BURK I.T.

1440 E Shipley Ferry Road
Kingsport, TN 37663

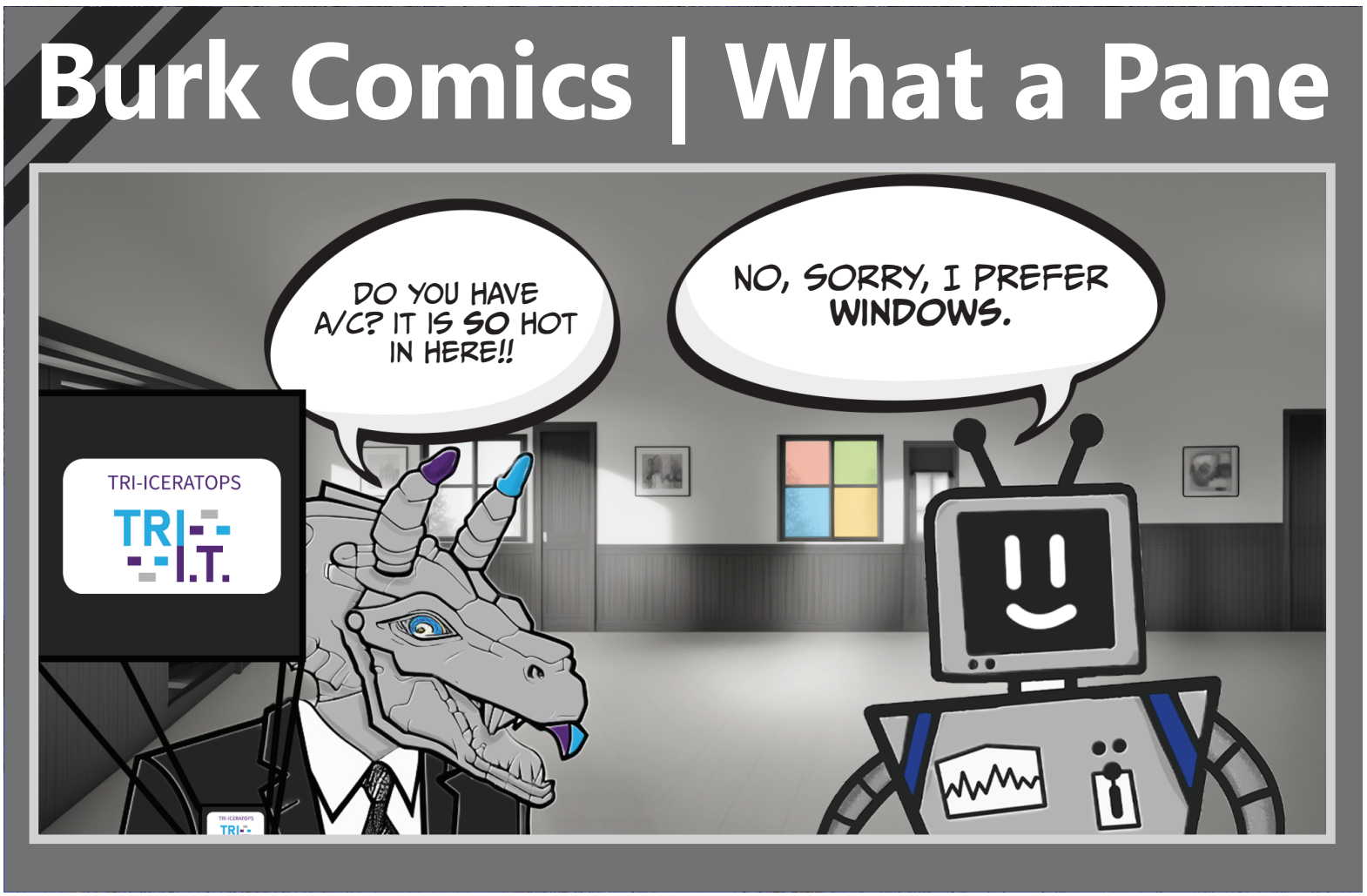
Get the Digital Version!

Check Out the Website!

Follow Our Social Media!

