

How To Effectively Apply Technology In Your Business



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

Technology can help your business to become significantly more efficient, engaging, and highly successful in your industry.

Implementing the right technology can greatly help transform business infrastructure.

Here are nine of the most common and groundbreaking technologies that can help your company succeed today.

Use of mobile apps

You can improve your business's overall reputation and seek higher brand recognition by introducing a mobile app with your business logo.

This keeps your products, services, and customer support at your client's fingertips wherever they are. And depending on the complexity of your business, it can be surprisingly affordable.

Business operation automation

Not only can this greatly improve efficiency and reduce costs, the use of automation technology helps free up resources that can be re-directed

to higher revenue-generating tasks that in turn, increase customer satisfaction.

Use of artificial intelligence

This modern technology can exhibit human-like behavior. For example, when your customers visit your website, they can benefit from communicating with a Chatbot.

Chatbots are a form of artificial intelligence that informs your customers with and answers their queries by using existing data.

AI can also enable your business to better use the large sets of raw data acquired from your customers behaviors. By analyzing and setting trend patterns, your business can ensure more effective decisions.

Virtual reality (VR)

You can use VR to form virtual environments and settings to understand concepts and ideas better. You can use it to design and showcase your latest products.

You can view a 3D model of a product before you actually manufacture it allowing you to make any necessary changes before you begin production by using VR models and testing.

Cloud computing

Cloud computing can help your business reduce IT infrastructure

costs by providing a virtual resource space for your operations.

Using a combination of hardware and software by hosting your data on virtual platforms, you can create a highly scalable infrastructure ready to grow (or shrink) as your business needs change.

Hybrid workplaces

Hybrid workplaces are a modern solution to the complex problem of social distancing. Offering employees to either work remotely or in-office can help to lower business costs.

In addition, hybrid workplaces allow employees to work more flexible hours, which boosts productivity. This allows for business expansion in terms of operations and employee base without substantial costs and investments of traditional offices.

Project management tools

These tools allow remote access, multiple project management, progress-tracking, and much more. Your teams can use such tools to meet deadlines, track their progress, and ensure effective project management.

Time-tracking tools

Time-tracking tools greatly complement project management tools as they help keep track of the time

Using a combination of hardware and software by hosting your data on virtual platforms, you can create a highly scalable infrastructure ready to grow (or shrink) as your business needs change.



Continued on page 4



Free VPNs Are Not Your Friend

“If you’re interested in a VPN for business or personal use, it can be tempting to go with a free option – but be careful. Some freeware (software published for free download) can be a great find, but much like work shoes or your mattress, you want to find something that does its job well, even if it costs a little more.”

Prior to the pandemic, VPNs (Virtual Private Networks) weren’t in the toolbox of the average office worker. Many of us sat down at our desk and logged into our computer, websites, and programs, then got started on our day.

Whatever we needed was a click away, our access already nestled into a secure network. Work-from-home has changed the game and requires a security boost wherever possible.

VPNs help with that by establishing secure connections, protecting your privacy, and allowing you to access your work network from home or anywhere else.

At a glance, VPNs seem to function similarly to remote desktop connections, which many businesses are more familiar with now, however they have some key differences. A remote desktop connection allows you to control a specific computer via software while a VPN provides encrypted access to a network while away.

If you’re interested in a VPN for business or personal use, it can be tempting to go with a free option – but be careful. Some freeware (software published for free download) can be a great find, but much like work shoes or your mattress,

you want to find something that does its job well, even if it costs a little more.

Cheap shoes and mattresses may leave your body sore while a free VPN could be a gigantic security risk to your company or home network.

Like many freeware programs, you can’t always trust a devel-

however, is unlikely to have the same level of security or the same capability to patch vulnerabilities, even if they have good intentions.

Additionally, you want whatever VPN you use to actually work. Free VPN services can’t support users the same way as a paid service. At best, they can be slow, lagging, or non-functional while their resources are spread thin across their userbase. At worst, you may be roped into some shady cybercriminal practices like botnets.

If you’re a small business looking to set up a VPN, we recommend researching which of the trusted, big-name VPN providers match your needs and budget.

Many come with free trials so you can test them out before you buy. If you have a managed service provider like Tech Experts or an IT department, please reach out to your technology partner and ask about options.

A secure VPN service is worth the cost to protect yourself from cyberattacks, vulnerabilities, and identity theft. Free is nice, but it’s better to take advantage of free things that don’t have the potential to infect and bring down your company’s network. Give us a call at (734) 457-5000 to learn more.



oper. There’s usually a catch, and for VPNs, that comes at the price of security. VPN services aren’t cheap to provide, for one, and the free ones aren’t shared out of charity; they likely have interest in selling your data, bombarding you with ads, infecting you with malware, or stealing your identity.

One of the main motivations for using a VPN in the first place is to create a secure connection. A paid service will provide that – that’s what they’re there for and that subscription is how fund their operations. A free service,



2021 Cyber Attacks - Lessons To Apply For A More Secure 2022

Hackers have hit a wide variety of industries this year, from computer manufacturers to insurance companies, schools to the NBA. A review of prominent 2021 cyber attacks reveals a few common themes. And organizations that apply the lessons learned from these attacks can look forward to a more secure 2022.

No one gets a free pass

It would be difficult to describe the profile of a typical data breach victim in 2021. Large corporations like Volkswagen and Experian got hit. At the same time, even small, low-profile businesses suffered in the Microsoft Exchange and Kaseya attacks. Ransomware crippled hospitals, manufacturers, municipalities, retail and more.

No matter how big or how small, any organization with Internet connections can become a target of attack. Hackers continually hone their skills and add to their toolsets. Consequently, businesses cannot afford to relax their security stance. Get started early on your New Year's resolutions by committing to invest in cybersecurity.

