

DID YOU KNOW?

The #1 threat to your security is...

YOU! And your employees. Like it or not, human beings are our own worst enemies online, inviting hackers, viruses, data breaches, data loss, etc., through the seemingly innocent actions taken every day online. In most cases, this is done without malicious intent – but if you as a manager or owner aren't monitoring what websites your employees are visiting, what files they're sending and receiving, and even what they're posting in company e-mail, you could be opening yourself up to a world of hurt.

That's because employees' actions can subject the company they work for to monetary loss, civil lawsuits, data theft and even criminal charges if they involve disclosure of confidential company information, transmission of pornography or exposure to malicious code.

One thing you can (and should) do is configure your firewall to document and monitor which websites users are visiting. Almost all enterprise-level firewalls have this ability built in; you simply need to configure it and monitor the reports (something we can certainly help you with). But it's up to you to set the rules, write it into an Acceptable Use Policy (AUP), TRAIN employees on what is and isn't acceptable and then get them to sign the AUP.



TRUST IS THE NEW CURRENCY

How Wealthy Are You?

Today, most business transactions – whether buying shampoo or tonight's dinner – are faceless. That's why in our digital world, trust is the new currency. This shift in consumer behavior, sometimes called the "trust economy," is more than the quality of products or services you offer; it's about constructing a bedrock of reliability and transparency so customers choose you over competitors.

"Trust keeps society running. Even the most trivial interactions rely on small acts of trust," the Economist reported. This isn't lost on company leaders either. PwC's 25th Annual Global CEO Survey reported that behind industry conditions, consumer trust is the most important predictor of a company's past and future financial performance.

However, trust is increasingly difficult to earn. Thanks to the recent emergence of AI, frequent mishandling of personal data by companies and relentless cyber-attacks,

customers are more skeptical than ever. As product and service providers, PwC points out that we are constantly evaluated by our customers on whether or not we are "forces for good in society." Make one slipup and that trust is gone, perhaps for good.

How you handle data and use technology to influence your customers' experience will decide your fate in the trust economy. Prioritize the most important drivers of trust – empathy, reliability and integrity – and grow your customer loyalty this year and in the years to come.

Technology's Role In Improving Customer Trust

Our dependence on technology is undeniable, yet this very reliance makes us vulnerable. Computer pioneer Willis Ware once said, "The only computer that's completely secure is a computer no one can use." This statement hits a nerve, especially

continued on page 2...



This monthly publication is provided courtesy of Shan Dholaria,

CTO of PcPlus Networks

OUR MISSION:

"As a business owner, you don't have time to waste on technical and operational issues, plus security is a BIG concern too. That's where we shine! We specialize in helping businesses streamline their IT, avoiding downtime by providing #1 Network Support, best-in-class Managed IT Services & Top-Notch Cyber Security solutions that deliver Guaranteed Uptime, Speed, Security & Compliance."

...continued from cover

for businesses navigating the complexities of digital security. The challenge, then, is to harness technology in a way that boosts, rather than undermines, customer trust.

Be Transparent About Data Usage

Ever been shopping for a new shirt only to have an online ad pop up later for the same shirt? It’s not a coincidence – it’s data. Although customers expect you to collect data, they want a say in it. According to a report by Qonsent, 94% of consumers feel that having control over the data they share with companies is important.

Make sure you have a clear privacy policy that tells customers:

- What data you collect
- How you use it
- Who you share it with
- How they can adjust what data they share with you

Additionally, don’t collect more data than you need, and ensure your team is well-versed in data security, drawing from clear internal processes around data management. Slack’s “Privacy Policy” page is an excellent example of data transparency. It’s written for the consumer (not in legalese), and it clearly explains what data is collected and why, and how users can change their preferences.

Take Cyber Security Seriously

Customers want to know if you have a good reputation for protecting their data and information. According to a 2022 McKinsey survey, 53% of consumers will only engage with a company after checking for a good security track record. Even one breach could mean losing a significant amount of your customer base.

To build trust with your customers, make sure your company’s cyber security strategy includes:

- Multi-factor authentication
- Proactive security software that stops attacks before they happen
- Regular security awareness training for all employees
- Frequent backups (local and remote, ideally)
- A disaster recovery plan to help you respond quickly and with authority, decreasing the risk of losing your customers after an incident

Leverage Technology To Improve Your Customers’ Experience

According to a 2018 report by Deloitte, customers spent 140% more with companies they had a positive experience with. Additionally, companies with positive interactions reduced customer service costs by as much as 33%.

Technology enables businesses to offer personalized, seamless experiences that resonate with customers. Consider how e-commerce platforms use encrypted payment transactions and tailored shopping recommendations to provide secure and helpful interactions. Or CRM systems that act like an assistant who never forgets a face or a conversation, so you can manage customer interactions with greater personalization.

