OCTOBER 2024

Your monthly newsletter, written for humans not geeks

TECHNOLOGY INSIDER

JOE'S SCARY WAKE-UP CALL...

Meet Joe, a business owner who's seen his company grow impressively over the years.

With a team spread across various locations, Joe invested in a Unified Communication (UC) system to keep everyone connected. Video calls, instant messaging, and shared documents all in one place made collaboration smooth and efficient.

But one morning, as Joe sat at his desk, his worst nightmare began to unfold.

Out of nowhere, video calls started dropping, his team couldn't access important documents, and their VoIP service was on the fritz.

Joe soon realized his business had been hit by a cyber attack. Cyber criminals had breached his UC system, the very tool that had been driving his company's productivity.

The situation escalated fast. The cyber criminals weren't just causing disruption, they were attempting to steal sensitive information. Joe's UC system, which had been a pillar of his business success, had become a target. The efficiency that once fueled his growth was now putting his entire business at risk.

Joe's experience is a cautionary tale for any business embracing modern communication tools. He learned the hard way that protecting your UC environment is critical.

First, Joe realized the importance of choosing the right software, much like picking a high-quality security system for your home. He needed a UC solution that offered strong encryption, access controls to ensure only authorized people could perform certain tasks, and tools to monitor and audit data movement.

And he didn't stop at software. Joe understood that his cloud-based UC systems needed the same level of protection as his physical office. This meant implementing firewalls, secure access methods, and tools to monitor potential threats in real time.

Hardware security also became a priority. Joe began investing in devices with built-in security features to protect his communication systems from future attacks.

Finally, Joe learned that the human element is often the weakest link in security. He made it a priority to train his team on recognizing phishing attempts (where scammers pretend to be someone else), using multi-factor authentication, and practicing strong password management.

Let Joe's story serve as a reminder: Being proactive about ALL your cyber security is essential. Is it something you've already realized? If not, and you need help along the way, we're here to guide you. Get in touch.

DID YOU KNOW...

Google and Microsoft use more power than some countries?

In 2023, Google and Microsoft each used a whopping 24 TWh of electricity. That's more than entire countries like Iceland and Ghana.

On the bright side, these tech giants are leading the way in renewable energy, with Google aiming for 24/7 carbon-free operations by 2030 and Microsoft striving to be carbon-negative by the same year.

TechFacts

1. The name for robot has dark origins. It comes from the Czech word for “robota,” which translates to forced labor or work. The word was first used to refer to a fictional humanoid, in a 1920 play.

2. Remember the Video Cassette Recorder (VCR)? When production stopped in 2016 the models were compact for their time. But the first-ever VCR was the size of a piano!

3. The original Xbox contained edited sound bites from transmissions from the Apollo missions. If you left the Xbox on the home screen, eventually, you’d hear whispers of conversation that was actual chatter from the Apollo mission.

Technology update

Microsoft Designer is now available across platforms

Microsoft has officially launched Microsoft Designer across its platforms. You can enjoy 15 free daily AI-powered design boosts, with an option to upgrade to 100 boosts per day with a Copilot Pro subscription.

New features include prompt templates for easy design creation, custom sticker and emoji creation, and an upcoming background replacement feature.

INSPIRATIONAL QUOTE OF THE MONTH

"If you don't give up you still have a chance. Giving up is the greatest failure."

Jack Ma, co-founder of Alibaba Group.

Will October's fun tech quiz be a trick or a treat?

1. What "B" is the term for wide bandwidth data transmission, able to transport multiple signals and traffic types?
2. Which company launched the best-selling RAZR phone back in 2004?
3. Which game console released in 2006 pioneered the use of motion controls in its gameplay?
4. Which device was first announced in 2007 with the slogan "This is only the beginning"?
5. What technology, now common in smartphones, was first developed by IBM in 1992 with their Simon Personal Communicator?

The answers are below.

1. Broadband
2. Motorola
3. Nintendo Wii
4. iPhone
5. Touch screen

NEW TO

MICROSOFT

Microsoft 365 Copilot gets new AI-powered features

Microsoft has rolled out new AI-powered features to its 365 Copilot, designed to make you more productive and creative.

