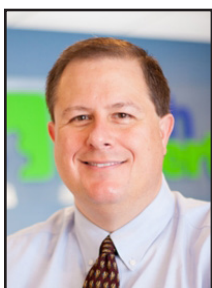


## Small Companies Can Benefit From Redundant Power And Internet



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

As a small business owner, you may not have given much thought to the importance of redundant power and Internet connections.

After all, you have bills to pay, customers to serve, and employees to manage.

However, if you rely on technology to run your business, it's crucial to understand why having backup systems in place is so essential.

As we've seen recently, power outages can happen at any time, and they can have devastating effects on your business. Not only can they interrupt your operations and cause costly downtime, but they can also damage your equipment and lead to data loss.

That's why it's crucial to have a backup power source in place, such as a generator or uninterruptible power supply (UPS).

A generator is an excellent option for businesses that need to keep critical systems running during a power outage. It can provide continuous power for hours, or even days, depending on the size and

capacity of the unit. A UPS, on the other hand, is a device that provides backup power for a short period, usually a few minutes, to allow for a graceful shutdown of your systems.

Regardless of which backup power option you choose, it's essential to test it regularly to ensure it's working correctly. You don't want to wait until a power outage occurs to find out that your backup power system is faulty or not powerful enough to handle your business's needs.

In addition to backup power, having redundant Internet connections is also essential for small businesses that rely heavily on technology. An Internet outage can cause just as much damage as a power outage, especially if your business depends on cloud-based applications or e-commerce transactions.

Redundant Internet connections ensure that your business stays connected to the web even if one connection goes down. This redundancy can be achieved by having two or more Internet service providers (ISPs) or using a load-balancing router that can distribute traffic across multiple connections.

Having redundant Internet connections can not only keep your business up and running during an outage, but it can also improve your overall Internet performance. By distributing traffic across multiple connections, you can reduce the load

on any one connection, which can lead to faster speeds and improved reliability.

As with backup power, it's important to test your redundant Internet connections regularly to ensure they're working correctly. You don't want to wait until a connection goes down to find out that your backup connection is not configured correctly or not fast enough to handle your business's needs.

In conclusion, as a small business owner, you can't afford to overlook the importance of redundant power and Internet connections. They may seem like unnecessary expenses, but they can actually save you money in the long run by preventing costly downtime, data loss, and equipment damage.

Investing in backup power and redundant Internet connections can also improve your business's overall reliability and performance. By having backup systems in place, you can give your customers peace of mind, knowing that your business can continue to serve them even during an outage.

Don't wait until it's too late to implement backup power and redundant Internet connections. Take the time to evaluate your business's needs and invest in the appropriate systems to ensure that your business stays up and running, no matter what challenges come your way.



In addition to backup power, having redundant Internet connections is also essential for small businesses that rely heavily on technology. An Internet outage can cause just as much damage as a power outage, especially if your business depends on cloud-based applications or e-commerce transactions.



*“By default, Chrome opens with a blank page or the Google search page. However, you can customize your homepage to show your favorite websites or a specific webpage.”*

## Make Your Chrome Browser Work Harder For You

Chrome is a popular web browser that many people use for browsing the internet. However, did you know that there are many ways to make your Chrome browser work harder for you? Here are some tips and tricks to help you get the most out of your Chrome experience.

### Use extensions

Chrome has a vast library of extensions that can help you do everything from blocking ads to managing your tabs. You can find extensions for almost anything you need to do, and many of them are free. Some popular extensions include Adblock Plus, LastPass, and Google Translate.

To use an extension, simply download it from the Chrome Web Store and add it to your browser. Once it's installed, you can access it by clicking on the extension icon in the top right corner of your browser.

### Sync your data

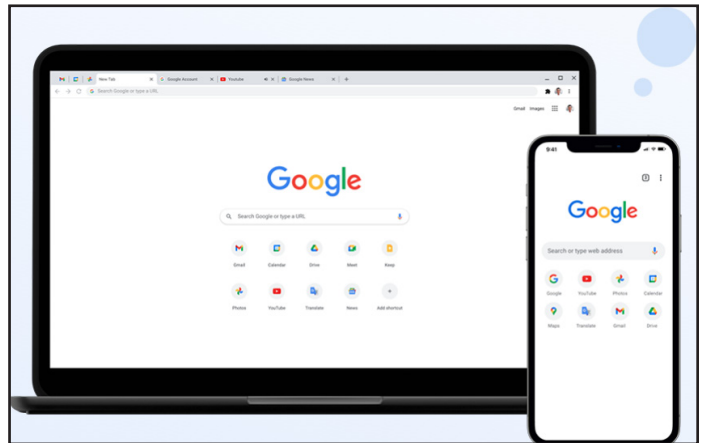
Chrome has a handy feature that allows you to sync your data across multiple devices. This means that you can access your bookmarks, browsing history, and saved passwords from any device with Chrome installed.

