microTECH Times

Covered I.T. 24/7—Never Worry Again!

How To Avoid The Pinch Of Downtime

While your cousins neighbor or Billy Bob in sales may know a lot about computers, how much time can you really spend bogged down with technology issues before your business looses money? Is your company safe? Consider greater risks like natural disasters, does your answer change?

Can you afford to close the doors of your business for 2 days? Imagine if your network went down due to a virus attack, hardware issues or software problems (all common in a standard year of operations for small businesses in the U.S.). How long would it take to get your company up and running again? Could you recover everything 100%?

Let's put a price on the losses. Quantify how much money you're loosing each year due to minor technology issues. Don't forget to include losses associated with paying employees to work when they really aren't able, missed opportunities to serve your current clients, and potential customer sales lost due to downtime.

IT risks are inevitable, be prepared!
Unfortunately, risk is a part of business; the question is how you handle situations that arise. Will you be a proactive business owner with a plan or will you fix things only when they're broken? Lessen the intensity and pain when downtime

strikes; gather your resources and create a plan so you can take action immediately when the time comes.

Identify risks and create realistic solutions.
Take time to asses risks that can impact your business and create a Business Continuity Plan or roadmap to navigate your company operations during adverse conditions. To get started, take a look at the threats associated with your business like earthquakes, fires, floods, malware attacks, utility outages, or even thefts. While each company has a little different list of threats, all of these risks ultimately have the same negative impact and there are many common recovery options to explore.

Preventative steps and action plans.
After you've identified the risks, take a look at preventative measures and plan solutions to ensure your business will continue even when there is trouble. Preventative measures may include things like off-site backup, flood and fire planning, additional resources for communication if the phone lines are down, secondary computers and/or an alternate worksite.

microenterprises

234 N Broadway Ste 2, Pennsville, NJ 08070

877-540-6789
www.microent.net

What's Inside

Irish Sayings

"May the dreams you hold dearest be those which come true and the kindness you spread keep returning to you."

"Never iron a four-leaf clover. You don't want to press your luck!"

"What do you get when you cross poison ivy with a four-leaf clover? A rash of good luck."

"Don't become broke by trying to look rich."

"May your pockets be heavy and your heart be light. May good luck pursue you each morning and night."

Happy St. Patty's Day

Tuesday, March 17th is St. Patrick's Day. No, you don't have to be Irish to celebrate. Since 1737 this fun holiday has been celebrated in America. Take a look at these fun facts and enjoy the celebrations.

St. Patrick's Day Origins. Did you know the first St. Patrick's Day was actually held in Boston in 1737? Irish settlers sat down for a religious feast to commemorate the death of St. Patrick in the fifth century. They held their dinner on March 17th because this date was confirmed in 1631 by the Vatican as the day of St. Patrick's passing.

St. Patrick's Day in Ireland... If you lived in Ireland between the birth of St. Patrick's day and the 20th century, there really were no St. Patrick's day celebrations. This day holiday really didn't exist. The British presence in Ireland was so strong that a celebration of the nations heritage simply wasn't on the menu. It seemed to be an Irish American celebration

How To Avoid The Pinch...

Prepare an action plan so everyone in your company knows just what to do in an emergency. Create a list of who to call in an emergency: managers, utilities, repair resources, and emergency response groups like your local fire station, police, and EMTs. Be sure to include insurance information too like the carrier name, policy number, and contact information as well as a list of assets with serial numbers to ensure you can claim and report losses as needed.

"Some half of small businesses never reopen after a data Armageddon... Fifty-nine percent of the 130 owners surveyed said they have no disaster plan because they 'haven't thought about it'... yet more than two-thirds (69 %) acknowledged they would lose money if their business were unable to function for a single day."

Real statistics Inc.com reported in a recent article titled, *Why You Should Stop Reading This and Go Get a Data Backup Plan*, results from a study about business owners just like you. Take a look at the excerpt above.

