www.CDTechnology.com

April 2024

TECHNOLOGY TIMES

Insider Tips to Help Your Business Run Faster, Easier and More Profitably

Thomas Hill, President & Founder

> "Responsiveness. That is what we will be known for. When a business is experiencing down time, every minute counts and they can count on us!"

TRIVIA

CONGRATULATIONS

Kristi DiMaio,

Of Gilded Mirrors, Inc

Who knew that the "S" in "HTTPS" stands for SECURE.

TURN TO PAGE 2 FOR THIS MONTHS TRIVIA

3 CYBERSECURITY MYTHS THAT WILL HURT YOUR BUSINESS THIS YEAR

Working amid the ever-changing currents of technology and cyber security, businesses often find themselves entangled in a web of misinformation and outdated ideas. But failing to distinguish between myth and fact can put your business's security at serious risk.

Based on expert research in the field, including CompTIA's 2024 global State Of Cybersecurity report, we will debunk three common misconceptions that threaten to derail your success in 2024.

Myth 1: My Cyber Security Is Good Enough!

Fact: Modern cyber security is about continuous improvement.

Respondents to CompTIA's survey indicated that one of the most significant challenges to cyber security initiatives today is the belief that "current security is good enough" (39%).

One of the reasons businesses may be misled by the state of their security is the inherent complexity of cyber security. In particular, it's incredibly challenging to track and measure security effectiveness and stay current on trends. Thus, an incomplete understanding of security leads executives to think all is well.

Over 40% of executives express complete satisfaction with their organization's cyber security, according to CompTIA's report. In contrast, only 25% of IT staff and 21% of business staff are satisfied. This could also be accounted for by executives often having more tech freedom for added convenience while frontline staff deal with less visible cyber security details.

continued on pg.2

continued from cover

"Either way, the gap in satisfaction points to a need for improved communication on the topic," CompTIA writes.

Get your IT and business teams together and figure out what risks you face right now and what needs to change. Because cyber security is constantly changing, your security should never be stagnant. "Good enough" is *never* good enough for your business; vigilance and a continuous improvement mindset are the only ways to approach cyber security.

Myth 2: Cyber Security = Keeping Threats Out

Fact: Cyber security protects against threats both inside *and* outside your organization.

One of the most publicized breaches of the last decade was when BBC reported that a Heathrow Airport employee lost a USB stick with sensitive data on it. Although the stick was recovered with no harm done, it still cost Heathrow £120,000 (US$150,000) in fines.

Yes, cyber security is about protection. However, protection extends to both external *and* internal threats such as employee error.

Because security threats are diverse and wide-ranging, there are risks that have little to do with your IT team. For example, how do your employees use social media? "In an era of social engineering, there must be precise guidelines around the content being shared since it could eventually lead to a breach," CompTIA states. Attacks are increasingly focused on human social engineering, like phishing, and criminals bank on your staff making mistakes.

Additionally, managing relationships with third-party vendors and partners often involves some form of data sharing. "The chain of operations is only as strong as its weakest link," CompTIA points out. "When that chain involves outside parties, finding the weakest link requires detailed planning."

Everyone in your organization is responsible for being vigilant and aware of security best practices and safety as it relates to their jobs. Make sure your cyber security strategy puts equal emphasis on internal threats as much as external ones.

Myth 3: IT Handles My Cyber Security

Fact: Cyber security is not solely the responsibility of the IT department.

While IT professionals are crucial in implementing security measures, comprehensive cyber security involves a multidisciplinary approach. It encompasses not only technical aspects but also policy development, employee training, risk management and a deep understanding of the organization's unique security landscape.

Because each department within your organization involves unique risks, people from various roles must be included in security conversations. But many companies are not doing this. CompTIA's report shows that while 40% of respondents say that technical staff is leading those conversations, only 36% indicate that the CEO is participating, and just 25% say that business staff is involved.

"More companies should consider including a wide range of business professionals, from executives to mid-level management to staff positions, in risk management discussions," CompTIA writes. "These individuals are becoming more involved in technology decisions for their departments, and without a proper view into the associated risks, their decisions may have harmful consequences."

Business leaders and employees at all levels must actively engage in cyber security efforts, as they are *all* potential gatekeepers against evolving threats.

Don't Listen To Myths

By embracing a mindset of continuous improvement, recognizing the wide range of threats and understanding the collective responsibility of cyber security, your business will remain safe, resilient and thriving, no matter what the future holds.

> *"Whenever we contact CD Technology, we always get a live person."*
>
> PRECISE INDUSTRIAL COATINGS, INC
>
> -Barry Kober
> Precise Industrial Coating

FREE REPORT:

What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"

Don't Trust Your Company's Critical Data And Operations To Just Anyone!

Download your FREE copy today at https://www.ComputerDepotBusiness.com/7security or call our office at (865) 909-7606.

Check Fraud Crimes Are "Washing" Away Bank Accounts

Headlines are usually flush with the latest digital breaches out to get businesses. Weak passwords, complex social engineering and business e-mail compromise are often the culprits we hear about. But while our eyes and ears were honed in on digital threats, old-fashioned paper-and-pen crimes were sneaking into our bank accounts.

According to the Financial Crimes Enforcement Network, fraudulent-check crimes rose 201.2% between 2018 and 2022. Experts say that the rise of check fraud began in 2020 when criminals started stealing stimulus checks. Once those ended, they needed a new source of income. In 2023, S&P Global noted that check fraud made up one-third of all bank fraud, excluding mortgage fraud. It's a cheap and relatively simple crime happening under our noses, and that's why they're getting away with it.

