant in the room: AI anxiety. A lot of people hear "AI" and think "job killer." But that's not necessarily true. When implemented correctly, AI doesn't steal jobs but enhances them.

Think of AI as the ultimate assistant. It can handle repetitive, time-consuming tasks (like data entry or answering common customer questions) so your team can focus on higher-level, creative work—the kind of stuff that can't be automated.

Picture this: In marketing, AI can sift through mountains of consumer data in minutes, but it still takes a human brain to develop the next big creative campaign. In customer service, AI can answer routine inquiries, but when a complex, emotionally charged situation pops up, you'll need a human with empathy to handle that.

The message is clear: AI makes work better, not redundant. When you help your team understand this, you shift the conversation from fear to excitement.

Invest in AI Training: Growth, not a Grind

Another big reason people are wary of AI. They simply don't understand how it works—and that's understandable. If we're being honest, AI can seem like magic or worse, a black box of mystery.

Don't let your employees feel left behind. If you're introducing AI into your business, make sure to pair it with **ongoing training.** This isn't just about learning new software—it's about showing your team how to **leverage** AI to make their jobs easier and more impactful.

You're not just offering training—you're empowering your employees to level up their skills and stay relevant in a tech-driven world. When your team sees AI as an ally, they'll embrace it as a tool for growth, not a threat.

Make it clear: AI is here to enhance their roles, not diminish them. Over time, as they become more comfortable with AI, they'll see it for what it is—a collaborator, not a competitor.

The Big Takeaway: AI Is Your Team's Secret Weapon

AI isn't a threat to your team—when properly introduced, AI can be an opportunity to learn and grow. When you bring your team along for the ride—through open conversations, continuous training, and a collaborative approach—you'll create an environment where AI is seen as a tool to future-proof the business, not a threat to job security.

To get started, here's a quick **AI Starter Pack**—user-friendly tools that can boost productivity right away:

- **Grammarly:** Perfect for anyone who writes emails, reports, or content. It helps with grammar, tone, and even style suggestions.
- **ChatGPT:** Great for generating ideas, drafting content, or answering questions in natural language.
- **Trello with AI plugins**: Helps teams manage projects and tasks, with AI providing smart suggestions for better workflow.
- **Zoom with AI integration:** Automates meeting notes and highlights key points, so you don't have to.
- **Zapier:** Allows you to automate workflows between apps—think "set it and forget it" for repetitive tasks.

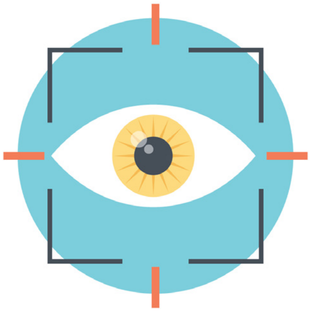
These tools are designed to make life easier and more productive without being overwhelming. With the proper guidance, they might just show your team see the positive side of AI.

Ready to Introduce AI to Your Business?

So, what's the next step? **Start by fostering a culture of curiosity and transparency.** Encourage your team to ask questions, provide training opportunities, and remind them that AI isn't here to take over—it's here to help them shine in their roles.

If you're looking to implement AI to benefit your business and your team, we're here to help. Whether it's choosing the right tools, offering training, or facilitating those critical conversations, we've got your back. Let's talk about how we can make AI work for you—and your team today.

Technology Update



Did you know… you could soon type with your eyes?

Sounds crazy, but Microsoft is developing an Eye-Gaze technology that will help people type and interact with applications using just their eyes.

It uses so-called ‘dwell-free’ typing, meaning you’d just need to look at keys on a screen and the technology would – supposedly – understand the actions you want to take. The tech also uses AI to gather information that makes predicting behavior patterns more accurate.

Do you think that’s cool… or scary?!

How To Make the Pain of Passwords Go Away

Passwords. They're the keys to our digital kingdoms, but also the biggest pain in our necks. They've been around since the dawn of the internet, and guess what? Even with replacements being introduced, they're not going away anytime soon.

I'm sure you've felt the pain of managing a billion passwords for all your accounts. It's exhausting and risky. Perhaps it's time you considered using a password manager.

The real beauty of password managers is you only have to remember one password – the master password to log in to your manager. Then, it does everything else for you.

- It creates long random passwords
- It remembers them and stores them safely
- And it will even fill them into the login page for you

That means no more racking your brain trying to remember if your password is "P@ssw0rd123" or "Pa55w0rd123" (both are really bad and dangerously weak passwords by the way). With a password manager, all the work is done for you.

We won't sugar coat it – password managers aren't invincible; they have their weaknesses. Cyber criminals can sometimes trick password managers into auto filling login details on fake websites.

But there are ways to outsmart criminals. First, disable the automatic autofill feature. Yes, it's convenient, but better safe than sorry, right? Only trigger autofill when you're 100% sure the website is legit.