Are you prepared for the unexpected? Even if you are not anticipating a natural disaster, smaller issues like a building fire, flooding from a broken water heater, or a cyber attack can be just as devastating. Planning ahead may mean the difference between recovering gracefully with minimal damages and closing your doors for good.

Ready to get started? If you need a hand evaluating your IT systems to avoid a pinch in an emergency, give us a call. We can help you analyze your current IT structure, identify risks, and set up a plan for preventative measures. We offer ongoing monitoring and support from our knowledgeable IT staff and low fixed monthly contract rates to cover all your IT support needs.

Offload your IT woes to a team of IT experts dedicated to the well being of your business. So you can focus on what really counts, keeping your doors open even in a crisis. Call today for your Network Assessment.

Network Assessment
Micro Enterprises LLC
877-540 -6789

Top 3 Types Of Attacks: A Hackers Pot Of Gold

Just because you're a small business doesn't mean that you're safe from a hack. Small business owners oftentimes think that they have nothing to worry about when it comes to hackers because they feel like they don't have enough information worthy of a hacker stealing. However, it's quite the opposite.

Hackers are more inclined to hack smaller businesses because they know that small business owners think this way. It actually makes it easier for them to get in their systems and take the confidential information they want. Here is a list of the top three types of attacks you should be aware of and share with your coworkers.

1. Phishing and spear phishing attacks are hitting inboxes daily. Be sure to think critically about all messages received before replying, analyze the e-mail header carefully, hover over links before you click to ensure they are legitimate, and call the sender if you're unsure about the message content.

2. Malware attacks are described as an unauthorized software installation. Unfortunately, these are pretty stealth attacks that can attach themselves and replicate quickly within your network. This type of attack is extremely dangerous because they're difficult to detect and remediate.

3. Cloud jacking. Because of the increase in cloud storage usage, there are a handful of vulnerabilities that are now more concerning than ever. Be sure you're using multi-factor authentication whenever possible, change your passwords regularly, and use strong passwords to protect your data. In addition, consider setting up a VPN and encryption to ensure your company stays safe.

Coronavirus Phishing Attacks

Although the Wuhan coronavirus has not caused significant infections in the U.S., it is still being used in e-mail phishing attacks to infect computers. Learn what to look for.
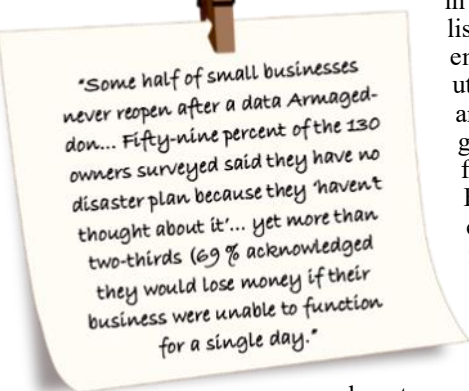
The infected emails contain... links to pdfs or .doc files. The links may appear to come from the CDC or even a coworker, but in fact, redirect users to a page that appears to be Outlook. Or, it can offer 'safety measures' in the form of a pdf. Clicking on any of these links exposes users to malware designed to access bank accounts, financials, and even bitcoin wallets.

Major events or holidays have also been used. Coronavirus was infamously used to invite recipients to a demonstration by global warming activist Greta Thunberg. It has also been used in invitations to Christmas and Halloween parties.

Protect yourself by never opening attachments from an unknown sender unless you confirm over the phone that the attachments are legitimate for your business. Be sure to inform all your staff and coworkers of the dangers Phishing scams pose for your company. Awareness is the best prevention.

Happy St. Patty's Day...

more than it was recognized by Ireland.

Why green? Celebrations today, boast an abundance of beer, namely Guinness, parades, and green everything! Even though, St. Patrick's color was originally blue, wearing green has become quite a staple for the holiday because of Ireland's nick name of being "The Emerald Isle", the green included in the Irish flag, and of course, the color of a shamrock.

