January 2023

CSU Connection

"Isn't it nice to think that **tomorrow** is a new day with no mistakes in it yet?"
- L.M. Montgomery

Happy 31st Anniversary CSU!

Our Mission

is to deliver outstanding IT support to your business in order to improve uptime, productivity. and profitability. You take care of running your business, We'll take care of your technology.

This monthly publication provided is courtesy of Michelle Sherman, President of Computer Services Unlimited.

Top 10 Business Resolutions

As the New Year beckons, people usually get ready by making a list of things they need to work on based on what they have learned over the past year.

The same thing is true for our business. We should think about what we need to work on and prioritize a list of items. At the top of the list should be cyber-security. By building on what has been learned over the past year, we can get better at defending our business against new threats.

We have come up with a list of ten resolutions that will help you secure your business from cyber threats. Share this list with your fellow employees and you will have created a shield for your business for the new year.

1. Think before you click

Cyber-criminals often use current news, sensational topics, and promises of shocking photos and videos to get you to click on malicious links. Don't fall for it! Stop and think before you click.

2. Change your passwords to pass phrases

In this day and age, attackers can effortlessly gather those pieces of information from social networks and data brokers. They can then put them into their cracking tools to churn out combinations, some of which can actually be your real passwords or pass phrases.

- Make your pass phrases hard to guess – (i.e. I ate5greenworms)
- Give each of your online accounts a unique pass phrase
- Do not use your own information as a pass phrase
- Don't use your name, birthday, address, or even the name of a pet as a pass phrase.

3. Use a password manager

81% of breaches are due to weak or reused passwords. A password manager stores and encrypts your information, allowing you to make unique passwords/phrases for each account. With a password manager you don't have to worry about having to remember multiple passwords/phrases.

4. Protect your privacy

As consumers, we must take resposibility for our own privacy settings.

5. Implement multi-factor authentication when possible

(https://staysafeonline.org/online-safety-privacy-basics/multi-factor-authentication/)

cont. on pg 2

6. Back Up Your Essential Data

Use the 3-2-1 backup rule:

3 -> Create one primary backup and two copies of your data.

2 -> Save your backups to two different types of media.

1 -> Keep at least one backup file offsite.

7. Keep Your Devices Up To Date

Updates and patches often contain the most up-to-date security developments. Don't leave the back door open for cyber criminals

8. Choose security over convenience

When asked to save your credit card information on a shopping website– DON'T. If that company is breached, then your credit card information as well as other vital facts about you will be for sale on the dark web

9. Embrace Cybersecurity Awareness and Training

80% of all ransomeware and data breaches are caused by human error. Simple and effective training can be the best defense.

10. Avoid Oversharing Your Personal Information –

What you share online can give thieves clues to your passwords, your routines and your life!

Monthly Update From Michelle

Have you scheduled any employee cybersecurity awareness training yet for 2023? It's often something that gets put on the back burner. After things like revenue initiatives and software upgrades. Yet, human error is a big driver of cyberattacks.

People don't usually click on phishing links because they want to. They don't purposely make their accounts easy to breach. Many don't know any better. Others know better, but rarely hear management talking about cybersecurity, so they don't feel it's a priority.

One fact that may surprise you is your reduction in risk with well-trained employees. When teams are regularly taught security awareness it can reduce cyber risk by as much as 70%. That's a big difference!

Think about that when looking for ways to improve your bottom line this year. Reducing risk reduces the chance you'll get hit with a costly cyberattack. Train employees regularly and you can reap tangible benefits while building a culture of cybersecurity.

If you need help putting together engaging security awareness training, just let us know. Email me at msherman@csuinc.com to schedule a chat.

Until then, stay safe,

Michelle Sherman

Shiny New Gadget of the Month:

Oura Ring Generation 3

The future of health wrapped around your finger; monitoring your sleep, heart rate, activity, and temperature with personalized insights. Featuring an enhanced sensor package to help you more accurately track and optimize your health.