Inside This Issue

Burk Comics | What a Pane



THE BURK Bulletin

September 2023

Our Mission

To create trusted relationships while providing Practical, Secure IT Results

That's the Burk I.T. Way

Cork | What is Cork and How can it Protect Your Business?

Burk IT has partnered with Cork to provide a cyber warranty designed to protect you from financial loss due to cyber-attacks.

- 61% of small businesses were the target of a cyber-attack
- $300,000 is the average cost of a cyber-attack to a small business
- 75% of SMBs say they would not survive past 3-7 days from a ransomware attack

When cyber-attacks strike, your main priority is to get back to business fast. The traditional cyber insurance process is anything but - from lengthy paper forms to long approval timelines, all while your business hangs in the balance. Cork and your MSP are here to bridge the gap with an affordable cyber warranty - no deductible required.

This unique warranty coverage incorporates the validation and monitoring of the client's existing IT security tools, effectively underwriting the warranty coverage using the tools already in place. The monitoring function also allows for the detection and remediation of cybersecurity risks in real-time, preventing the incident before it can become a financial hit to the client.

Even with the best cybersecurity tools deployed, cyber-attacks are still a real threat. When an attack does happens, Cork's cyber warranty covers: Ransomware, Spear Phishing, and Business Email Compromises. Cork's cyber warranty is designed to provide peace of mind knowing you will have the resources you need to weather a cyber storm.

What's New

Burk has a brand new podcast! Featuring Michael Trotter-Lawson, Noah Parker, and Tyler Rasnake, the show has the trio discuss the latest in technology news. Tyler is the technical expert, tackling these stories with his many years of IT engineering experience. Michael and Noah are the laymen, asking the questions that you would ask, while providing a more marketing-centric viewpoint.

Join them every other week to hear unique and insightful commentary into the ever-changing world of technology!

Client Spotlight

Working with Burk IT has been an absolute pleasure. Burk IT pursued us for a year before I finally switched to them. From the very beginning they demonstrated a deep understanding of our unique requirements and challenges. Their expertise and outstanding service sets them apart from the rest. Burk IT seamlessly integrated their solutions into our existing infrastructure and there were no issues as we made the change from our previous IT to Burk IT. Their team's professionalism, prompt response, and willingness to go the extra mile have made them a trusted partner for all our IT needs. Burks ongoing support is invaluable and our staff members are allowed to call and ask questions anytime. They are ready to assist us, addressing our concerns promptly and effectively. Burk IT staff is very friendly and it is obvious that they care about Mountain Region Speech & Hearing and our success.

Karen Dale
Executive Director
Mountain Region Speech & Hearing

Burk Blog | Don't Sabotage Cybersecurity Training With These Mistakes

We live in an era where organizations are increasingly aware of the ever-changing cybersecurity landscape. Despite billions of dollars invested worldwide to fend off cyberthreats, cybercriminals still manage to penetrate even the strongest security defenses.

They relentlessly exploit vulnerabilities with one primary target in mind — employees. Cybercriminals perceive employees as the weakest link in an organization's cybersecurity perimeter. However, you can address and shore up this vulnerability through proper training.

Strengthening employee security awareness is paramount in safeguarding your business. In this blog, we'll look at why employees are prime targets for cybercriminals and explore the critical significance of enhancing their security awareness. By recognizing vulnerabilities, we can proactively mitigate risks and empower your workforce to actively defend against cyberattacks.

Mistakes to avoid

Don't let these preventable mistakes hinder your cybersecurity initiatives:

Approaching security training as a one-off activity

Don't treat cybersecurity training as a mere checkbox exercise. Instead, foster a culture of continuous learning by providing regular opportunities for your employees to stay updated on the latest threats and security best practices. Make security awareness an ongoing journey rather than a one-time event.

Delivering dull, outdated and unrelatable training

Engagement is vital to proper training. Avoid dry and obsolete content that fails to capture your employees' attention. Instead, strive to provide training that is timely, engaging and relatable. Leverage interactive platforms and user-friendly tools to create an immersive learning experience that resonates with your team.

Measuring activity instead of behavior outcomes...