Apply security patches quickly

When hackers exploited vulnerabilities in the Microsoft Exchange server, they disrupted 60,000 companies and government agencies in the US. Microsoft released security patches quickly. However, many organizations delayed applying the patches. The attack group Hafnium then ran Internet scans to find and exploit unpatched servers.

Take the time to apply software and firmware updates quickly. Take it a step further and turn on automatic updates where possible. This applies not just to servers but to all devices with access to the system.

Step up endpoint security

The rapid switch to remote work

completely changed the security perimeter for many organizations, and hackers took advantage. For instance, when insurance giant CNA sustained a ransomware attack, 15,000 devices were encrypted, including those used by remote employees.

When remote work takes center stage, organizations need to strengthen endpoint security. Begin by creating and updating an inventory of all devices connecting to the system.

Enforce strong authentication policies and keep endpoints encrypted. Additionally, monitor the endpoints for unusual activity when connected to the network.

Monitor those business partners

In April, the REvil gang attacked Quanta, a supplier for Apple. REvil used the attack to pressure Apple, claiming to have obtained secret blueprints for yet-to-be-released Apple products. Similarly, parking app Park Mobile suffered a breach because of a vulnerability in a third-party software app.

While strengthening inhouse security, organizations cannot forget about their business partners. Be sure to vet third parties, building security policies into vendor contracts. Then continue to monitor those relationships, including performing regular audits.

Automate the backup process

Fortunately, the list of 2021 cyber attacks includes some positive notes. Attackers hit Polish video game development firm CD Projekt, encrypting devices and accessing source code. However, because the company had quality backups in place, they were able to restore the lost data without paying the ransom.

For decades, security experts have emphasized the importance of per-

forming regular backups. Automating the process takes the burden off IT and delivers peace of mind.

Strengthen authentication and identity management

In April, attackers used a compromised password to access the networks of Colonial Pipeline, disrupting gas supplies and causing panic.

As government officials investigated, they concluded that stronger protections, such as multi-factor authentication, could have prevented the attack.

Identity and access management form a critical component of securing valuable digital assets. Companies should assess and strengthen authentication methods and tighten access controls.

Take protective steps against phishing

According to a recent report on cybersecurity breaches, phishing remains the most common type of cyber attack. For instance, in an attack on Nebraska Medicine, hackers gained entrance to the system and planted malware, eventually exposing over 200,000 patient records.

To protect against phishing and other social engineering attacks, organizations should implement email filtering and continuous network monitoring.

But the most important safety measure remains addressing the human factor with regular, targeted security awareness training.

Treat 2021 cyber attacks as a wakeup call

Reflecting on the high-profile cyber attacks of the past year can provide both the motivation and a blueprint for addressing cybersecurity. And the cybersecurity experts at Tech Experts bring the expertise and tools you need to keep your data and networks safe.

“No matter how big or how small, any organization with Internet connections can become a target of attack. Hackers continually hone their skills and add to their toolsets. Consequently, businesses cannot afford to relax their security stance. Get started early on your New Year's resolutions by committing to invest in cybersecurity.”



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

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

Ten Awesome Social Media Automation Tools

In the last decade, developers from famous social media platforms have changed the way we use their applications. Social media platforms are now excellent tools for marketing products and brands—these platforms act as great sources of exposure for small, medium, and even huge businesses.

Here are 10 of the top Social Media Automation Tools, which you can utilize as the first step towards automating your business.

Workflow

Workflow helps you organize a proper system as needed and share content according to plan. It allows you to promote the right content with the right audience at the right time.

Hootsuite

Hootsuite enables you to keep an eye on your competitors and communicate with your audience and users by creating a community dedicated to your business.

Sendible

You can automate replies to the audience’s queries, collaborate with others, generate valuable reports, and schedule updates with Sendible. This multi-purpose tool will help you organize and plan posts so

your marketing team can focus on important tasks and activities.

CoSchedule

This automation tool helps you schedule your posts, thereby saving a lot of time and effort. CoSchedule enables you to schedule up to 60 posts at once.

Chatfuel

Chatfuel enables you to create a chatbot that engages customers and provides accurate responses in real-time to enhance customer satisfaction.

Agorapulse

You can schedule your social media posts and track the performance of your posts to make better decisions. You can engage a larger audience using their informative reports. Their social media management features are amazing.

SEMrush

This all-in-one digital marketing automating tool is the best PPC and SEO toolkit. This tool allows you to automate posts, promote campaigns, track results, and generate valuable analytics.

Tailwind

This scheduling tool also helps with

analytics. Tailwind will not only help you automate posts, but it provides posting recommendations so you can reach more potential leads.

Later

With 600,000 happy users, you can already assume this tool’s popularity. This tool allows you to manage your social media comments.

Furthermore, it lets you schedule Instagram posts and increase engagement.

Iconosquare

Iconosquare provides personalized information for social media platforms. This way, your business can progress with social media marketing campaigns using informed decisions. Save time with their in-depth analytics and reporting.

Automating your marketing process and method helps minimize errors and understand customer behavior while saving time, effort, and money. You can even schedule the entire campaign and stay ahead of competitors.

So choose the best social media automating tools from the list above and take the first step to business automation.

How To Effectively Apply Technology In Your Business, continued

spent on each individual task on a project. This helps your team perform tasks within the given time-frames for increased productivity. This will also help identify tasks that are potential time wasters or require more careful planning.

Social media platforms for marketing

Using social media platforms to market your products,

services, business, and brand is one of the principal uses of technology today.

Utilizing several social media platforms in tandem allows you to reach a larger audience worldwide and boosts your brand recognition and sales.

Plus, it also helps you identify the potential market gaps that you may be able to fulfill.