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

March 2024

Kim Nielsen, CISSP, CCSA
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!"

Are You Part of A Culture Of Cybersecurity?

Cybersecurity and cyber-compliance go hand in hand, and they're much more than just buzzwords that you may have heard at work!

Keeping your most private data secure is not only important to your job; it's mandated by law in many industries and important to the people whose *personally identifiable information* (PII) you manage and maintain.

Does your workplace encourage cybersecurity and compliance? By making this a part of company culture, the organization can become a safer place for everyone—and all the data stored on the network!

Why a Culture of Security Matters

A successful cyberattack can lead to data breaches, financial losses, and reputational damage. By following cybersecurity best practices and being vigilant about cybersecurity threats, employees can help to safeguard the company's assets and protect their own personal information.

When you have a good relationship with your coworkers, or even a semi-amicable one, then you probably try to avoid making your daily tasks harder for each other. Collaboration and open communication are key to productive, happy teams. If you demonstrate to coworkers that you place a lot of value in

Continued on pg.2

Continued from pg.1

cybersecurity and compliance, they will be more likely to lean into their own security awareness training, and so on.

Now, you're just one person who doesn't have the power to change everyone's mind overnight! It's important that upper management is also implementing, and enforcing, policies encouraging an everyday culture of cybersecurity and compliance awareness.

Building a Culture of Cybersecurity at Work

So, how can you help contribute to your company culture in a positive way?

- Make sure you're paying attention during your security awareness training and stay up to date on cybersecurity best practices. This can be done through online resources, training programs offered by your employer, or even simply by talking to colleagues who are more knowledgeable about cybersecurity.
- Follow company cybersecurity policies and procedures. This includes things like using strong passwords, being careful about what links they click on, and reporting suspicious activity to the IT department. Don't know how to do something? Just ask!
- Be an advocate for cybersecurity in the workplace! As the saying goes, *"if you see something, say something!"* and this is great advice for any odd behavior you notice in the workplace or on company servers or computers.
- Talk to colleagues about the importance of cybersecurity and suggest improvements to the company's cybersecurity posture when you notice any weaknesses that could be improved upon. Stay abreast of the latest scams and attack methods out there and learn how to avoid falling victim to them!

Cyberattacks can have a devastating impact on businesses of all sizes. That's why it's so critical that every single employee holds themselves, and their colleagues, accountable for staying cyber-secure and cyber-aware.

Conclusion

Do you know where to turn if you recognize a scam? Learn how and where you're meant to report suspicious activity BEFORE you're facing down an active threat. Know how to contact your IT team and supervisors and use strong authentication requirements on all accounts to prevent hackers from digging too deep!

Security Corner

Misinformation Isn't Just Frustrating...It's Dangerous Too!

It happens all the time: A coworker gives you a quick workaround for a long-winded procedure, or friends offer cool new applications to try, or we download new browser extensions based on good reviews from others.

Did you know that in our digital world, misinformation isn't just a social problem…it's a serious cybersecurity threat?! Don't fret; here is your guide to combating cybercriminal misinformation and becoming a better steward of your secure data.

How to Fend Off Misinformation

Cybercriminals are increasingly using misinformation tactics, like spreading false stories or crafting deceptive content, to manipulate users and sneak into secure spaces. That is why it's so crucial that everybody else stays vigilant and informed!

So, what can you do to fight this digital deception?

- **Stay educated.** Know the difference between cybersecurity best practices and misinformation, and be aware of the common scams out there!
- **Be skeptical.** Don't just accept information at face value. Verify, especially when it comes to promoting good information hygiene.
- **Avoid sharing unverified information** and encourage your colleagues to do the same.

With these tips, you'll be ready to spot, question, verify and combat misinformation about cybersecurity… whether it's spread on purpose or not!

For more information about the dangers of misinformation, call us at 248-362-3800 or visit: http://tinyurl.com/5dwjb9bs

Are Your Smart Home Devices Spying On You?

The integration of smart home devices has become synonymous with modern living. They offer convenience, efficiency, and connectivity at our fingertips.

But a recent study has raised concerns about the darker side of these smart gadgets. It suggests that our beloved smart home devices may be spying on us. It's natural these days to invite these devices into your home. Yet there is also the need to scrutinize their various privacy implications.

The Silent Observers in Our Homes
Smart home devices can range from voice-activated assistants to connected cameras and thermostats. They have woven themselves seamlessly into the fabric of our daily lives.

These gadgets promise to make our homes smarter and more responsive to our needs. But a study by consumer advocate group ***Which?*** raises unsettling questions. What is the extent to which they may be eavesdropping on our private moments?

The study examined the data practices of popular smart home devices.

