February 2021

TechTidbit.com

brought to you by Tech Experts

Three Ways That Technology Has Transformed Businesses

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

Breakthroughs in technology have torn apart old ways of working, as new alternatives have become impossible to ignore.

Here are three examples of ways that technology has transformed businesses everywhere.

Instant customer service

As new methods of communication have emerged, businesses have been able to significantly increase the quality and availability of the customer service they offer.

Instead of relying on face-to-face meetings or telephone calls to answer customer questions, businesses can now help through immediate online channels like live chat.

This is convenient for many customers, as they can talk at the exact moment they need help. It allows them to get immediate answers to their questions without needing to navigate telephone menus or book an appointment.

AI chatbots enable customers to get answers to their questions without humans involved. The technology that powers AI chatbots is getting both more affordable and more advanced, making them a good alternative even for small companies.

By allowing questions to be asked in natural language, chatbots offer a way for businesses to help their customers 24/7 and can significantly reduce the demands on customer service staff.

A revolution in advertising

Google and Facebook have completely changed the face of advertising.

By giving businesses the ability to deliver highly targeted ads, Google and Facebook give businesses the tools they need to deliver the right message, to the right person, at the right time. And then analyze the results with an extreme level of precision.

Far from being confined to global brands with huge marketing budgets, this technology has given businesses of all sizes access to the same advertising venues and tools that huge businesses use.

The amount of money that businesses need to invest in advertising has decreased. Small businesses are able to run campaigns that get results for only a few dollars.

Remote working during the pandemmic

How do you think businesses would have coped if the pandemic had arrived in 1990 instead of 2020?

Technology has enabled millions of businesses to keep running at a time when it's been impossible for much of the world to physically meet.

Tools like Microsoft Teams have made it easy for colleagues to collaborate and work together. With real-time messaging and countless options for video calls, people can work well as a team regardless of where they're based.

Cloud computing has made it easy to access the software and data everyone needs to do their jobs, often from whatever device they can get their hands on.

Instead of relying on face-to-face meetings or telephone calls to answer customer questions, businesses can now help through immediate online channels like live chat.

Heads Up: Hackers Are Exploiting Email Forwarding Rules

"If a hacker takes advantage of this, then all your email will be sent to and read by someone you do not even know."

Mark Funchion is a network technician at Tech Experts.

The ways in which hackers attack accounts are endless, and a lot goes into keeping your accounts both safe and usable.

A newer attack style that is being used (and one we have personal experience with resolving) is the manipulation of email forwarding rules.

Email forwarding rules are rules that are set up in your inbox to forward a message to another mailbox as soon as it arrives.

The danger for the email owner is that these rules can also clean up after themselves by deleting the message, preventing a copy of the forward from showing in the "Sent Items" folder, and deleting the message from the "Deleted Items" folder.

If a hacker takes advantage of this, then all your email will be sent to and read by someone you do not even know.

Think about the items in your inbox, especially the ones that are sensitive and/or confidential. Can you risk there being a period of time where your messages are being forwarded without your knowledge?

Also, as the hackers are good at cleaning up and hiding their tracks, you need someone with the experience and expertise to resolve this for you if it does occur.

One of the big dangers with this attack style is that changing your password or adding two-factor authentication will not stop the current breach once the rule is in place.

Forwards will continue to be sent because the rule is not password dependent. It's the same with two-factor authentication; if you enable this after the rule is in place, it will not do you any good.

There are steps that can be taken to prevent these types of attacks, however most of them are not settings that an end user would be familiar with.

It's important to not allow forwarding to occur to email addresses outside of your domain, and relatedly, it's a good idea to allow the full sync of settings between the web client and the local desktop client.

For example, Office 365 by default will not sync these settings, so if someone gains access to your email and creates a forward on the web page, you and your IT department will not see it if they look in your Outlook client on your local computer.

These rules can be hidden if the hacker knows what they are doing. This means a quick open-and-check-if-a-rule-exists is not sufficient. Steps need to be taken to make sure there are no rules, not just a lack of visible rules.

Checking for these rules if there is a suspected breach is critical because of another potential problem: if you do a password reset on another account that you are concerned about (for example, your bank because you use the same password), that email with details gets forwarded to the hacker and they may be able to gain access to that account.

Hackers will continue to evolve as they need to. As this exploit is discovered and procedures are put in place to mitigate their effect, the next exploit will be used and the cycle will start again. Having a partner to help you navigate through all these potential issues is essential.

Being aware of these exploits, watching for new ones, and making necessary changes to keep your business safe is a big part of what Tech Experts does.

Handling these concerns is part of our core business, giving you the peace of mind to handle your core business.

Changing the font in a document can save printer ink. The theory is, if you switch to a lighter stroke, you'll use a little less ink per page, meaning around a 10% saving when printing large quantities. Check your printer settings, too. Many have a toner saving mode built in.

