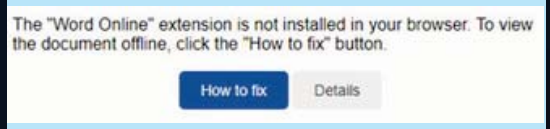
CYBER TIMES

Insider Tips To Make Your Business Run More Securely And More Profitably

CLICK TO FIX HACK

Hackers are now exploiting a social engineering tactic called "ClickFix" to trick users into downloading malware right onto their machine.



These fake alerts appear credible and convince users to bypass security measures, putting your accounts and data at serious risk.

Here's how we can help:

We can help implement enhanced security measures, provide user awareness training, and ensure your team can recognize these increasingly convincing social engineering attacks before they take down your organization.

This monthly publication is provided courtesy of Rick Rusch, CEO of Secure ERP, Inc.

OUR MISSION:

Too many businesses are exposed and vulnerable to cyber attacks. With a unique Guardian Angel Protection solution, our clients get back to their business and sleep better knowing their data is secure.

The perception that SMBs have limited resources, smaller budgets and often a "that won't happen to us" mindset makes them attractive to hackers. Although it's true that SMBs don't have the resources of Fortune 500 companies, you don't need that kind of money to protect your business. Here are six simple strategies hackers hate because they're affordable, surprisingly easy to set up and highly effective.

1 Two-Factor Authentication

The #1 way hackers get access to business accounts is through stolen credentials. Two-factor authentication (2FA) and multifactor authentication (MFA) have existed since the mid-2000s and remain among the best ways to protect your information. 2FA requires things to log in – your passwords and a second factor, like a text message code. If a hacker guesses or steals your password, they still can't get past that second layer of protection. Many platforms, including Google Workspace and Microsoft 365, already offer 2FA for free. Still, it's underutilized by SMBs, with an MFA adoption rate of only 34% or less, compared to 87% among large companies, according to JumpCloud's 2024 IT Trends Report. 2FA is very simple and effective – don't sit this tip out!

2 Updates

Cybercriminals love outdated software because it's full of unpatched vulnerabilities they can capitalize on. Ransomware attacks are notorious for targeting vulnerabilities in operating systems and applications months after security patches are available. Set up automatic updates for your systems, apps and software so you're always running the latest version. Employee awareness

continued on page 2...

...continued from cover

training, regular reminders and even revoking access until patches are installed can help hold employees accountable.

3 Employee Training

Over 90% of data breaches start with phishing e-mails, CISA reports. Designed to look like real e-mails from banks, retail companies or coworkers, they are stuffed with harmful links designed to steal your passwords and data. Cybercriminals bank on naive employees who can't tell real e-mails from fake ones, and AI is making these e-mails even harder to detect. Regular employee awareness training is one of the top defenses against phishing attacks and can reduce phishing risks from 32.5% to 5% in 12 months, according to a recent study by KnowBe4. Research shows that the most effective employee awareness training includes real-world examples, simulated attacks and regular reinforcement through short, interactive training sessions.

4 Data Encryption

The modern world operates on data, and encrypting this data is the most effective method to protect it. In fact, most cybersecurity insurance policies require it. Encryption is like turning your information into code that only authorized people can unlock. Even if hackers intercept your e-mails or customer data, encryption keeps it useless to them. SMBs often hesitate due to costs or complexity, but modern tools like Google Workspace and Microsoft 365 make it simpler and more affordable.

5 Limit Employee Access

Every employee with open access to every folder, file and document significantly increases the risk of accidental (or intentional) changes to your system. Setting up limited access can feel inconvenient initially, but it doesn't have to disrupt employee workflows. An experienced IT team will ensure that employees can run all the applications they need while having access only to what's necessary. For example, a marketing intern doesn't need the ability to access payroll data or network settings. If employees need access to complete specific tasks or projects, consider using a system that grants temporary admin access. Once their project is done, the access goes away.

