

ALERT! RDP Tool Users

Do you use remote desktop tools in your company? Be aware of the recent cyber attacks on RDP tools.

Vulnerabilities.

Attackers are looking for a few key things to take advantage of RDP users:

∅ Weak passwords.

If you haven't updated your passwords this year, Do it today!

∅ Outdated versions of RDP.

Attackers are smart! They search for outdated versions of RDP so they can take advantage of the flaws that haven't been patched. Keep your tools updated regularly.

∅ Restrict the login attempts.

Don't let users have unlimited login attempts. Lock down the account after a few tries so an administrator must verify the login issue before the person obtains access to your systems.



Why Do I Need To Commit To IT Management...

(Continued from page 1)

you will want to make sure that your business is secure. The best way to do this is to have someone specialized in computers help you do it. Outsource your IT to someone with experience so that there is one less thing for you to worry about when it comes to day to day operations.

Benefits of outsourcing your IT solutions. There are many reasons to outsource your IT to someone else. Some of those reasons are:

1. Improved overall security -

Keeps your data more secure when you're accessing it and when it is stored. In addition, it will be available for recovery when you need it most.

2. Faster response times when you need help -

If you have a commitment to an IT provider, then the moment something happens you will have them at your fingertips to tackle the challenge.

3. Lower expenses -

With a regular IT agreement you can balance your budget for IT related services. A cloud solution will also help you avoid replacement and maintenance costs for those expensive servers and network equipment.

4. Lets you focus on what really counts, your business -

Outsourcing your IT and moving to the cloud will allow you to have more time to focus on your business needs and not the safety of your business files.

Eliminate IT security and management from your list of business concerns.

When you have your data in the cloud with proper security in place you won't have to worry about how your daily operations are running. You can push your business to the next level with confidence. Cloud services are a great way to improve your company's flexibility too. Ready for a growth phase this year? Cloud solutions can help you scale up with ease.

If you don't know how to file the taxes for your business you hire an accountant, right?

Why not do the same for your IT management and security needs? Don't patch things together and hope for the best. Hire someone today so you can focus on more important challenges for your business. Call today for a Network Security Audit to see how a managed service provider can help improve your security.

Micro Enterprises LLC
877-540-6789

Communicating Safely: BYOD Policies

These days everyone has a cell phone and everyone uses it for business and personal use. Be sure to set policies in place that promote healthy habits to ensure your network security.

Clarify your BYOD policy. Create and implement a clear policy for your employees when they bring their own devices to work. Make antivirus and anti-spyware programs mandatory, use two-factor authentication when possible, and be sure to set proper expectations with your staff so they understand if a breach occurs, their device may be subject to a full audit (this may include divulging personal and work information).

Implement your BYOD policy.

Nail down the key components for your

BYOD policy which should include things like allowed devices, acceptable use, proper maintenance expectations, and security minimums.

Communicate the importance of the policy and enforce it. Semi-annually, bring the BYOD policy up in your company meetings to review the expectations for your organization. Keep everyone informed of the plan to keep your company data safe.

Security is everyone's job! Your company needs everyone to take the role of a security advocate to keep your data safe. Update, share and track your BYOD policy and devices to keep your organization on track and reduce risks.

Support Your Support Staff

Relationships are all about being supportive for each other. Support your support staff with tools to work more efficiently.

Technology is ever growing and changing. Adapting to all of the changes is important for your business to keep up with your competition. Show your employees how to use technology properly in order to make their work more productive.

Make your data available anytime anywhere. This helps employees get work done more efficiently. When you need collaboration from an employee who is out of the office, make them easier to connect with by implementing a communication software like Google Hangouts, Slack, or Teams.

Clearly define tasks and expectations.

Input on specific projects may mean you need to track each milestone. Take a look at software such as Basecamp, Asana, or Teamwork to assign tasks and share the details of their assignment.

Collaboration tools help you streamline

your operations, improve efficiencies, and ultimately help you deliver more for your clients.

Will You Be Mine...

(Continued from page 1) you're on the right track with your network tools, security and backups... Give us a call. We are ready to love on your network. The Network Security Audit is a road map for us to navigate your business needs and improve your operations. Things like renewing your firewall licensing, closing up vulnerable ports, updating your RDP tools and computers can help tremendously.

Sweet on the lips, heavy on the... pocketbook? No, we won't hit you with some outrageous bill. The audit itself is done in just a few hours and the information we gather is 100% yours to keep regardless of how our courtship goes. As a matter of fact, if you aren't satisfied with our Network Security Audit, just tell us! We are always looking for ways to improve and would love your feedback.

Be our valentine. So, take the leap! Give us a call today to schedule your Network Security Audit and you'll be surprised at the results — maybe we will even get a second date?

