BURK I.T.

1440 E Shipley Ferry Road
Kingsport, TN 37663

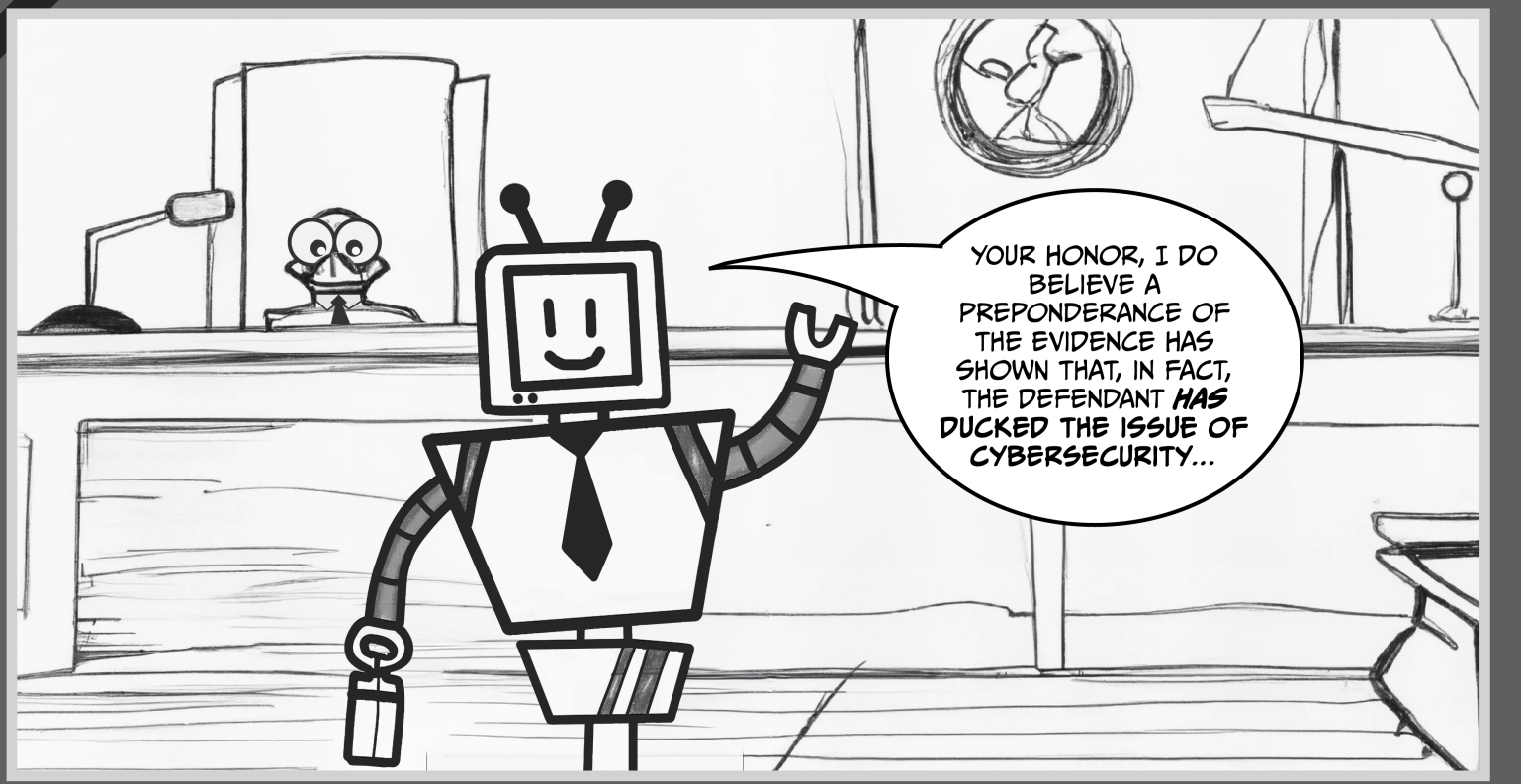
Inside This Issue

Get the Digital Version!

Check Out the Website!