When choosing a password manager, go for one with strong encryption and multi-factor authentication (MFA) where you generate a code on another device to prove it's you. These extra layers of security can make a big difference in making your accounts impenetrable.

Enterprise password managers offer useful features like setting password policies and analyzing your teams' passwords for vulnerabilities. Plus, they often come with behavior analysis tools powered by machine learning tech. Highly recommended.

But here's the thing – no matter how advanced your password manager is, it's only as good as the person using it. So, do yourself a favor: Train your team to stay vigilant against scams, and always keep your password manager up to date.

We can recommend the right password manager for your business and help you and your team use it in the right way. Get in touch.

Do You Have A BYOD (Bring Your Own Device) Policy?

Letting employees use their personal devices for work might seem like a win for your budget, but have you thought about the risks?

More and more companies are ditching office PCs and letting people bring their own laptops, tablets, or phones. Sure, it sounds great—until you realize personal devices often don't have the same level of security as company-owned ones. And that's a big deal when it comes to keeping your business and customer data safe.

Cybercriminals love targeting personal devices because they often lack the layers of protection you'd find on corporate machines. That's why it's crucial to ensure every personal device has security features installed and stays updated. No one wants to learn the hard way that their outdated phone became the gateway to a data breach.

Another thing to consider is access control. Personal devices are more likely to be used by family members (looking at you, kids!) or friends. Setting up strict access controls ensures that work devices stay, well, for work. You don't want anyone accidentally (or intentionally) messing with sensitive company info.

And mixing work with personal data? That's just asking for trouble. It opens the door to privacy issues, not to mention the possibility of compliance breaches. Make sure your employees know the risks and give them guidelines on how to keep personal and work data separate.

BYOD might seem like a smart, cost-effective choice, but the potential security risks and costs of a data breach can quickly erase any savings. Sometimes, investing in company-managed devices ends up being the smarter move in the long run.

You'd Be Lost Without It, So Don't Forget Email Security

Let's talk about something super important: Email security.

Yep, we know it might not sound like the most thrilling topic, but it's a big deal. Businesses like yours face more cyberthreats than ever.

We've seen our fair share of cyberattacks, and let us tell you, many of them start with a simple email (official figures say it's a massive 90%!). Yep, that innocent-looking message in your inbox could be the gateway for cybercriminals to wreak havoc on your business.

So, why is keeping your business email secure so important?

Well, for starters, it's your first line of defense against cyberattacks. Think of it like locking the front door of your house to keep out intruders. If your email is secure, you're making it a whole lot harder for cybercriminals to sneak in and steal your sensitive data.

But implementing proper email security measures safeguards your valuable data from getting lost or falling into the wrong hands. It's not just cybercriminals you're at risk from; an employee could accidentally leave a laptop on a train or in a coffee shop. That could mean all your important business communications and documents were suddenly open for someone else to read. It would be a nightmare, right?

You might be thinking, "But I'm just a small business. Why would I be a target?" Ah, but here's the thing – cybercriminals don't discriminate based on business size. In fact, small and medium-sized businesses are often seen as easier targets. That's because they may not have the same level of security measures in place as larger corporations. So, don't think you're off the hook just because you're not a Fortune 500 company.

Now that we've established why email security is crucial, let's talk about how you can ramp up your defenses. First off, use strong, unique passwords for your email accounts. None of that "p@ssW0rd123" nonsense, please. Better still, use a password manager to create and store uncrackable passwords.

Consider implementing two-factor authentication for an extra layer of security (where you generate a login code on another device to prove it's you). And don't forget to keep your software and security patches up to date – those updates often contain important fixes for vulnerabilities that cybercriminals love to exploit.

Lastly, educate your employees about the importance of email security. They could be your strongest defense or your weakest link when it comes to keeping your business safe from cyberthreats. Teach them how to spot phishing emails (emails pretending to be from someone you trust) and what to do if they suspect something isn't right.

Remember, a little prevention now can save you a huge headache (and money) later. If we can help with that, get in touch.

Q&A

Will a free VPN (Virtual Private Network) provide enough security for my employees' work phones?

No. The chances of a free VPN logging and selling your data or infesting your device with malware are a lot higher than if you used even the cheapest paid VPN on the market.

I hate sudden reboots for updates on Windows 11, is there a way to avoid them?

Yes! Open "settings" and click on "Windows update" and then "advanced options," you can then set your "Active hours." Updates can be scheduled, where possible, outside of these hours.

I hate my password manager, is it easy to change?

You can export your data, but it's important to use a secure computer to do it. You should also be careful not to back up the unencrypted file.
We can help you – get in touch.

Submit Your Questions Here:
info@meetingtreecomputer.com

This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Follow Us