December 2017

TechTidbit.com

brought to you by Tech Experts

Five Ways To Take Your Business Paper Free

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

If you're a small business owner, chances are you always have one eye on your operating costs and the best way to reduce or eliminate extra expenses and improve staff efficiency.

One way in which you can gain some great cost savings is by eliminating paper.

Paper-based tasks increase storage, postage, and compliance costs and can be a major overhead for modern-day businesses.

Here are five ways you can reduce paper usage and save yourself some cash in the process.

Smart Project Management

Traditionally, the process of managing company projects that involve different departments and multiple people generates massive amounts of paperwork.

More contemporary organizations are taking the smart project management approach through the use of cloud-based solutions, such as Basecamp, Asana or Trello, which allow you to ditch the paper while running a project online with unlimited users.

Electronic Payroll

Rectifying payroll issues costs half of all small business an average of $850 annually.

Using decent payroll software reduces the errors and facilitates paperless processing. An electronic payroll system automates all the manual calculations such as tracking hours worked, calculating salaries, and filing taxes.

Salaries can also be paid electronically rather than printing checks or visiting the bank.

The additional benefits of electronic payroll include self-service functionality, and allowing staff to view their payroll data, such as personal details, tax deductions and pay slips online from any device.

Receipts and Invoices

Eliminate paper (and postage costs) by offering customers the option to receive electronic receipts either by email or text.

Your customer will then have it for future reference. Ask suppliers to issue and email digital invoices, which you can save into your accounting software.

Cloud Storage

Small businesses spend a lot of money to purchase, fill and maintain filing cabinets!

Switching to cloud storage can reduce most of this cost as many services, like Dropbox, offer a free allowance.

Most cloud-based options also allow you to organize documents into separate folders.

Customer Relationship Management (CRM) Software

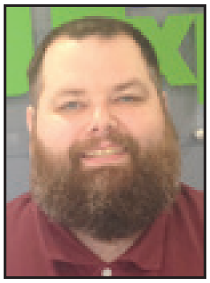
CRM software can reduce the extent to which you rely on paper to store and track customer details, purchase orders, quotes and other correspondence.

Features include the ability to store customer data and interactions, manage staff details and vendors, and store documents.

> Paper-based tasks increase storage, postage, and compliance costs and can be a major overhead for modern-day businesses.

The Risks And Benefits Of A Guest WiFi Connection

> *"The cost of setting up a guest WiFi connection doesn't have to cost an arm and a leg either. Another plus to offering free WiFi to your customers is that it costs almost nothing to supply it."*



Ron Cochran is a Field Service Engineer at Tech Experts.

In today's day and age, everyone wants or needs to be connected to the Internet.

Whether a person is at your place of business for a teeth whitening session or eating their favorite club sandwich, the need to be connected is ever present. Here is where innovative thinking comes into play.

Giving your customers or clients a WiFi connection can increase satisfaction.

It can be aggravating to wait around because the doctor is running late, the repair is taking longer than expected, or any other unexpected inconvenience that eats into their personal time.

However, if they can work, surf the Internet, poke around on Facebook, or catch up on their favorite TV shows, they'll be less likely to track the passage of time or complain about the wait.

By offering your visitors WiFi, you can also gather data about them. If you require customers to sign in via a social media service to access your WiFi, you can get customer information that will allow you to interact with them and promote your business.

Setting up a WiFi connection doesn't mean that the users have access to your company's main network. You can keep all of your business data safe and secure.

First, you'll want a separate router or WAP so that you can isolate their connections from your business network.

While setting up Internet for your customers might seem like a breeze, it's important to be aware of the potential risks.

Sometimes, customers may abuse public WiFi and use it to download inappropriate images or pirated software and media. This will slow down your Internet and network connection.

Fortunately, these issues and concerns can be addressed if you use the right kind of hardware-software combination and you have a knowledgeable IT company set it up for you.

The cost of setting up a guest WiFi connection doesn't have to cost an arm and a leg either. Another plus to offering free WiFi to your customers is that it costs almost nothing to supply it.

You'll want to have an additional router to keep customer WiFi separate from your business Internet to prevent any security issues, but a $50 router will easily allow you to provide customer connectivity and make sure guests don't have access to your company's network.

Depending on customer usage, you may need to increase bandwidth or add a separate Internet account, but you can address that when the need arises.

Now that you're getting ready to offer free WiFi to your customers, you need to consider how much bandwidth you'll need. Bandwidth determines the speed of the Internet, so it is important to have enough of it for customers to be able to browse without frustration.

Offering free WiFi is great, but it means nothing if the connection is too slow to be useful.

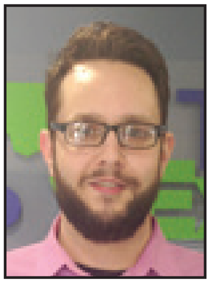
You can also control the speed of their connection which will also keep your Internet connection from becoming slow. I would plan on giving each user 1.5 megabits of speed.

You can also limit usage to a certain radius, restrict the times of day it's available, and limit their time on it to a certain number of minutes before they have to reconnect.

Overall, the thought of offering a WiFi connection at your place of business is an easy, cheap investment to stay up on the changing times. Just remember to keep the client/customer connections separate from your business network, lock down the security, and restrict bandwidth hogging applications - and you'll be right on track.

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

Small Business Cyber Security: How Safe Are You?



