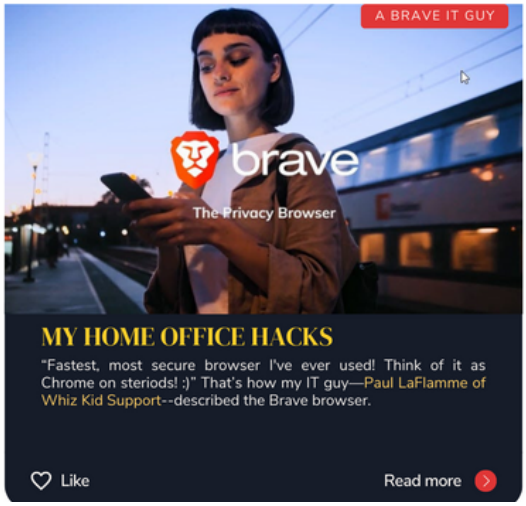
Monthly Newsletter
Volume 12

THE TECH CHRONICLE

March 2024 www.centrend.com Wednesday

WHAT'S INSIDE?



Big Changes to the Tech Chronicle – Get Info Faster!

Hi everyone, we're excited to announce a new format for the Tech Chronicle! From now on, we'll use "Smart Brevity" to deliver the need-to-know tech news and security updates.

Why the Change?

- **Save Time:** We all get too many emails and newsletters. Smart Brevity means shorter articles, so you get the important info without the fluff.
- **Easier to Understand:** Complex tech topics are explained in simple terms.
- **Actionable Info:** We focus on what matters to you so you can make better decisions for your business.

Special Thanks

This change was inspired by **Joe Deramo**, founder of **HighRoad Communications** and **Home Office** Hacks. We want to bring his focus on clear, valuable communication to you.

Subscribe to Home Office Hacks

What to Expect

Same great content, now even more focused on helping you:

- **Stay ahead of cybersecurity threats**
- **Manage your IT more efficiently**
- **Make smarter technology investments**

Our Promise

While the newsletter is shorter, we promise it is every bit as researched and detailed "behind the scenes" so you get accurate information coupled with actionable advice.

Please send us your feedback. We hope you love this new format and the time it saves you, our valued reader.

Don't Fall for It: Tax Season Scam Prevention

Tax season is stressful enough without scammers trying to steal your money or identity. Be on high alert for these common tricks:

This article will discuss the typical strategies used by scammers during tax season, offer prevention advice, and outline what to do in the event that something goes wrong.

- ***Fake IRS threats***

Scammers pretend to be the IRS, demanding payment or personal info. The IRS will contact you by mail first.

- ***Refund theft***

Scammers file a fake tax return in your name to steal your refund. Beat them to it by filing early!

- ***Phishing emails & texts***

These look official, but clicking links can install malware or trick you into giving up your data.

Protect Yourself

- **Hang up, delete, ignore.** Scammers rely on you getting flustered.
- **NEVER share your Social Security number or bank info** unless you made the call using a trusted number.
- **Go to the source.** If unsure, contact the IRS directly at irs.gov or their official phone number.
- **Report scams!** Help protect others by reporting suspicious activity to the IRS (https://www.irs.gov/businesses/small-businesses-self-employed/tax-scams-how-to-report-them).

What If I've Been Scammed?

- **Act fast:** Contact your bank or credit card companies to stop fraudulent charges.
- **Report it:** Notify the IRS about the scam (https://www.irs.gov/businesses/small-businesses-self-employed/tax-scams-how-to-report-them)

Don't let scammers ruin your tax season. Stay informed and stay safe!

Ensuring Business Continuity: The Power of Backup and Disaster Recovery

Problem: Disasters (hardware failures, cyberattacks, etc.) can cripple your business and cost you dearly.

Solution: Business Continuity (BC) planning, with a focus on backup and disaster recovery (DR).

Why BC Matters:

- **Data protection:** Backups are your safety net if anything goes wrong.
- **Quick recovery:** A good DR plan gets you back online fast, limiting losses.
- **Reputation:** Customers trust companies that are prepared for the worst.
- **Saves money long term:** Proactive BC is cheaper than scrambling after a disaster.

Why BC Matters:

- **Assess your risks:** What are the biggest threats to your business?
- **Set goals:** How much downtime is acceptable? How often do you need backups?
- **Choose your backup method:** There are different options (full vs. incremental, etc.).
- **TEST and TRAIN:** Drills make sure your plan works, and your team knows what to do.

Additional Point:

- **Review your BC plan regularly:** At least annually, and after major company changes or industry events.

Call to Action: Don't gamble with your business. Start building your BC plan today!

Hackers are in your texts: Are you ready to fight back?

Problem: Spam texts aren't just annoying, they're a cybersecurity risk.

How Spam Texts Harm You:

- Phishing: Trick you into giving up passwords, bank details, etc.
- Malware: Install malicious software on your device.
- Identity Theft: Steal enough personal info to open accounts in your name.

Protect Yourself:

- Never click suspicious links or open strange attachments. Even if the sender seems familiar, it could be a scam.
- Don't share your phone number publicly. Limit who has access.
- Use your phone's spam filter. Many devices have them built-in.
- Report spam texts. Carriers use reports to block malicious senders.
- Keep your phone updated. Updates often fix security flaws.

Additional Tips:

- Be extra careful with texts about money. Call your bank directly (using their official number) instead of replying.
- Use strong passwords everywhere, and turn on multi-factor authentication. This makes it harder to hack your accounts.

Remember

If a text offer seems too good to be true, it probably is!

Rethinking Endpoint Protection: Go Beyond Windows Defender

Problem: Cyberattacks are increasingly sophisticated; relying solely on basic antivirus like Windows Defender isn't enough.

Solution: Organizations need advanced endpoint protection to secure devices and data against malware, ransomware, zero-day attacks, and more.

Why Beyond Windows Defender?

- **Threats Outpace Basic Protection:** Cybercriminals constantly create new attack methods, outsmarting simple defenses.
- **Windows Defender is Limited:** While useful, it lacks the advanced features and customization of dedicated security solutions.
- **Layered Security is Key:** Combining tools and best practices offers the most robust defense.

Example: Webroot

- **Innovative Approach:** Webroot leverages cloud-based AI for real-time threat detection, focusing on speed and minimal system impact.
- **Features:** Offers protection against malware, phishing, identity theft, and more.
- **Consider:** Explore independent reviews and compare Webroot to other security solutions to ensure it fully matches your needs.

Call to Action: Rethink endpoint protection to safeguard your organization's future. Research and invest in a solution that aligns with your specific security needs.