

MTC TECH TALK

*For Humans
Not Geeks!*

Your resource for the latest technology updates and opportunities for your success.

Your Need-To-Know Guide to Cloud Security: 7 Best Practices




What's In This Issue?

Your Monthly
Technology Update

We All Make Mistakes

Make Your Chrome Browser
Work Harder for You

The Difference Between
Backup, Disaster Recovery
and Business Continuity

Meeting Tree Computer
 (845) 237-2117

Cloud computing has dramatically changed how we work. Zoom, Microsoft 365, and Gmail – the wide gamut of collaboration tools that have become part of our daily lives- are all cloud-based applications that many of us can't imagine doing without anymore.

As with everything in life, there are pros and cons when it comes to Cloud solutions. Their ease of use is a definite pro, but security can be challenging.

In the past, most of our IT infrastructure was set up inside the office building and protecting data that resided within our own four walls was comparatively "easy". Cloud infrastructure, however, reaches beyond our immediate control requiring a very different approach to data security.

Luckily, Cloud providers nearly always offer some level of security for their environment, but just like anyone else, they are vulnerable to attacks. Sometimes, even more so. Companies like Microsoft, Amazon, and Google are incredibly high-yield targets for cybercriminals with mad hacking skills. And although their tech teams are prepared and trained to expect the worst, they still need your help to close the backdoors.

This article looks at the most effective ways to protect your data in the Cloud. Some are simple to implement by yourself; others may need a more specific level of expertise.

Multi-Factor Authentication (MFA)

The most obvious way to protect your data is to introduce robust security to your cloud login procedure. That's where MFA comes in. MFA, or Multi-Factor Authentication, is the equivalent of adding an electronic lock to the front door and only giving the keycode to people with the proper ID. This added level of verification protects your accounts from being accessed by people unauthorized to do so.



Encryption

As we all know, ease of storing, sharing, and transferring data is one of the most significant benefits of working in the Cloud. Instead of performing these actions without considering security, try adding encryption to the mix.

With end-to-end encryption, your data gets encoded from the moment it leaves your device until the moment that you use it again. Encryption scrambles information into an unreadable format, stopping cybercriminals from being able to hijack it while in transit. And should your cloud provider suffer a breach, the stolen data will be useless without a decryption key – which only you have access to.

Many cloud services will provide encryption as part of their services. It's best practice to make 100% sure that it's being done, though, instead of simply assuming.

Cloud Security Posture Management

No, this isn't about taking care of your back. Instead, CSPM, or automated threat detection, constantly monitors your services, allowing you to spot and remediate security issues before they become a problem.

It's not generally something that you will be comfortable deploying yourself; however, an expert IT security partner will be able to implement this added level of security for you across all your systems and applications.

Manage Your User Accounts

When considering sensitive data, managing who can access what information is crucial; for example, some team members, especially in IT, may have high-level admin accounts with full access to your entire system, while others may only need access to email to do their job.

The "least privilege" principle refers to the concept that any process, program, or user should only be provided with the bare minimum privileges (access or permissions) needed to perform a function. In most cases, privileges are assigned based on role-based attributes such as the business unit, tasks, or seniority.

Install that Update

As with all applications, cloud applications receive regular

software updates to keep them working optimally and patch any security weaknesses. These patches must be applied immediately to prevent cyber criminals from taking advantage of vulnerable backdoors that allow unwanted access to your network.

So the next time you see a notification saying that an "update" is available, take care of this right away.

You Still Need to Back Up

You have a backup, right?

Just because all or most of your data is in the Cloud doesn't mean you shouldn't be backing it up.

No network is impossible to breach and so your cloud security strategy – and indeed your entire security strategy – should always include offline data backups. This way, if something happens that makes your cloud services unavailable (such as your provider suffering a major disaster of its own), your business won't get caught up in the chaos.

It also means that, in the event of a ransomware attack, you still have all your data to work with. Of course, you still have to worry about where the stolen data could end up, but you can at least continue working.

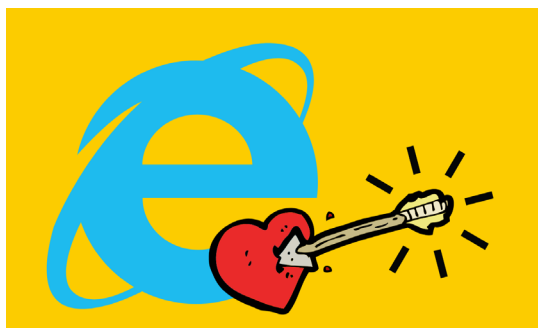
Keep It Simple

Cloud services make things easier for everyone, and your security should feel simple too. Ensure that tools such as 2FA and encryption are easy to use and that your policies and procedures are simple to follow to encourage people to work with them.

There's a lot to talk about when considering cloud security. If you need clarification on what you can do to prevent unwanted hacker interference or downtime, if you find that your cloud services aren't as secure as you'd like, or if you don't know where to start, call on the experts. That's us.