Follow Our Social Media!

Burk Comics | A Fowl Case

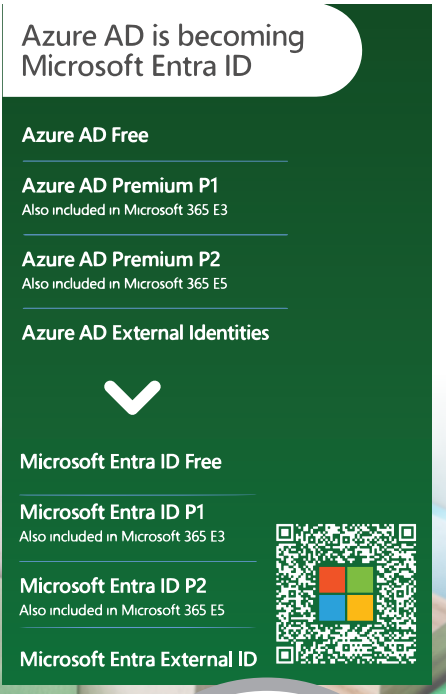


THE BURK Bulletin

Microsoft Azure Active Directory is becoming Microsoft Entra ID

When we (Microsoft) introduced Microsoft Entra in May of 2022, it included three products: Microsoft Azure Active Directory (Azure AD), Microsoft Entra Permissions Management, and Microsoft Entra Verified ID.1 We later expanded the Microsoft Entra family with Microsoft Entra ID Governance and Microsoft Entra Workload ID.3 Today, Microsoft Entra protects any identity and secures access to any resource—on-premises, across clouds, and anywhere in between—with a product family that unifies multicloud identity and network access solutions.

To simplify our product naming and unify our product family, we're changing the name of Azure AD to Microsoft Entra ID. Capabilities and licensing plans, sign-in URLs, and APIs remain unchanged, and all existing deployments, configurations, and integrations will continue to work as before. Starting today, you'll see notifications in the administrator portal, on our websites, in documentation, and in other places where you may interact with Azure AD. We'll complete the name change from Azure AD to Microsoft Entra ID by the end of 2023. **No action is needed from you.**



Client Spotlight

One of the concerns we had when considering switching to Burk I.T. was response time. Our IT function was in house, so the thought of getting IT help from someone two hours away seemed inefficient and inconvenient. But after considering the cost of internal IT and the trouble of finding qualified IT employees, we decided we would give Burk I.T. a chance. The move has worked out better than expected. Before Burk, we often found it difficult to locate our IT guys (two), they may be at lunch, on vacation, or busy traveling between branches. Now, with Burk, a qualified technician is always available. The staff is knowledgeable and can easily correct issues, often times accessing my computer through VPN for a quick resolution. We are very pleased with Burk I.T.

Rob Barger
CEO and President
First Century Bank

MANAGED SERVICES • 423.578.8000 • WWW.BURKITC.COM
BURK I.T.

What's New

Our Team is Growing! Burk I.T. is looking for a new engineer to join our existing customer-centric support desk team. Though I.T. experience is an important factor, this job centers around great customer service, strong communications skills, and a willingness to go the extra mile to ensure the customer is happy. We are looking for candidates with integrity, reliability, flexibility, and a positive attitude!

If you are interested in learning more about the position or know someone else who might be, you can find more details at BurkITC.com/jobs.

August 2023

This monthly publication provided courtesy of Stephenie Griffith and the Sales & Marketing Team at Burk I.T.

Our Mission

To create trusted relationships while providing Practical, Secure IT Results
That's the Burk I.T. Way

Why You Need to Beef Up Employee Security Awareness

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.

The vulnerabilities within

Is your organization dealing with any of the following?

Lack of awareness

One of the key reasons employees fall prey to cybercriminals is their limited knowledge of common cybersecurity threats, techniques, and best practices. Cybercriminals can launch phishing attacks, malware infections, and social engineering ploys by exploiting this knowledge gap among your employees.

Privileged access

Employees often hold privileged access to critical systems, sensitive data, or administrative privileges that cybercriminals crave. By...