Today, over 33 million U.S. residents claim Irish ancestry, according to the U.S. Census. This is quite extraordinary since it is more than seven times the population of Ireland itself. It is our nations most frequently reported nationality next to German. Even though St. Patrick was never really canonized by a pope, he is still one of the most well known saints to which we now turn rivers green, dress to impress, and consume absorbent amounts of beer and beef to celebrate his contributions to Ireland.

Get your green on! St. Patrick's day is one of the most globally celebrated religious holidays with parades, parties, food and festivals on every content, so enjoy!

Maintain Virtual Machines Just Like You Maintain Your Regular Computers

What is a virtual server? I can't even see it, but it always seems to need some work done to keep things running. Why do I need to maintain virtual servers?

What is a virtual server? A virtual server is a server that shares hardware with other like systems and is generally hosted by a third-party resource. Virtual servers are a great way to expand your operations with no equipment costs. However, virtual servers do require the same level of maintenance and attention as a regular server in your office.

Security first! Virtual servers and computers are not a new concept, but are a rising trend for businesses today. Virtualization also allows small and mid-sized companies to take advantage of enterprise security solutions from the third-party vendor hosting their environment. In many ways, this makes your server more secure because it is isolated within a structure of many servers. However, each virtual server is its own separate server.

Updates and maintenance are a must. Virtual or not, updates and maintenance are essential to keep your company information save and retrievable should a problem arise. Virtual servers, much like individual computers, require the same security updates, patches and maintenance. Don't be surprised if your IT provider charges a small fee to maintain your virtual servers. It is possible for virtual servers and computers to be attacked by hackers, just like the physical computers in your office.

Questions about virtualization? Ready to take the leap? Give us a call today for a full assessment to see how to virtualize your operations.

March Madness Rewards Just For You!

It's March Madness and all bets are on! However, betting on the games are always a risk. So, we're offering a "sure thing" for you to line your pockets with a little extra cash.

March Madness... is the most competitive month of basketball games throughout the year. 68 teams come together to compete in 7 rounds of games for the national championship title.

Want a sure thing? While we cannot predict the winning team, we can line your pockets with a little extra cash for game time. We're just asking for the name of one business owner who could benefit from our services.

If you know a fellow business owner who would like a Network Assessment, give us a call today!

Micro Enterprises LLC

877-540 -6789

"We make all of your computer problems go away without adding additional full-time I.T. staff!"

**Ask about our fixed price service agreements — Computer support
at a flat monthly fee you can budget for, just like payroll!**

Inquiring Minds...

5 Unique Tips For Phone Productivity. You can do more business even faster if you tweak your phones applications and organize them more efficiently. Try implementing these five unique tips to help you increase your productivity.

1. Create a better tool box. According to Computer World's contributing editor JR Raphael, the first step is to organize your home screen. Think of it as a tool box. Put the tools you actually need and use every day on the first panel. Everything else goes to other screens.

2. End distractions. If you are prone to mindless web browsing, try Firefox Focus. Focus is meant to be used to look up one thing, not tap, go to Instagram, tap again to Facebook while 30 minutes quickly slip away. According to Better Human, Focus does not keep history, does not remember passwords, and does not keep you logged in. You are in and out in a flash with no extra detours.

3. Limit touches. Notifications are a huge time waster. Most experts recommend turning off notifications for an hour if you need to focus completely on a project. Studies say distractions can mean it takes roughly 20 minutes to get back into a project with full focus. Notifications change your minds direction to race down a trail of information unrelated to your task at hand. Jory MacKay of Meister Task, goes a step further. He says it is not how much you use your phone, the issue is really how much you impulsively touch it. Marketing firm dscout.com says we touch our phones 2,617 times per day. MacKay recommends distance. Carry the phone in your bag, instead of next to your body. Or place it just out of reach and out of sight to give yourself tech free time to be more productive.

4. Save time with a snap. A smaller suggestion, but an incredibly useful one is to remember that your phone takes more than just selfies. Need to talk to tech support about an error message? Use your camera to snap a picture of the error message and e-mail it to tech support. This can save you valuable time when troubleshoot problems. Technicians can view the issue at hand and determine the right person to help you and best course of action before they even get on the phone with you.