1991 – 2021
30
YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

Single Sign-On: More Secure Than It Sounds ……..……..Page 1

FREE: Business Owner's Guide To IT Support Services And Fees …………………..Page 2

Security Corner: 3 Tips For Secure Gift Giving ………..Page 3

What To Include In A Year-End Technology Review ..………………..…..Page 3

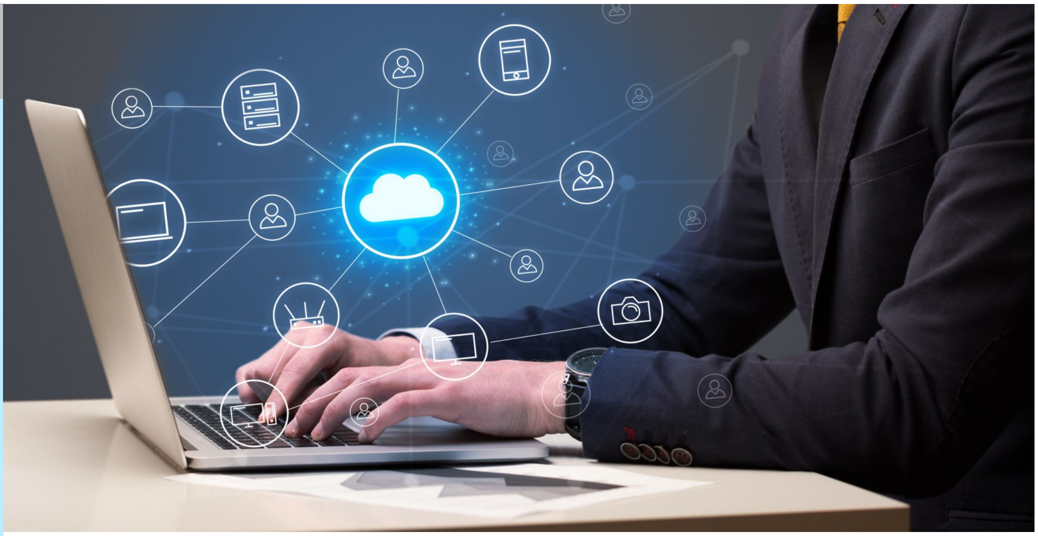
Apps To Improve Customer Experience ……..Page 4

Tips To Avoid PC Buyer's Remorse ……...………………Page 4

December 2022

Kim Nielsen, CISSP
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"



Single Sign-On: More Secure Than It Sounds

With so much advanced cybercriminal technology and the ever-expanding Dark Web, more and more businesses and professionals are turning their focus toward greater online security. These changes are happening all over the world. For example, has your company recently started asking (or requiring) you to participate in phishing exercises or security awareness trainings?

As a result of more people taking action to protect their private online data, there's a rise in the use of password managers, multi-factor authentication, stronger password use or requirements, and much more. One of the ways that you can protect your accounts from hackers is through the use of **single sign-on**.

What Is SSO?

Single sign-on, better known as SSO by users, is an encrypted database that holds the key to your various accounts. You only have to log onto that one main hub, the single sign-on platform, and then you have access to all the associated web based applications. This effectively secures all your accounts by verifying your identity once, and simultaneously makes these various programs much easier to use. This saves a lot of time and, therefore, money if you regularly need the connected applications throughout your workday.

SSO often goes hand-in-hand with multi-factor authentication. The more secured your main hub of data is, the less risk you have of your personal information being compromised or your accounts hacked and used to spread malware to your friends lists. Still sound overly complex? Here's a real world example that you definitely know about: Google. When you log into that one central Google account, you can access your email, Drive,

Continued on pg.2

Continued from pg.1

YouTube and a whole lot more. SSOs are a fast and secure way to easily access a network of interconnected applications without having to sign in to a bunch of different sites. In fact, you might already be using SSO in your personal life already.

Other Advantages of SSO

It's quickly gaining popularity now, but SSO is not a brand-new concept. Before cybersecurity became as much of a priority as efficient workflow, many businesses viewed the practice as one extra barrier to start applications, or a costly hindrance rather than a security tool. However, SSO does more for convenience these days, too.
Consider this: You're the manager of an organization with three different security levels, but everyone uses the same SSO platform. How can you guarantee that lower-level employees aren't accessing files or applications that are either inappropriate or a waste of time for their position?