Happy Valentine's Day!

Back-up Baby: Because Your Competition Doesn't Care If Your Company Cannot Recover

Data is the most important aspect of your business. Your computer can break very easily or something unforeseen can happen to the files. It's easy to restore your operating system or any programs that you may have had on your computer, but your data isn't recoverable in the event something were to happen to your computer. This is why it is super important to always have a back up of all of your pertinent business data.

It is important to have at least two different backups with one being in a different location so that if one fails you have another option. This way no single event will destroy all of your copies. Storing your data in two different formats such as cloud storage and a hard copy will give you additional options should one become corrupt or compromised. In addition, best practice is to keep one copy offsite just in case there is a natural or physical disaster at your business.

3 common types of backups for businesses. The most common types

of backups for businesses are:

- ∅ Local and Network Backups
- ∅ Cloud Backups
- ∅ Online File Storage

All of these options are great options to use to back up your business data. Just make sure wherever you back up your data, it is done in a secure location so that no one can physically get into your business data. Most cloud backups and online file storage sites are very secure. Do your research to choose one that is right for you and your business.

Backing up your data should be done on a regular basis. Think about how much you add to your company data files each day. Can you easily recreate this information? Back up your data at least weekly, if you work with a high volume of information you should backing up everyday. You can lose a lot of data in just a short period of time if you forget to do this. Let us know if you have any questions about back ups.

What Is The Use Of Random Access Memory?

Random Access Memory (RAM) is the memory used by the central processing unit (CPU) when the computer is running. RAM stores information that needs to be used quickly, but nothing permanent.

What's the use of RAM? RAM is a part of the base structure in your computer and often thought of as the most important aspect. This memory is the core that supports the computers performance and ability to support various types of software. The more RAM your Central Processing Unit (CPU) has access to, the faster your computer will run. RAM is also accessed by the software you use to support the various pieces you're using. If there is not enough RAM available, software may run sluggishly or not at all.

Not so random... RAM really isn't so random. It impacts your computers performance greatly and is one of the most important parts of your machine.



“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...

Lock Down Security With A Password Manager.

A scary-sounding headline in the Washington Post declared: Your password has probably been stolen. Here's what to do about it.

Passwords are a huge risk. As much as we become numb to the latest data breaches, the reality is that it has quite likely affected every one of us in some way. One effective way to combat that threat is to use a password manager, which not only keeps track of all of your passwords and usernames in one spot but also helps you create new, unique -- and complicated -- passwords.

Password strength. First, a word of advice: even if you don't sign up for a password manager, improve your existing passwords. If you're unsure about the strength of your passwords, check SplashData's annual list of the 100 worst passwords of the year. Amazingly, "123456" ranked first YET AGAIN (five years running), followed by "password" at number 2. Mix things up. We recommend using a sentence to create a password. For example, "I have 344 clients in NY!" This sentence would make the password: Ih344ciNY! Which meets all the standard password criteria for a strong password; more than 8 characters, including lower case and capital letters, a number, and a special character.

Ready to learn more about a password manager for your company? Tech website The Verge published an article on how to use a password manager, and listed the three most popular versions as 1Password, LastPass, and Dashlane. Though each is similar, The Verge chose LastPass because it's the cheapest and

is available on most platforms. All of these solutions work on Mac or PC. Most of them even have various access levels you can set so everyone in your company can access the passwords they need for their daily activities.

All you need is one master password to log in and then the manager stores the rest for you, though you do have to import them either via your browser or manually. You can then sync the manager to other devices. Each of the managers also has an audit, which lets you know how secure your passwords are and which ones are weak. And please say that you DO have different passwords and don't simply re-use each one across dozens of sites - right? But how do you know everyone in your company is complying with these basic rules?

These password managers will also help you to change all of your passwords to something you'd never generate on your own. Password managers come with password generators that randomly create strong passwords with whatever criteria you select. This is helpful when you need to update your passwords. Admittedly, the process to update passwords every 6 months can get a little tedious. But in the end, it's far better than dealing with having your data stolen and having to restore your company data back to normal. That can translate into lost revenue, angry clients and a host of additional costs for your company. Secure your passwords today with a reputable password manager.



**PO Box 503
Deepwater, NJ 08023
877-540-6789
www.microent.net**

Sweet Security Solutions!

Worried about security? Concerned your company is falling short on monitoring network activities? Scared one little slip up will cause a catastrophic failure, data loss, or interruptions in your business?

Give us a call today for a **Network Security Audit** and learn about a few sweet security solutions to help secure your company data and maintain a smooth working environment.



We're not asking to move in, just proposing a new way of buttoning up your network to ensure your company data is safe 24/7/365 and recoverable.

Micro Enterprises LLC 877-540-6789