Key Findings from the Study
The study scrutinized several popular smart home devices such as smart TVs, doorbell cameras, and thermostats.

Widespread Data Sharing
A significant number of smart home devices share user data with third-party entities. This data exchange is often unbeknownst to users. It raises concerns about the extent to which companies are sharing our personal data as well as doing so without explicit consent.

Potential for Eavesdropping
Voice-activated devices, like Alexa, are common. Smart speakers and assistants were found to be particularly susceptible to potential eavesdropping. The study revealed some eyebrow raising

information. There were instances where these devices recorded and transmitted unintentional personal audio data.

Security Vulnerabilities
The study also identified security vulnerabilities in certain smart home devices. This highlights the risk of unauthorized access to sensitive information. Inadequate security measures could potentially expose users to cyber threats.

Navigating the Smart Home Landscape Safely
Here are the key steps to navigate the smart home landscape safely.

1. **Optimize Privacy Settings –** Take advantage of privacy settings offered by smart home devices. Many devices allow users to customize privacy preferences.
2. **Regularly Update Firmware –** Ensure that your smart home devices have the latest firmware updates.
3. **Use Strong Passwords –** Put in place strong, unique passwords for each smart home device. Avoid using default passwords.
4. **Regularly Audit Connected Devices –** Periodically review the smart home devices connected to your network. Seeing just how many there are may surprise you. Remove any devices that are no longer in use or that lack adequate security measures. Keep a lean and secure smart home ecosystem to mitigate your risk.

Online Security: Addressing The Dangers of Browser Extensions

Browser extensions have become as common as mobile apps. People tend to download many and use few. These extensions offer users extra functionalities and customization options. While browser extensions enhance the browsing experience, they also pose a danger which can mean significant risks to online security and privacy.

Key Risks Posed by Browser Extensions

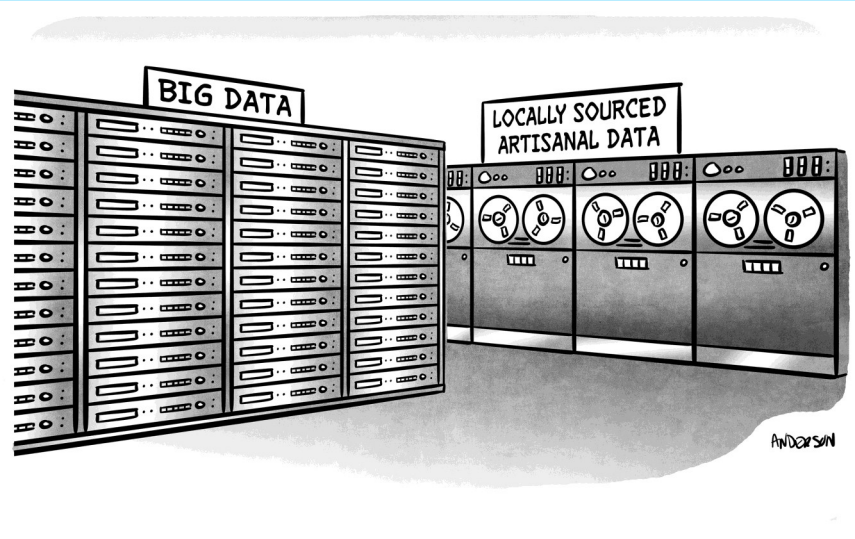
• **Privacy Intrusions** – Many browser extensions request broad permissions. If abused, they can compromise user privacy. Some of these include accessing browsing history and monitoring keystrokes.

• **Malicious Intent** – There are many extensions developed with genuine intentions. But some extensions harbor malicious code. This code can exploit users for financial gain or other malicious purposes.

• **Phishing and Social Engineering** – Some malicious extensions engage in phishing attacks. These attacks can trick users into divulging sensitive information.

Mitigating the Risks: Best Practices for Browser Extension Security

1. Stick to official marketplaces.
2. Review permissions carefully.
3. Keep extensions updated.
4. Limit the number of extensions you install.
5. Use security software.
6. Report Suspicious Extensions.
7. Regularly audit your extensions.



How Small Businesses Are Unlocking Growth With Generative AI

Staying ahead in business often means embracing cutting-edge technologies. New tools can unlock new avenues for growth. Especially for small businesses. SMBs are often looking for affordable and efficient ways to gain a competitive advantage.

One such transformative force is Generative Artificial Intelligence (GenAI). This is a technology that goes beyond automation and the AI we used to know. It can create content, solutions, and unlimited possibilities.

How Are Small Businesses Using GenAI?

• Image & content creation and personalization
• Enhanced customer experience
• Data analysis and decision-making
• Efficient social media management