March 2015

TechTidbit.com

brought to you by Tech Experts

How The "Internet of Things" Will Affect Small Business

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

Just when you thought you had the Internet mastered, something new crops up on the horizon.

One of the newest advances that will likely revolutionize the world is the Internet of Things (IoT).

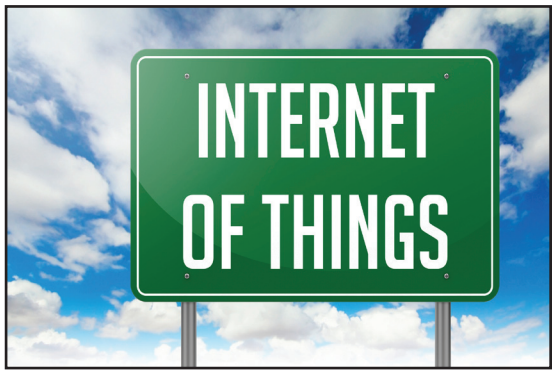
If you haven't heard of this, you're not alone, but this idea is fast becoming a realization. Simply put, the IoT refers to how it is possible to remotely control and monitor just about anything via sensors and, of course, your Internet connection – from opening your home's garage door from your office to the level of dog food remaining in your pooch's bowl.

This concept recently gained definition at Apple's Worldwide Developer Conference when the company unveiled two applications for iOS8.

The first was the HealthKit app, which lets users keep up with health and fitness data without wearing an actual tracker.

The other was the HomeKit that can remotely control electronic devices like lights and cameras at home.

While these developments are geared toward individuals, the impact this type of technology can have on businesses is astronomical, especially in revolutionizing small business.



The most readily recognizable change the IoT can bring for small businesses is an increase in efficiency and, consequently, productivity.

Once the proper equipment is installed, inventory can be checked right from the Internet without ever making a trip to the warehouse or sales floor.

When this inventory is monitored by a computer, it is also free of human error, so it is more accurate. The IoT can be adapted to send alerts when systems require maintenance as well.

The Internet of Things won't just improve how small businesses operate, it will create opportunities for entirely new small businesses to develop.

After all, someone has to install and repair the required equipment. There will also, undoubtedly, be other ways to capitalize on this new technology that cannot be presently foreseen. So, while automating many processes with IoT may phase out certain roles, it will open the door for new roles to be filled.

One of those potential roles may be in security, preventing hackers from having a heyday in the IoT.

With more online connectivity, there are more access points to small business systems.

This will require IoT experts to be vigilant against new threats and discover ways to thwart the efforts of cyber criminals.

Online Safety: Is Your Website Secure?

Michael Menor is Vice President of Support Services for Tech Experts.

For all too many companies, it's not until after a breach has occurred that web security becomes a priority.

While more than a few examples of recent breaches may leap to mind, know that these aren't exclusive to big name retailers who accept credit cards. If you have a website for your business, you may be at risk.

As more and more business is done using the World Wide Web, websites themselves have become increasingly attractive to cybercriminals.

Websites are such a lucrative target for an attack because not only are there so many sites to attack, but an overwhelming majority of all websites can be easily exploited by some of the most common vulnerabilities.

Attackers, no longer driven by notoriety and ideology, have focused more on techniques that allow them to profit from their illegal activities.

Exploited sites allow the theft of credit card data, financial information, identities, intellectual property, and anything else cyber criminals can get their hands on.

The integrity of the company's internal network can be affected as well if the website provides access to it.

There are many online services that allow anyone to create a webpage in under ten minutes.

Unfortunately, these quick solutions also make it easier for attackers. Without proper training and knowledge, many of these sites are left with multiple vulnerabilities. A few of these vulnerabilities will be discussed.

The Heartbleed Bug is a vulnerability that allows attackers to obtain confidential data such as usernames, passwords, emails, and even proprietary company data and communications.

Even if you think you might be protected because you use encrypted forms of communication, you're not safe. Attackers will be able to eavesdrop into your communications and steal data from beneath you.

Like Heartbleed, one of the most prominent vulnerabilities affecting web applications is cross site scripting (XSS).

This vulnerability can allow an attacker to hijack web communications. The attacker may target a vulnerable website by tricking the user into submitting sensitive information or performing a privileged action within the target website's web controls.

Application Denial of Service attacks have rapidly become a commonplace threat for doing business on the Internet — more proof that Web application security is now more critical than ever. Denial of Service attacks can result in significant loss of service, money and reputation for organizations.

Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services.

Denial of Service attacks are centered on the concept that by overloading a target's resources, the system will ultimately crash.

An HTTP Denial of Service attack can also destroy programming and files in affected computer systems.

In some cases, HTTP DoS attacks have forced Web sites accessed by millions of people to temporarily cease operation.

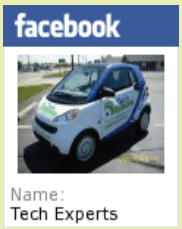
Websites that can be compromised pose a serious risk and thus serious preventative measures should be taken to combat it.

Scrambling to fix the problem after the fact is costly, stressful, and can potentially result in legal action. Breaches also cause damage to your company's image and brand, which may be permanent.

Know your vulnerabilities and don't rely on ten-minute-or-less website creators to keep you safe.

If it's too good to be true, it probably is.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

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

The Importance Of Centralized Storage

Scott Blake is a Senior Network Engineer with Tech Experts.