6 Data Backups

Ransomware is one of the biggest threats facing SMBs today, with 46% having experienced attacks, according to a recent report by OpenText Cybersecurity. Hackers lock up your data and demand payment to get it back, but even payment isn't a guarantee you'll see your data again. Use the 3-2-1 rule – keep three copies of your data on two different types of storage media, with one stored off-site, such as in the cloud or on an external hard drive disconnected from your main network. Just as important: test your backups regularly. Nothing's worse than restoring your data after an attack, only to discover that your backups are incomplete or corrupted.

These simple, cost-effective strategies are a nightmare for hackers and a boon for SMBs looking for more peace of mind. If any of these strategies are missing from your cybersecurity, now is the time to integrate them into your business.

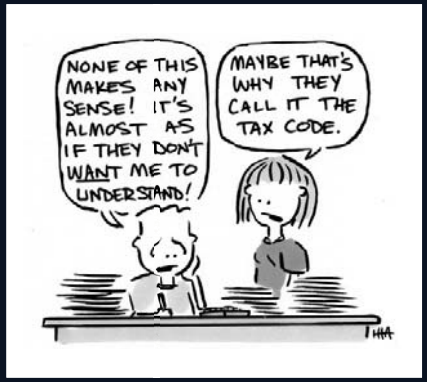
FREE Cyber Insurability Assessment Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our cybersecurity pro will virtually come to your office and conduct a comprehensive review of the same gaps cyber insurance companies are asking about to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To Get Started And Claim Your FREE Assessment Now, Call Our Office At 317-514-8812.

CARTOON OF THE MONTH



ROCKING THE BUSINESS WORLD:

GENE SIMMONS' GUIDE TO ENTREPRENEURSHIP

There's no denying Gene Simmons is a quirky character, even without the makeup. Globally renowned as a rock star in the band Kiss, it's no surprise he showed up to his interview at a recent industry conference clad in all black and wearing dark sunglasses that seemed glued to his face. But behind the moody persona, Simmons is an incredibly successful entrepreneur with a net worth of $400 million. However, it wasn't always this way.

Simmons opened up about his childhood, revealing a depth often masked by his public persona. "The fire in your belly, it never burns hotter than when you can remember what it felt like to be hungry," he explained. Simmons rose from a poverty-stricken childhood in Haifa, Israel, where he sold fruit roadside to survive. The son of a Holocaust survivor, Simmons learned early on that perseverance was nonnegotiable. In fact, he's critical of anyone with a passive work ethic. "There [are] so many opportunities. We're just sitting there going, 'I wish somebody would give me a chance,' and the chances are just going right by you," he said. What differentiates regular people from uber-successful ones, Simmons insisted, is their willingness to fall in love with the labor that success requires. "The most successful people in the world are no different than you are, except they work longer and harder, that's all."

Many Americans aren't taught about taxes or the workings of the economy during their school years, but that's no excuse to let opportunity pass us by. According to Simmons, understanding business is a personal responsibility – or, as he put it, an "inferred fiduciary duty to yourself." This means always looking for knowledge that positions you strategically for success. "Be at the right place, with the right thing and the right time. That's on you," he said.

For any business leader, staying informed and having a continuous improvement mindset is critical to navigating the ever-shifting landscapes of capitalism and economic turbulence. This includes being open to diversification, another of Simmons' strategic business tips. His investments are not siloed in the music industry. Instead, they are spread from restaurant chains to reality TV. This approach cushions financial risks and opens up multiple revenue streams. "It really is because all the knowledge…is available on [the Internet] for free. The rest is just hard work," he pointed out. For Simmons, the secret is simple: tap into the vast online reservoir of information, pair it with relentless effort and keep innovating.

Most people consider business success strategic and tactful, not a particularly creative pursuit. But Simmons argued otherwise. "Business is art. Every step you take is either going to make you money or it's going to cost you money," he said. It's a delicate dance, and Simmons' rising journey from selling fruit in Haifa to building a vast empire exemplifies how determination and smart decision making can turn adversity into opportunity. This underlines a vital truth for all entrepreneurs: success comes from seizing opportunities, continuous learning and unwavering commitment to innovation and excellence.