This is where some research comes in. Different SSO services may integrate with software, or have their own internal features, that let the group's administrator create specific roles and privileges. They can then assign one to every individual, and from a bird's-eye view of the organization, create various permissions and access for all three security levels. All of this creates, not only secure accounts for each employee, but an organization that's better defended against intentional and accidental threats alike.

With threats all around, securing all of your accounts is paramount

Conclusion

Cybercriminals are always looking for ways to hack into accounts, steal log-in credentials, and/or sell your personal identifying information (PII) on the Dark Web. With threats abound, securing all of your accounts is paramount. That means:

- Complex, alphanumerical passwords that differ for every account
- Set up multi-factor authentication with QR codes, fingerprint or face ID, one-time passwords, or another preferred method to confirm your identity before log-in
- Logging out of accounts and shutting down systems when you're done using them
- Secure password managers with encrypted databases to easily autofill log-in fields
- Locking down your workstation whenever you're away, even if it's only a few minutes

Updating your systems and software as new versions become available

These are just some of the moving parts that go into your overarching cybersecurity posture. Keep an ear out for breaking industry news, trends, defenses and threats so that you can recognize and react to breaches as they come. More importantly, you can secure your accounts before hackers even get close.

Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim your FREE copy today at

https://www.cti-mi.com/itbuyersguide1222/

Security Corner

Happy, Healthy Holidays: 3 Tips for Secure Gift-Giving

It's almost the holidays. We know it's on your mind…Just as you're thinking about what to get your spouse, kids or friends, you're also itching for the newest version of your phone, hoping to finally get that tablet you've been asking for, or hinting about some other cool gadget that keeps showing up on TV.

Slow down! You're hankering for cool new technology, and cybercriminals are banking on your excitement overshadowing your common sense.

Did you know? November through January sees and average *70% increase in ransomware attacks*! This is due in part to the holiday season, causing so much flurry that it's easier for cybercriminals to slip under the radar – or for people to be too exhausted to care.

During winter holidays, you're just as likely to *receive* new digital devices as you are to give them. Take care when setting up these gadgets, with these 3 quick tips!

1. Default passwords are easily broken in a brute force or password spraying attack, so change login details IMMEDIATELY
2. Choose lengthy and complex passwords (*Did you know? A recent study by Specops Software found 93% of passwords used in brute force attacks have more than 8 characters!*)
3. Set up security software as recommended by your IT service provider ASAP

For more information about safe holiday shopping, call us at 248-362-3800 or visit: https://bit.ly/3UlwDaJ

What To Include In A Year-End Technology Review

When the year is coming to a close, it's the perfect time to plan for the future. Most businesses begin the year with the hope of growing and improving operations. Much of how a business operates depends on their use of technology.

So, it makes sense to look to your IT for areas of optimization. A year-end technology review provides an opportunity to look at several areas of your IT. The goal is to take time to focus on improvements you can make to boost your bottom line. As well as what tactics to take to reduce the risk of facing a costly cyberattack.

Small businesses that make smart use of technology are well ahead of their peers. Here are some of the ways they excel:

- Earn 2x more revenue per employee
- Experience year-over-year revenue growth nearly 4x as high
- Had an average employee growth rate over 6x as high

The bottom line is that companies that use technology well, do better. They are also more secure. According to IBM, businesses that have an incident response plan reduce the costs of a data breach by 61%. Using security AI and automation can lower costs by as much as 70%.

This year-end, take some time to do a technology review with your IT team or managed IT provider. This will set you up for success and security in the coming year.

Considerations When Reviewing Your Technology at Year-End

The goal of a year-end technology review is to look at all areas of your IT infrastructure, security, efficiency, and bottom-line considerations will be the key drivers for future initiatives.

Technology Policies

When technology policies get outdated, people stop following them. Review all your policies to see if any of them need updating to reflect new conditions. For example, if you now have some staff working from home, make sure your device use policy reflects a work from home policy.