Do you know where all of your data is? Is the file you're looking for saved to workstation-01 or workstation-12? What happens when a user deletes a file you need from their workstation? What happens if your workstation dies?

If you're a business owner or manager and have trouble answering those questions, centralized storage of your data may be your answer.

You can remove the stress of accidental deletions, have direct mapped access to your files, secure your data from intrusion and, most importantly, make it easy and simple to back up your data.

Centralized storage can include an external hard drive, USB flash drive, NAS (Network Attached Storage) device, cloud environment, or storage on a server. The best method is determined by your business structure.

Smaller businesses may opt for simple external devices attached to a workstation or a NAS device to save and back up their data. Simple external devices such as larger-sized USB flash drives and external hard drives are a low-cost solution.

NAS devices cost more, but they are useful additions to business networks. Most mid-ranged NAS devices offer raid levels 0, 1, and 5, so they can be customized for speed or data protection.

Some NAS devices are running a server-style operating system that will integrate into your existing AD. This will offer additional security features over a simple external hard drive or USB flash drive.

Businesses and home users that opt for the simple and least expensive method need to be very diligent about their data. Smaller devices are more susceptible to theft and damage.

They also tend to have shorter lives than other more costly methods. Should you go this route, make sure you maintain backups of your data and immediately replace your device at the first sign of possible hardware failure.

Data recovery from a simple solution device may not always be possible and it can become very costly to try.

Larger businesses will want to opt for on-site storage with network drives and backup solutions in place. Or they may want to invest in the cloud for a storage.

Most medium-to-large scale businesses already have some form of a network server and backup in place, so all that may be needed is additional hard drive space or the creation of folders to house data.

You may also want to install a dedicated server for just data storage and possibly to handle your printing management. Cloud-based storage can be costly depending on the amount of data that needs to be stored, the security level, and the number of simultaneous connections to your data.

Cloud-based methods tend to be best as a secure backup option, but can be used for raw storage. With web-based access, all your employees need is an Internet connection to access their data.

Both on-site server storage and cloud storage offer strong backup options, the ability to restore deleted files, ease of access from off-site locations, and the sharing of files and folders across a wide area.

Whether you choose to go with a low-cost simple solution or a more robust solution, centralized storage brings peace of mind that your data is accessible and secure.

Your business will become more efficient and streamlined just by maintaining your data in one easy-but-secure location for your employees to access.

For more information about implementing centralized storage in your business, call the experts at Tech Experts: (734) 457-5000.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(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) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Beware Of These Tax Return Scams

In the online world, it seems that there is always a new threat cropping up on the horizon. There is one, however, that has been returning year after year following the onset of online tax filing.

This is the prime time for tax phishing scams, and it is important to recognize the signs of a cybercriminal going after your identity and holdings.

Since tax season is often a mystifying time financially with ever-changing laws that directly affect your pocketbook, it isn't far-fetched to believe the IRS or a related government agency may need to double-check your data or ask for additional information via email or text.

This is a situation that sophisticated thieves are well aware of, and they do not hesitate to exploit citizens' lack of knowledge of how the revenue service actually conducts its business.

In fact, approximately 25,000 phishing emails (messages asking for personal data like Social Security numbers and the like) and 611 scam websites were shut down during the last tax season. It is probable that far more efforts went unreported.

Fortunately, it is easy to thwart criminals' efforts to gain access to your personal information and financial holdings when you are on the alert.

First, no government agency will ask for such information through an unsecured email or text. If the tax agency, tax-preparation company, or related organization needs additional sensitive information from you, you will be contacted by mail, phone, or directed to a secure website.

In the case you are suspicious of a particular communication, double check that the email or physical address matches that of the legitimate organization.

Also, beware of messages that do not use your full name with something generic, such as "Dear valued customer," or warn that there will be dire consequences if you do not reply right away.

If there is any doubt whether an email or text is a scam, report it to the organization in question or law enforcement agencies.

Remote Access And Security For Your Business

Working remotely is on the rise and is revolutionizing how business is conducted as a whole. As companies make the switch from centralized networks that require being physically present in the office to expansive virtual environments, it is possible to access corporate data from just about anywhere. Those companies that resist embracing remote access risk being left behind technologically and miss out on all of the benefits using things like clouds or application virtualization can bring.

Just by providing remote access to corporate files and programs, employees can work from anywhere on the fly. This allows your team to work on projects while at home or out of town, greatly increasing productivity and reducing the stress of trying to meet deadlines when life gets in the way and prevents being physically in the office. Remote access also lets employees view or share important documents from other devices, such as smartphones or tablets, to quickly verify information on the fly or perform last-minute tasks with ease.

With remote access, new security concerns also arise. With the transfer of sensitive data, there is the risk of it being intercepted by a third party that isn't committed to your company's success or has the intent of doing harm.

Consequently, it crucial to secure your remote access system. Secure remote access will ensure that files are encrypted during transfer, scan for malware, authenticate user identity, and control who has access to particular information.

In these ways, proper security measures not only prevent those outside the company from gaining access to private data, but also manage who can view and use data internally.

With the proper security, a business can thrive beyond expectation. Employee performance can skyrocket by having access to work data 24/7 and from any location because physical presence in the office is no longer a prerequisite to getting work done.

Business continuity is also greatly improved because inclement weather or natural disasters don't shut down operations and the meeting of deadlines. Secure remote access can even boost employee morale and productivity by facilitating work in varied locations using multiple access mechanisms.

If you require assistance setting up or securing remote access to your business, let us know and we will show you what works best for your situation.