One of the standout updates is the integration of Copilot into Word, PowerPoint, and SharePoint. This makes tasks like generating images and editing text faster and easier. For example, you can now quickly adjust the tone of your content in SharePoint or generate visuals directly within Word and PowerPoint.

Could an email signature be a hidden threat to your business?

You're wrapping up a meeting when your phone buzzes with a new email. It's from a key supplier and looks urgent. The message is short, direct, and ends with the familiar email signature you've seen countless times.

Without hesitation, you act on the request, but hours later, you discover that the email wasn't from your supplier at all. The signature that convinced you it was legitimate was a clever forgery. Now you're dealing with the fallout of a security breach that could have been avoided.

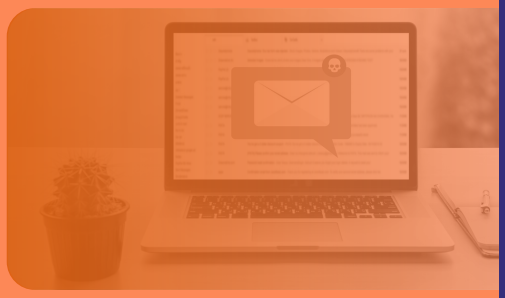
This isn't a far-fetched scenario. It's happening more often than you might think. Email signatures, those blocks of text at the end of every professional email, are being weaponized by cyber criminals.

While you've (hopefully) invested in securing your networks and training your team, the security of your email signature might be the last thing on your mind. But ignoring this small detail can open the door to big risks.

An email signature is more than just a formal way to sign off. It's a digital fingerprint of your business identity. It contains crucial information such as your name, job title, contact details, and often your business's logo and links.

For your clients and colleagues, it's a mark of authenticity. But for cyber criminals, it's a treasure trove of information that can be exploited to deceive and defraud.

What makes email signatures particularly vulnerable is their consistency and familiarity. The more frequently someone sees your signature, the more they associate it with legitimacy. Cyber criminals take advantage



of this by creating emails that appear to come from you or your trusted contacts, complete with a forged signature that looks almost identical to the real thing.

The reality is that many businesses overlook the security of their email signatures. They're often seen as an afterthought, something that's nice to have but not critical to protect. This can be dangerous. Without proper security measures, your email signature can easily be spoofed, making your business – and your clients – vulnerable to attacks.

Understanding the risks is the first step toward protecting your business. For instance, if your email signature includes links, those links can be manipulated to direct recipients to malicious websites. Your title and contact details can be used to create highly authentic looking emails.

To safeguard your business, rethink how you approach email signatures. Start by standardizing the format across your company. When everyone's signature looks the same, it's easier to spot anomalies that could indicate a security threat.

Make sure that the links in your signatures are regularly verified to point to secure, legitimate websites. And, while it might be tempting to include lots of information in your signature, remember that the more data you provide, the more opportunities you're giving cyber criminals to exploit it.

We can help you get your team started - get in touch.

Q: How frequently should we perform backups?

A: Ideally, constantly to make sure your data is fully protected and can be quickly restored if needed.

Q: How should we manage and track our IT assets, like hardware and software licenses?

A: Use an IT asset management (ITAM) system to track all hardware, software licenses, and related information. We can help with this.

Q: What steps should we take to ensure our cloud services are secure?

A: Use strong access controls, encryption for all data, and regularly update all software. You can also monitor for suspicious activity. Get in touch for help.

Business gadget of the month

Tounee telescopic laptop stand

You know that working on a laptop can be more convenient than a desktop PC.

But what's not ideal is the position you must work in.

Enter the Tounee telescopic laptop stand. It adjusts to exactly the right height and angle that means no more aches and pains.

And even rises high enough that you can stand to work rather than sitting down all day. When you're not using it, fold it away.

$50.00 from Amazon.

This is how you can get in touch with us:

CALL: 408-559-2800 | **EMAIL** info@trutechnical.com
WEBSITE: www.trutechnical.com

TRU Technical Partners
IT SUPPORT & CYBERSECURITY