To enable syncing, click on the three dots in the top right corner of your browser and select “Settings.” From there, click on “Sync and Google services” and turn on the toggle switch for “Sync.” You'll then need to sign in to your Google account to enable syncing.

### Use keyboard shortcuts

Keyboard shortcuts can save you a lot of time and make your browsing experience more efficient. Some common Chrome shortcuts include:

- Ctrl + T to open a new tab
- Ctrl + W to close the current



tab

- Ctrl + Shift + T to reopen the last closed tab
- Ctrl + Shift + N to open a new incognito window

You can find a full list of Chrome shortcuts by clicking on the three dots in the top right corner of your browser and selecting “More tools” > “Extensions” > “Keyboard shortcuts.”

### Customize your homepage

By default, Chrome opens with a blank page or the Google search page. However, you can customize your homepage to show your favorite websites or a specific webpage.

To set a custom homepage, click on the three dots in the top right corner of your browser and select “Settings.” From there, scroll down to the “On startup” section and select “Open a specific page or set of pages.” Click on “Add a new page” and enter the URL of the page you want to set as your homepage.

### Use the Omnibox

The Omnibox is the search bar at the top of your Chrome browser. It can also be used to enter URLs, search your bookmarks and history, and even perform calculations.

To perform a search in the Omnibox,

simply type your search term and hit enter. To search your history or bookmarks, type “history” or “bookmarks” followed by your search term. To perform a calculation, simply type the equation in the Omnibox.

### Manage your tabs

If you're like most people, you probably have multiple tabs open at once. Chrome has several features that can help you manage your tabs, including:

- Pinning tabs to keep them open and organized: To pin a tab, right-click on the tab and select “Pin.”
- Using tab groups to group related tabs together: To use tab groups, right-click on a tab and select “Add to new group.”
- Muting tabs that are playing audio: To mute a tab, click on the audio icon in the tab.

By using extensions, syncing your data, using keyboard shortcuts, customizing your homepage, using the Omnibox, and managing your tabs, you can improve your browsing experience and become more productive.

Try out these tips and see how they can make your Chrome experience even better.



## Proven Ways To Mitigate The Cost Of A Data Breach

Cybersecurity is an essential aspect of running a business. In today's digital world, it's crucial to have a plan in place to respond to incidents, adopt a zero trust approach to security, and use tools with security AI and automation.

By taking these measures, you can help reduce the cost of a data breach and lower the risk of cyberattacks.

Putting in place an incident response plan is crucial for any organization. In the event of a cyberattack, having a well-planned and executed response can help contain the breach and prevent further damage.

In fact, a practiced incident response plan can greatly reduce the cost of a data breach, by an average of \$2.66 million per incident. It's important to regularly practice and update this plan to ensure that your organization is prepared for any potential cyber threats.

Another effective cybersecurity measure is to adopt a zero trust approach. This means that instead of trusting everything within your network, you should verify everything and everyone.

By adopting a zero trust approach,

you can significantly reduce the cost of a data breach. Organizations that don't deploy zero trust tactics pay about \$1 million more per breach.

It's important to carefully evaluate the access levels of your employees

and respond to cyberattacks. By using these types of tools, you can reduce the cost of a data breach by 65.2%.

If you're feeling overwhelmed by the thought of improving your organization's cybersecurity, working with a trusted IT partner can help.

A trusted IT partner can help you develop a cybersecurity roadmap, implement best practices, and ensure that your organization is protected against cyber threats. They can also provide regular security assessments and help

you stay up-to-date with the latest threats and vulnerabilities.

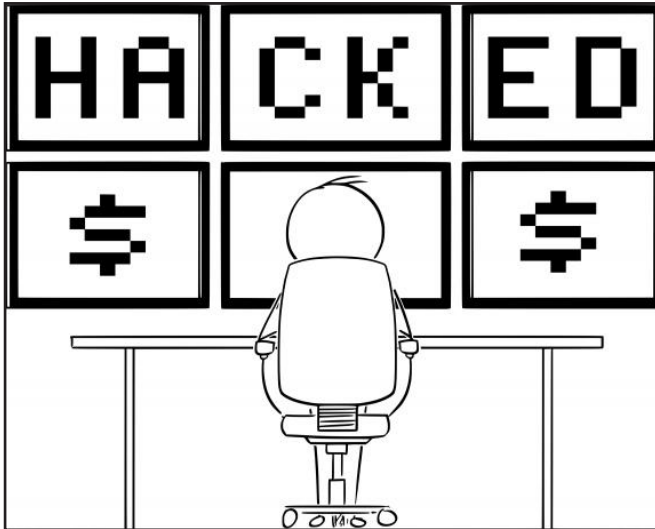
Cybersecurity is a critical aspect of running a business in today's digital world. By putting in place an incident response plan, adopting a zero trust approach, and using tools with security AI and automation, you can greatly reduce the cost of a data breach and lower the risk of cyberattacks.