When you update policies, let your employees know. This gives them a refresher course on important information. They may have forgotten certain things since first joining your company.

Disaster Recovery Planning

When is the last time your company did an incident response drill? Is there a list of steps for employees to follow in the case of a natural disaster or cyberattack? Take time to look at disaster recovery planning for the new year. You should also put dates in place for preparedness drills and training in the coming months.

IT Issues & Pain Points

You don't want to go through a big IT upgrade without considering employee pain points. Otherwise, you might miss some golden opportunities to improve staff productivity and wellbeing.

Survey your employees on how they use technology. Ask questions about their favorite and least favorite apps. Ask what struggles they face. Let them tell you how they feel improved technology would make their jobs better. This, in turn, benefits your business. It can also help you target the most impactful improvements.

Privileged Access & Orphaned Accounts

Do an audit of your privileged accounts as part of your year-end review. Over time, permissions can be misappropriated. This leaves your network at a higher risk of a major attack. You should ensure that only those that need them have admin-level permissions. The fewer privileged accounts you have in your business tools, the lower your risk. Compromised privileged account passwords are an open door exposing your business to major damage.

■ Apps To Improve Customer Experience

In today's world, people can order something on their phones and see it on their doorstep the next day. Keeping up with expectations means leveraging the right technology.

As 2023 is on the horizon, it's the perfect time to improve your customer experience. Thanks to cloud technology, you don't have to spend a fortune to do it. Just put in place some of the applications below.

These apps focus on making leads and customers happy.
1. Online Survey Application
2. Smart Chat Bot
3. Business Mobile App
4. Facebook Messenger Support
5. VoIP Phone System with a Good Mobile App
6. Text Notification Apps
7. All-in-One CRM & Sales

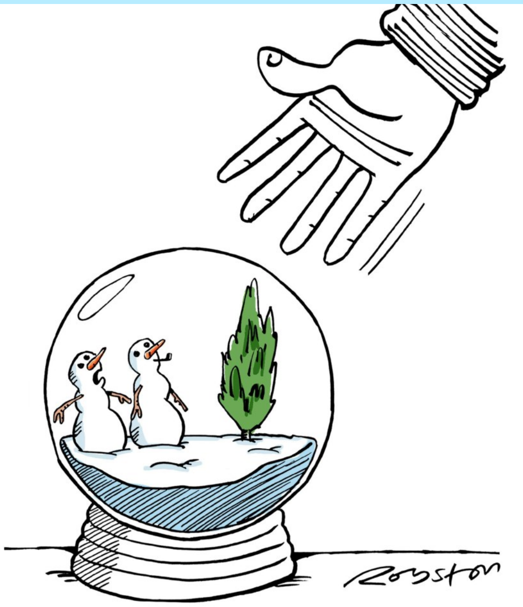
■ Tips To Avoid PC Buyer's Remorse

Have you ever bought a new computer and then had buyer's remorse a few months later? Maybe you didn't pay attention to the storage capacity and ran out of space.

Or you may have glossed over memory and experienced constant freeze-ups.

An investment in a new PC isn't something you want to do lightly. Doing your research ahead of time and consulting with a trusted friend or IT shop can help. It will keep you from making major mistakes that could come back to haunt you later.

Here are several things to consider before you put down your hard-earned money on a new computer.
1. The Amount of Memory (RAM)
2. User Reviews for Longevity
3. Whether the PC is for Personal or Business Use
4. The Processor Used
5. For Laptops: The Case Type
6. Storage Capacity
7. Hard Drive Type



"Looks like we're in for another extreme weather event."

■ Setup Checklist For Microsoft Teams

Microsoft Teams is a lot of things. It's a video conferencing tool, a team messaging channel, and a tool for in-app co-authoring, just to name a few.

During the pandemic, the popularity of Teams skyrocketed. You can think of Teams as a virtual office in the cloud. It's a centralized hub where teams can communicate, collaborate, and manage tasks. There is also an external communication component to Microsoft Teams. You can also use the app to video conference with anyone.

Here are some of the features of MS Teams you might find helpful:

- Set Up Your Teams/ Departments
- Add Team Members
- Set Up Team Channels
- Set Up Team Tabs
- Schedule MS Teams Training