Above all, though, it’s the quality of every interaction you have with customers that builds trust. Whether over the phone, by e-mail or across a store counter, remember that your customer wants to trust you. You just have to deliver.

Embrace Trust And Earn Loyalty

Nearly half (46%) of consumers say they’ll consider another brand if data practices are unclear, according to the McKinsey survey. On the flip side, organizations prioritizing digital trust are more likely to experience a 10% annual boost to their top and bottom lines. Listen to your customers. Prioritize a trust-based approach to your business and digital security, and you’re not just winning trust now, you’re setting up for years of loyal customers.

“I DIDN’T KNOW”

Unfortunately, That Excuse Doesn’t Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It’s coming...

- That day a hacker steals critical data, rendering your office useless...
- That day when your bank account or credit card is compromised...
- Or that day when your customers’ private lives are uprooted...

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life.

The ONLY way to STOP THEM is this:

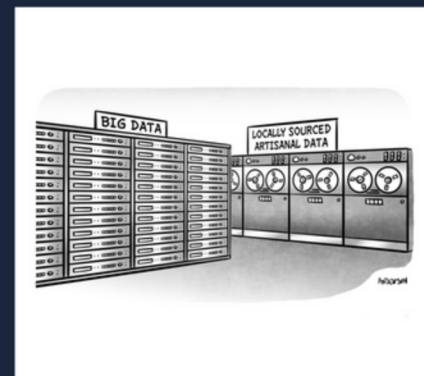
You Must Constantly Educate Yourself On How To Protect What’s Yours!

Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our FREE “Cyber Security Tip of the Week.” We’ll send these byte-sized quick-read tips to your e-mail inbox. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step ahead of the bad guys. And because so few people know about these security secrets, every week you’ll learn something new!

Get your FREE “Cyber Security Tip of the Week” at: www.PcPlusNetworks.com/cybersecuritytips/



CARTOON OF THE MONTH



MIKE ROWE ON THE POWER OF AUTHENTICITY



In today's marketplace, where consumer trust is the linchpin of success, authenticity emerges as a key differentiator for businesses. Who better to break down the power of authenticity than one of the most down-to-earth TV personalities in America – Mike Rowe?

Known for his unscripted, real-life experiences, Rowe has had a career – spanning from his unconventional presentations on QVC to his adventures in Discovery's *Dirty Jobs* – that offers rich lessons on the power of authenticity in life and business.

Balance Authenticity And Authority

In 2001, Rowe worked at San Francisco's KPIX-TV. Eventually, he started a segment called "Somebody's Gotta Do It," where he interviewed tradespeople. Rowe imagined that he, the host, would explain the interviewee's work to the audience. After all, that's how his hosting experience had been so far.

Down in the sewers of San Francisco with Gene Cruz, Rowe began his opening line for the show. Just then, human feces splattered across his face. In response, Cruz said something that later became Rowe's mantra: "Down here in the sewer, it's best to keep your mouth shut." But Rowe kept trying his line – and failing. Between invasive cockroaches and rats, he couldn't get it right. Finally, Rowe gave up and let Cruz do the talking. The show was a massive hit and later became Rowe's foundation for his legendary performance on *Dirty Jobs*.

Instead of talking as the expert, Rowe let the real expert talk. In the city sewers, he realized he had to strike a new balance between expert authority and authenticity in order to connect authority and authenticity in order to connect sincerely with his audience.

"At that moment, I transitioned from – what I would call in cable TV anyway – the age of authority, where all the information came from an expert or a host, into the age of authenticity we're living in today, where the viewer is more skeptical and prefers to get their information by watching a conversation instead of a lecture," he explains.

Somewhere between authority – knowing your business and having all the facts – and genuine authenticity – being completely yourself with no offense (which your audience doesn't want to see anyway) – is where authenticity lives, Rowe says. The key to building a loyal audience is to figure out how to strike that balance.

Authenticity Is More Than Passion

In an early episode of *Dirty Jobs*, Mike plunged into a septic tank alongside Les Swanson. After 15 years as a guidance counselor and psychologist, Swanson had left his career to start a septic-tank-pumping venture near Madison, Wisconsin.

"It was Les Swanson who said to me, 'I'm not here because I'm passionate about septic tanks,'" Mike reflects. "I'm here because I wanted to do something different."

Rowe's journey mirrored a similar path. He'd crawled into sewers and septic tanks, using his skills in conversation to shine a light on others' important work.