If you need help improving your organization's cybersecurity, consider working with a trusted IT partner like Tech Experts who can guide you through the process and ensure that your organization is protected against cyber threats.

and partners, and ensure that they only have access to the information and systems they need to do their jobs.

Using tools with security AI and automation is also an effective way to reduce the cost of a data breach. These tools use machine learning and artificial intelligence to detect and respond to cyberattacks. By automating your cybersecurity processes, you can free up your IT team to focus on other tasks while ensuring that your organization is protected against cyber threats.

Advanced Threat Protection (ATP) is an example of a tool that uses security AI and automation to detect



*“Another effective cybersecurity measure is to adopt a zero trust approach. This means that instead of trusting everything within your network, you should verify everything and everyone.”*



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

Need Help? Email [support@MyTechExperts.com](mailto:support@MyTechExperts.com), or call (734) 240-0200



Contact Information

Tech Experts Support Team

(734) 240-0200

support@MyTechExperts.com

Main Office

(734) 457-5000

info@MyTechExperts.com

Sales Inquiries

(888) 457-5001

sales@MyTechExperts.com



TECH EXPERTS

15347 South Dixie Highway

Monroe, MI 48161

Tel (734) 457-5000

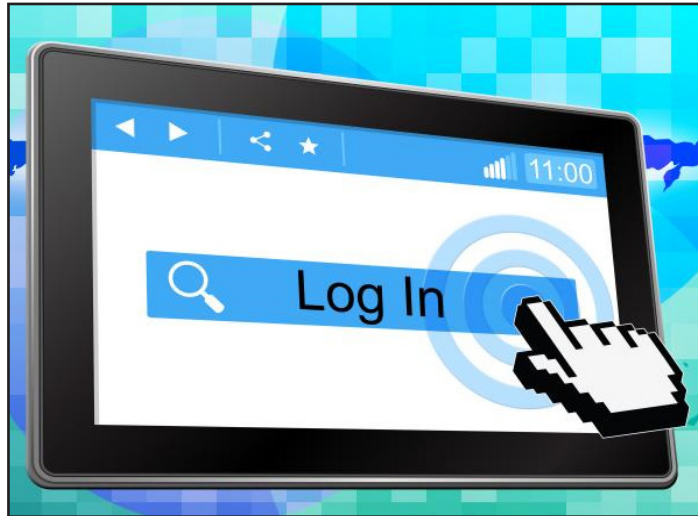
Fax (734) 457-4332

info@MyTechExperts.com

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

## Why Should You Use Different Passwords For Different Accounts?

It's common to have multiple online accounts for social media, online shopping, banking, and more. While having different accounts makes our lives more convenient, it also presents a security risk if we use the same password for all of them.



Instead, use a combination of upper and lowercase letters, numbers, and symbols.

In addition to having different and strong passwords, it's also important to update them regularly.

This is because if a hacker gains

access to one of our accounts, they can potentially gain access to all of them if we use the same password. This is why it's crucial to have different passwords on different accounts.

Having different passwords on different accounts is one of the most basic but important steps you can take to protect your online security.

By using unique passwords, you reduce the risk of a hacker gaining access to all of your accounts if they manage to crack one password. This is particularly important for accounts that contain sensitive information, such as online banking or medical records.

One reason why people tend to use the same password for multiple accounts is because it's easier to remember.

However, there are ways to create strong and unique passwords without having to remember them all. One option is to use a password

manager.

A password manager is a tool that generates and stores unique passwords for each of your accounts. All you have to do is remember one master password to access the password manager. Some popular password managers include BitWarden, Dashlane, and 1Password.

Another way to create strong and unique passwords is to use a passphrase instead of a single word.

A passphrase is a combination of several words that are easy for you to remember, but difficult for others to guess. For example, instead of using the password "password123" you could use a passphrase like "MyDogate2BonesToday!".

It's important to note that having different passwords is not enough to ensure complete security. It's also important to use strong passwords that are difficult to guess or crack.

This means avoiding common words, phrases, or personal information that could be easily guessed.

access to an old password that you no longer use, they can still potentially use it to gain access to other accounts if you've used the same password for multiple accounts. It's recommended to update your passwords every six months to a year.

One thing to keep in mind is that while having different passwords on different accounts is important, it's not the only step you should take to protect your online security. It's also important to enable two-factor authentication whenever possible.

Two-factor authentication adds an extra layer of security by requiring a second form of authentication, such as a code sent to your phone or an app.

While it may seem daunting to remember multiple passwords, password managers can help significantly.

By taking these basic steps, you can greatly reduce the risk of a security breach and protect your sensitive information online.