How Criminals "Wash" Checks

AARP says that most check fraud involves check "washing." This is when criminals use bleach or acetone to wash away the ink used to write the payee and check amount after stealing it from your mailbox or fishing it from a drop box. Once washed, the check dries, is filled out with new information and deposited at banks or cash-checking shops.

According to AARP, a 60-year-old man had a check for $235 stolen and cashed for $9,001.20 – all within 24 hours. It's not just the US either. An Ontario business owner sent a check for $10,800 to the Canada Revenue Agency to make tax payments for his maple syrup company. Days later, it had been stolen and deposited into another account.

It's a low-budget, fast-cash reward for criminals. Even worse, some banks have deadlines for reporting this kind of crime and won't reimburse you if you alert them too late.

6 Tips To Prevent Check Fraud

Thankfully, there are a few simple steps you can take to significantly reduce your risk of check fraud.

1. Pay Online: Pay bills online using a private Wi-Fi connection and a secure portal, like through your bank or vendor website.

2. Mail Safely: Use the post office for mailing checks; avoid leaving them in personal or outdoor mailboxes.

3. Use Gel Ink: Use non-erasable gel ink in blue or black for writing checks; these are harder to erase than ballpoint pen ink.

4. Collect Mail Daily: Pick up your mail daily. If away, arrange for collection.

5. Monitor Your Accounts: Regularly check your bank account online – a few times a week is best.

6. Report Incidents Immediately: Report fraud quickly to your bank and Postal Inspection Service. Most institutions are required to reimburse stolen funds if the theft is reported within 30 days.

It might be a digital world, but criminals will use every tactic to get hold of your hard-earned cash. Add these simple tips to your routine to significantly reduce your risk of check fraud.

CONTACT US WITH YOUR SPECIFIC TECHNOLOGY SERVICE NEEDS

CD TECHNOLOGY

Call (865) 909-7606
To schedule a FREE
10 minute discovery call

Ask About These:

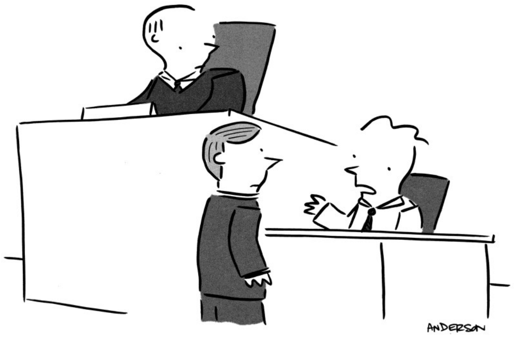
- Flat Rate IT Support
- 24/7x365 Network Monitoring
- Secure Email Access from any web browser
- Anti-Virus, Anti Spam Spyware Protection
- Small Business Phone Systems
- HIPAA Compliance Service
- Data Back-Up Service
- 24x7 Help Desk
- Online Training
- Encrypted VPN Solutions
- Office 365

We are Partners with:

- Lenovo
- Microsoft Certified
- Sophos
- Intel Technologies
- HIPPA Secure Now
- Seagate Certified
- Xerox Business
- Business Phones

Phone: (865) 909-7606

thill@CDTechnology.com



"I wouldn't call it identity theft, I just self-identify as other people."

Here is your chance to win
Lunch On Us!
This Month's

TRIVIA

What are the April rains expected to bring next month?

Email your answer to
RHill@CDTechnology.com
A winner will be randomly selected from all correct responses.

CD TECHNOLOGY
10721 Chapman Hwy #30
Seymour, TN 37865

PLACE
STAMP

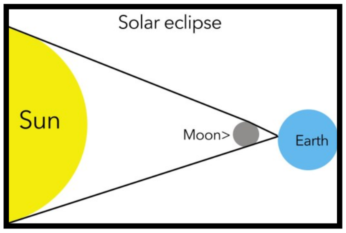
April 2024

INSIDE THIS ISSUE

CD TECHNOLOGY - AFFORDABLE IT HELPDESK AND CYBER SECURITY SUPPORT IN 20 MINUTES OR LESS

Total Solar Eclipse To Be Visible In U.S.

On April 8, American camera buffs and those interested in all things celestial won't have to cross an ocean to experience a total solar eclipse.



A total solar eclipse completely obscures the light of the sun, leaving just a faint visible solar corona.
The 15-mile footprint or path of totality will be most visible in on a path through parts of Texas, Oklahoma, Arkansas, Missouri, Illinois, Indiana, Ohio, Pennsylvania, New York, Vermont, New Hampshire, and Maine. The path will just nick Michigan at the lower southeast corner.

Solar eclipses happen only when the moon passes directly in front of the sun, obscuring it from view.

Those planning to take in this rare spectacle should check with NASA and other online weather sources to ensure the best location. It is necessary to avoid areas of cloud cover and unpredictable weather disturbances.

Without good blocking features on camera and sunglasses, viewers can risk blindness. The eclipse cannot be viewed safely with the naked eye. Eclipse viewing glasses are widely available. We have ours!

Here is a throwback to the last one...

The Hill Family August, 2017

Contact Us

CD TECHNOLOGY

Serving our East Tennessee Neighbors

For over 25 years

5416 S Middlebrook Pike
Knoxville, TN 37921
Phone: (865) 692-4247

or

10721 Chapman Hwy
Seymour, TN 37865

Phone: (865) 577-4775

Email: thill@CDTechnology.com

Visit us on the web at
www.CDTechnology.com