"The lesson isn't to not have passion. Passion is important to follow – bring it with you in all things," Rowe says. **"But real job satisfaction comes from finding an opportunity and finding a way to be great at it, and then finding a way to love it."**

SHINY NEW GADGET OF THE MONTH

HP Sprocket Portable Photo Printer

The HP Sprocket Portable Photo Printer is a little gem for photo enthusiasts. This pint-sized printer brings your digital



snaps to life directly from your smartphone. Its Bluetooth connectivity is a breeze, and the ZINK Zero Ink tech means no more splurging on cartridges. What you get are vibrant, smudge-proof 2" x 3" sticky-backed photos, ready to stick anywhere.

But here's the kicker – it's not just a printer. With the HP app, your photos can get a makeover with funky filters and stickers, making each print uniquely yours. Ideal for parties, this gadget lets multiple friends connect and print simultaneously, each with their own LED color cue. Super portable, it's like carrying a photo booth in your pocket. Charge it up, toss it in your bag, and you're set for 35 prints of fun.

IT Security Tip

You need to have step-by-step instructions about what to do if employees believe they have witnessed a cyber-incident. Training needs to happen NOW – not when the problem is happening. A simple training program can be very effective. Things like physically disconnecting the machine from the network (or the power from the machine), notifying PcPlus Networks of any suspicious e-mails or unusual activity and what to do if you lose your mobile device are all parts of a simple yet effective employee cybersecurity plan.

Give us a call and we will help you develop your plan.



1010 Lakes Pkwy
Lawrenceville, GA 30043

INSIDE THIS ISSUE

Trust Is The New Currency –
How Wealthy Are You? P. 1

Get your FREE “Cyber Security Tip
of the Week” P. 2

Mike Rowe On The Power
Of Authenticity P. 3

TRUST

By Hernan Diaz

We'll pause from your regular stream of business book content for an award-winning fiction novel called *Trust*.



Trust by Hernan Diaz is an enthralling Pulitzer Prize-winning novel that masterfully blends genres and timelines. Set against the backdrop of New York's roaring '20s and the Great Depression, it delves into the lives of Benjamin and Helen Rask, a power couple whose fortune is as immense as the mysteries surrounding it. Diaz skillfully weaves a complex narrative that challenges readers to discern fact from fiction, exploring themes of wealth, power and deceit.

This literary puzzle captivates with its deep dive into class, capitalism and the influence of power on reality. Both a gripping tale and an intellectual journey, *Trust* offers a fascinating exploration of personal relationships and societal constructs, making it an exhilarating read.

BIG TECH COMPANY ADMITS IT'S LISTENING TO YOU

We've all suspected our devices are listening to us. How else could the clothing company you just told your sister about over brunch show up as a targeted ad on your Instagram feed? The tech community has largely denied listening without our permission. In fact, in 2017, Facebook had to publicly deny that it listens to its users (that's what they use location services and ad tracking for).

But Cox Media Group (CMG), a multibillion-dollar media empire that owns and operates TV and radio stations worldwide, admitted it's doing just that.

How Are They Doing It?

404 Media gathered published marketing information from CMG and determined that it uses AI to identify conversations via smart devices – collecting information about our spending behaviors, interests and how we spend our time – to deliver ads to us. CMG calls it “Active Listening.” Though any mention of CMG's Active Listening platform has been removed from its website, the archived information is still accessible.

A document published by CMG's VP of digital strategy said, “Yes, our phones are listening to us,” and “CMG has tech capabilities to use to your business advantage.” For example, it claimed to use audio data to create detailed customer profiles, which benefits consumers (fewer irrelevant ads) and businesses (targeted marketing). Still, no one knows *exactly* how they do it, technically speaking. Would it still adhere to safety restrictions imposed by companies like Apple that prevent other companies from listening to its devices? No one knows.

CMG later published a statement saying, “CMG businesses do not listen to any conversations or

access to anything beyond a third-party aggregated, anonymized and fully encrypted data set that can be used for ad placement. We regret any confusion...”

Business Insider states, “It's important to note that it's not clear whether this technology and marketing is actually happening.” Nevertheless, this incident is an important reminder to refresh your privacy settings and pay attention to the real possibilities of companies listening in.

Adjust Your Privacy Settings Now

Although tech leaders like Google and Apple have policies around how and when they listen to you, fake apps and shady companies do not. Any app with access to your microphone could listen to your most private conversations.

Take a moment and really look at the permissions you've given your apps. Ask yourself, does this app really need to listen in? If it's not essential, it's better to revoke that microphone access in your device's settings. Another smart move is to tweak your settings so that an app can only use the microphone while you're actively using it. Finally, never download apps unless you know how, when and why they collect data about you, especially voice data.



Get More Free Tips, Tools And Services at our website: www.PCPlusNetworks.com

(678) 523-5599