The finger is the ideal source of accurate heart rate data, more sensitive to movement, and more accurate across all skin tones.

4-7 days of battery life (full charge in 20-80 minutes

ouraring.com

What's Changing in the Cybersecurity Insurance Market?

Cybersecurity insurance is still a pretty new concept for many SMBs. It was initially introduced in the 1990s to provide coverage for large enterprises. It covered things like data processing errors and online media.

Since that time, the policies for this type of liability coverage have changed. Today's cyber insurance policies cover the typical costs of a data breach. Including remediating a malware infection or compromised account.

Cybersecurity insurance policies will cover the costs for things like:

- Recovering compromised data
- Repairing computer systems
- Notifying customers about a data breach
- Providing personal identity monitoring
- IT forensics to investigate the breach
- Legal expenses
- Ransomware payments

What Cybersecurity Attack Trends Should You Watch out for in 2023?

Cybersecurity risks are getting worse. Attacks continue to get more sophisticated. They are also often perpetrated by large criminal organizations. These criminal groups treat these attacks like a business. To protect your business in the coming year, it's important to watch the attack trends. We've pulled out the security crystal ball to tell you what to watch out for.

- **Attacks on 5G Devices**

Hackers are looking to take advantage of the 5G hardware used for routers, mobile devices, and PCs. Any time you have a new technology like this, it's bound to have some code vulnerabilities.

- **One-time Password (OTP) Bypass**

This alarming new trend is designed to get past one of the best forms of account security – Multi-factor authentication.

cont. on pg 4

Some ways this is done include:
- Reusing a token
- Sharing unused tokens
- Leaked token
- Password reset function

- **Attacks Surrounding World Events**

People need to be especially mindful of phishing scams surrounding global crisis events.

- **Smishing & Mobile Device Attacks**

Mobile devices go with us just about everywhere. Look for more mobile device-based attacks, including SMS-based phishing ("smishing").

- **Elevated Phishing Using AI & Machine Learning**

Criminal groups elevate today's phishing using AI and machine learning. Not only will it look identical to a real brand's emails, but it will also come personalized.

7 VOIP Setup Tips For a More Productive Office

Companies that don't set up their VoIP system efficiently, can experience issues. This includes things like dropped calls, low bandwidth, and features left unused.

If you've been struggling to make your cloud phone system more efficient, check out these tips below. They provide setup best practices for VoIP.

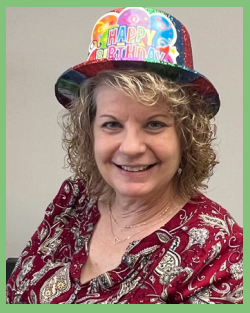
1. Check Network Capabilities
2. Prioritize Your VoIP Software Using QoS Rules
3. Provide Quality Headsets for Your Team
4. Set Up Departments & Ring Groups
5. Create Your Company Directory
6. Have Employees Set Up Their Voicemail & VM to Email
7. Train Your Team on the Call Handling Process

5 Ways to Balance User Productivity with Solid Authentication Protocols

One constant struggle in offices is the balance between productivity and security. If you give users too much freedom in your network, risk increases. But add too many security gates, and productivity can dwindle.

There are ways to have both secure and productive users. It simply takes adopting some solutions that can help. These are tools that improve authentication security. But do it in a way that keeps user convenience in mind.

- Use Contextual Authentication Rules
- Install a Single Sign-on (SSO) Solution
- Recognize Devices
- Use Role-based Authentication
- Consider Adding Biometrics



January is Michelle's Birthday Month! If you gift her with a referral we'll gift you with a $500 Amazon Gift card

The greatest gift anyone can give us is a referral to your friends. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll gift you a **$500 Amazon Gift card**.

Simply introduce me via email at msherman@csuinc.com and I'll take it from there. I personally promise we'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

We Love Referrals!