Jason Cooley is a Network Technician at Tech Experts.

In 2017, Equifax, one of the largest credit bureaus in the US, suffered a data breach that exposed the names, Social Security numbers, date of birth, and some driver's license numbers for 143 million people.

An additional 209,000 people also had their credit card information exposed.

The attack was discovered on July 29th, but according to Equifax, the breach began sometime in May.

Let that sink in. One of the companies that rates credit scores and stores tons of financial information, had their data stolen for months.

Some would think that the larger the company (especially with sensitive data), the better the security. That isn't always how it works out.

eBay, the online giant, is not immune. In 2014, 145 million user accounts were compromised. The list goes on, and it contains some pretty big names. Target (2013), JP Morgan Chase (2014), The Home Depot, VeriSign, and even Sony's Playstation Network (2011) have all suffered at the hands of hackers.

Don't panic just yet, though. There are many things to consider when it comes to data security. From businesses to your personal data at home, we all obviously want to keep our private information private.

While there is no foolproof way to keep yourself safe, there are some things that you should know.

This isn't a movie

The Hollywood portrayal of hackers is over-the-top for many reasons. Having one person just sitting around and deciding, "Well, I think I will hack the government or this bank," isn't a realistic vision of reality.

Most of these data breaches come due to an unknown security vulnerability. Then groups of people will try to exploit this vulnerability.

There are different needs for everyone

While cyber security can affect everyone, you shouldn't be overly afraid as an everyday consumer.

Most well-known websites are secure and checking out with personal information is often doubled down with extra security.

Still, if you are uncomfortable, use a wallet site, such as Paypal. More and more websites offer these types of payment options, putting down yet another layer of safety to keep your financial information safe.

What about my business?

That greatly depends on what kind of business you have. If you have a convenience store, there's a pretty good chance your credit card processing is the only issue with data you'd have. Since this is typically handled by a vendor, you don't have as much to worry about.

Now, if your company stores any sensitive data (especially the personal information of others), you are going to need to step up the security.

How much do you have to lose?

This isn't a trick question. Really, how much do you have to lose? Financial information? Client information?

As bad as it is to have your data compromised, if you run a business that deals with any sensitive customer or client information, you should not only be careful, but you should be protected.

A managed service provider, like Tech Experts, can help maintain your network and data security. This may include firewalls, blocking specific websites, and running routine checks of the security. Sensitive data, like data that can be used in identity theft, should be protected proactively.

You can't save it once it's been taken.

> *"The Hollywood portrayal of hackers is over-the-top for many reasons. Having one person just sitting around and deciding, "Well, I think I will hack the government or this bank," isn't a realistic vision of reality."*

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

Browsing The Internet In Safety

Evan Schendel is a help desk specialist at Tech Experts.

Browsing the Internet safely comes with many hurdles. Not all of them are obvious, however. These hurdles are numerous and potentially dangerous, but with the proper knowledge and mindfulness, they can be avoided quite easily.

Viruses and Spyware

The Internet is a minefield of harmful applications and criminals trying to take anything they can, but these attempts can be counteracted.

A user must always watch out for suspicious links or websites. Some websites, though legitimate-looking enough, may be spoofed or fake, hiding malicious code or something equally devious.

Hints to these websites being fake can lie in any aspect of the page, but most commonly, it is a slightly different URL or domain name, typically off by only a letter or two. The viruses dwelling in pop-ups usually attempt to scare users into clicking their product and downloading the malware or spyware-stuffed application linked in the pop-up.

Spyware can not only steal information input while loaded onto a system, but also slows the system to a crawl and tends to be easy to pick up. Simply navigating to a poisoned web page or opening a suspicious e-mail can infect a workstation with spyware. The real dangers lie in file-sharing sites, where any file could be dangerous. When downloading any application, evaluate it carefully and make fully sure that not only the site is legitimate, but also that the application is safe too.

Preventative measures do exist, and any workstation should have an anti-virus and anti-spyware application installed and running to prevent most malicious applications from doing any serious damage.

Phishing and Scams

Viruses aren't the only dangers that come with browsing the Internet. Many scams plague the Internet, preying on people uneducated about their existences.

Older scams were typically e-mailed, with scammers posing as relatives or people who could offer the victim a large sum of money, but only if they helped them out with a fraction of what they claimed they could pay the victim.

While it seems silly that these scams could work, many fall prey to the empathetic connection one might have when speaking a person in apparent need. These scams, while still common, occur less and less while newer and more sophisticated traps are being developed. Phishing attempts also come in a method previously discussed – pop-ups. These can have dangerous-looking warnings, alerting you that your machine is infected with a petrifying number of viruses and scaring the user into clicking their links or graphics.

These links or graphics can lead down a dangerous path, including giving the scammers your credit card information. In the event a pop-up like this occurs, do not panic or give in. If it is a pop-up, close the window and make certain you click nothing else on the page. If it is a re-direct to a suspicious page, close that as well, and immediately scan the system for any viruses or spyware just to be safe.

No computer is untouchable, but best practices and well-implemented safety measures can make a computer system much more secure, letting you browse the Internet without fear. In addition to anti-virus programs, constant system updates and application patches can keep any potentially dangerous backdoors or vulnerabilities covered and safe.

With this information kept in mind, falling prey to viruses, spyware, and scams will be far less likely and sites will seem much safer.

Cloud Monitoring