Get in touch today to find out what we can do to help keep your data secure.

Monthly Technology Update



You may have received flowers, chocolates, or heart-shaped gifts on Valentine's Day, but Microsoft delivered an arrow straight through the heart of Internet Explorer: the software giant officially retired the browser last month.

With the latest update to Microsoft Edge, Internet Explorer 11 can no longer be launched on most versions of Windows 10, making the Explorer divorce complete.

Browse on internet explorers!

Make Your Chrome Browser Work Harder for You



Do you use Google Chrome? You can be more productive by using Extensions.

There are thousands of

these small, free, add-on programs available for the world's most-used web browser.

Some just turn your cursor into a pizza slice – because why not? But some have more practical uses that can help you get the most out of your day.

Here are our top picks...

Dualless

If you work on a laptop and miss the benefits of a big desk with dual monitors, this extension could be for you. Dualless allows you to split your browser window in two, so you can view two windows or applications at the same time. You can adjust the respective sizes to suit your needs.

RescueTime

Ever look at the clock and wonder where the day went? RescueTime can tell you. It tracks the time you spend in tabs and windows, and even categorizes them from 'very productive' to 'very distracting'. Are you brave enough for this one?

BlockSite

This is especially helpful if you're trying to stay productive away from the office. BlockSite allows you to create a list of websites you'd like to avoid, either all the time, or just in working hours. And it has a neat insight tool that shows you how you've been using your time.

Unhook

Sometimes you need to watch a YouTube video for research. But how often do its recommendations lead you down a rabbit hole? Unhook removes the recommended sidebar, and stops screen suggestions, comments and the trending tab, so that you only watch what you intended – and no more. You're welcome.

There's more to productivity than Chrome extensions – but small wins all add up. If you need more help and advice with your software choices, get in touch today.

We All Make Mistakes

What's your plan for dealing with someone who causes a cyber security incident?

In nearly all cases, online security breaches are the result of an innocent mistake by a member of your team – usually because they've clicked a link in a scam email which opens the door to a cyber-attack.

Oops.

The attack can become worse if that person is afraid of owning up because they think there will be negative consequences. The delay allows viruses to spread until they do maximum damage.

Oops again.

But if they know what to do the moment they realize what's happened – and your company culture encourages admitting mistakes – you stand the best chance of limiting the damage, or shutting down an attack completely.



That means:

- Your people need to be well trained in cyber security threats
- They must know the procedure when they spot a mistake
- They need to know it's better to report what's happened than hide their mistake

This is how you protect your business and protect your team.



The Difference Between Backup, Disaster Recovery and Business Continuity

If you think "data backup" is synonymous with "disaster recovery" and aren't sure what "business continuity" means, you're not alone: most of the business owners we talk to make the mistake of not knowing the difference, so here is a quick tutorial:

First data backup. This simply means that a copy of your data is being replicated to another device or location. External hard drives, offsite backups, and even USB devices all provide data backup. Data backup is obviously important. However, the more important consideration is whether or not your backup solution provides easy disaster recovery, aka, the ability to recover all your files, software, and functionality quickly, easily, without corruption, and with minimum downtime.

For example, if your server died and you only had file-level backup, it would take a while to get back to work. You would have to replace the server, all software and data would have to be

re-installed, and the whole system would need to be reconfigured with your settings and preferences. This process could take hours or even days – and that's if you have all your software licenses and a clean copy of your data.

Then there's business continuity. Business continuity is your business's ability to continue operating even after a major disaster. For example, if you run an accounting firm and your building burns to the ground, you'd be out of business if all your files were on the server only. However, if you had your network in the cloud, your employees could continue to work from home or some other location, giving your business continuity.

Of course, you need all three at some level. If you want a simple and easy way to get all of this handled, give us a call! We specialize in planning, implementing, and managing this kind of project, so you don't have to.

Do You Currently Have An IT Support Company?



On a scale of one to 10, where 1 is awful and 10 is amazing, what score would you give them? If the answer isn't "absolutely delighted", let's jump on a call.

We're now accepting new clients again. If you'd like to set up a 15-minute exploratory call, go to <https://calendly.com/meetingtreecomputer>

Sometimes a simple 15 conversation can change your life. This might not be that 15 minutes, but it might be great for your business.

Reach out and let us know how we can help.

This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Q&A

My mouse has stopped moving. What do I do?

If your mouse freezes, or the cursor disappears, it can be really tricky to do anything. This is where keyboard shortcuts come to the rescue. Press "ALT" and "F4" together to open the shutdown menu, then restart your device. When it reboots, things should be working correctly.

Should my business upgrade to Windows 11?

In short, yes. It's not urgent but Windows 10 will no longer automatically receive new features and updates. So it's good to make the move sooner than later.

I know I need a password manager, but which is best?

Good question... and there are lots of options. Different businesses have different requirements, so it really all depends on you. We'd be happy to make a recommendation once we understand your needs. Get in touch.

Submit Your Questions Here:
info@meetingtreecomputer.com



Follow Us