How Do You Know When Your Systems Are Due For An Upgrade?

Some problems are difficult to spot. They bubble under the surface without getting noticed until it's too late.

Other problems hit you straight in the face, normally at the worst possible time.

When it comes to your business's IT, you need to keep an eye out for each of these, as things can get nasty if you don't stay on top of things.

Keeping your IT updated is a good start, but it isn't enough on its own. How do you know what to look out for? Let's look at some of the main culprits.

The slow creepers

Slow computers are a big one, and they're quite tricky to spot because they gradually slow down over time.

This means that people using them gradually adjust to degrading levels of performance without necessarily being aware that's happening.

The same is true for software. As staff get used to using slow and buggy tools, it gets normalized and the IT gremlins become acepted as part of their daily life. It's always worth fixing slow devices and processes. Speeding them up will let your staff be more productive. And give morale a boost too.

Out of date systems

Another thing that can be difficult to spot is when warranties run out.

On top of official warranties, IT systems also have a separate lifespan for how long vendors will continue to offer updates. Pushing this to the edge can significantly impact features, compatibility, as well as security.

Your customers don't have much patience for slow or clunky processes.

It can be difficult to measure how much business you lose on the back of this, so frequently auditing your systems is key to avoiding missed opportunities.

Too old to scale

If your IT systems aren't scalable, there's a real risk that your business will need to start turning down work because you're not able to handle swings in demand.

It's worth bearing in mind that there's a far greater chance of experiencing big changes in consumer behavior in 2021, both during and in the aftermath of this pandemic.

Also, if you're running out-of-date IT systems, you're living with the risk that you won't be able to quickly adopt new ways of working, as technology changes your industry.

What can you do?

An important first step is to have an IT strategy in place that acts as a foundation for your business.

Instead of reacting to problems as they come up, an IT strategy will help you plan for future scenarios. As well as acting as a solid foundation to help your business make the best possible decisions about the future.

A good IT strategy creates a technology roadmap for getting your business up to speed and keeping it there.

"If your IT systems aren't scalable, there's a real risk that your business will need to start turning down work because you're not able to handle swings in demand."

Create new service requests, check ticket status and review invoices in our client portal: http://www.TechSupportRequest.com

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

Everyone On Your Team Needs Cyber Security Training. Including You!

Every good business leader knows that training is essential for a highly productive team.

But have you ever considered giving your staff cyber security training? You really should.

What is it?

It's about increasing their awareness of the ways that criminals try to break into your IT system, and the devastating consequences if they do.

So, they'd learn:

- How to spot the different types of fake emails and messages, and what to do with them
- The risk of social engineering by email, phone, or text message
- Why we use basic security tools such as password managers and multi factor authentication (where you generate a code on another device)

By holding regular cyber security training sessions, you can keep everyone up to date. And develop a great culture of security awareness.

It's another layer of protection to help ensure that your business doesn't become part of a scary statistic (one small business is hacked every 19 seconds).

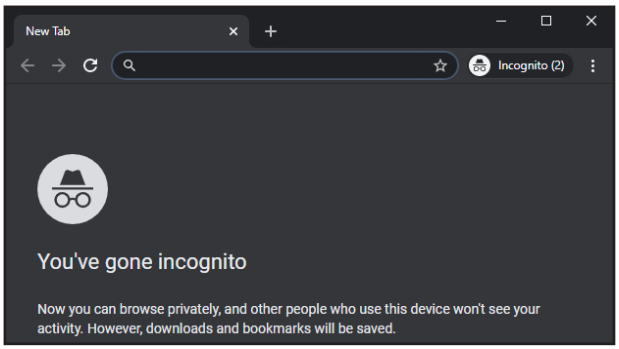
As the company owner, it's critical you do the training, too.

You'll be one of the most targeted people in the business, as you probably have access to all the systems, including the bank account.

If you don't already have cyber security training in place, we'd love to help. Give us a call at (734) 457-5000, or an email to info@mytechexperts.com.

Is It Time To Go Undercover?

When you hear the phrase 'incognito mode,' do you think of the undercover detective image in the Chrome window?



Well, incognito mode, or private browsing isn't just there to hide your browsing history.

It can be utilized for an added layer of protection against cyber-crime. You see, when you use a private browsing window, it doesn't record the websites that you've visited (not on that machine, anyway). Cookies and other trackers are only used in that session - not saved.

Nor does it automatically remember your login details, save temporary files, or store cookies.

Private browsing also allows you to log into several accounts on the same app at the same time, which can be convenient for things like social media, email, or file sharing.

Did you know that administrators CAN still see employees' activity in incognito? So, you don't need to worry whether an employee is secretly spending too much time on Facebook.

If you'd like any further information on how to keep your business more secure, we'd love to talk. Give the helpdesk a call at (734) 240-0200 or email us at support@mytechexperts.com.