SECURITY SPOTLIGHT:

FTC SAFEGUARDS

The FTC Safeguards Rule is a regulation established by the Federal Trade Commission that requires defined financial institutions to implement measures to protect the customer's private financial data from disclosure and theft.

This impacts a wide range of companies including mortgage lenders, payday lenders, check cashers, finance companies, mortgage brokers, collection agencies, financial advisors, tax preparers, and auto dealers.

Guardian Angel Protection by Secure ERP, Inc.

TRIVIA

This Hollywood actress is also the co-founder of a technology called "frequency hopping" that laid a key foundation for future communication systems, including GPS, Bluetooth and Wi-Fi.

A. Grace Kelly
B. Veronica Lake
C. Hedy Lamarr
D. Ann Sheridan

Answer: C. Hedy Lamarr. Although she helped develop the ingenious idea with George Antheil in the early 1940s, it was not until 1990 that she received an award for her contribution.

CYBERSIDE CHAT

Fluffy Robot For Your Bag: Cute Or Creepy?

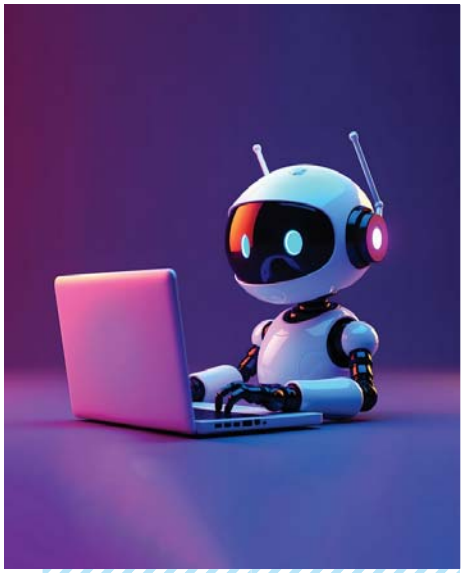
One of CES 2025's quirkiest (creepiest?) reveals was the Mirumi robot – a part-owl, part-sloth companion that clips to your bag and swivels its head to watch others as they stroll by. Created by Yukai Engineering, it's equal parts adorable and unsettling – perfect for sparking conversations or just freaking out strangers on your commute.

Smart Sharing: Location Updates Without Oversharing.

Instead of sharing your location 24/7, choose "Share trip progress" in Google Maps or "Share ETA" in Apple Maps to send updates only when you're on the move. It's a simple, practical way to keep friends or family in the loop and stay safe during late-night rides or busy travel days.

Are You Using AI To Create Charts Yet?

You don't need to be a design expert; you just need to know how to ask the right questions. Try prompting, "What type of chart or visual would work here?" to let AI help you turn data into clear, impactful visuals in seconds.



Fitness Apps Are Tracking More Than Your Heart Rate:

Apps like Fitbit, Strava and Nike Training Club don't just track your workouts – they also sell your data to advertisers. Since around 80% of top apps share your info, it's a good idea to review and limit your sharing permissions to protect your privacy.

INNOVATIVE TECH TRENDS TO EXPLORE IN 2025

Forget smart vacuums — 2025 brings AI-powered communication coaches, advanced collaboration tools and next-level wearable tech to transform business operations.

1. AI Communication Coaches:
These tools provide real-time feedback on tone, body language, and phrasing during video calls, helping professionals improve communication and engagement. Why it matters: They democratize professional development, leveling the playing field for smaller businesses.

2. Advanced Collaboration Tools:
AI-driven meeting summaries, instant translation and integrated team chats streamline remote work. Why it matters: They break language barriers and improve **team efficiency.**

3. Wearable Tech:
Smart glasses, watches and sensor-embedded clothing enhance productivity and safety in industries like logistics and healthcare. Why it matters: Wearables provide instant data, reducing errors and improving response times.

Embrace these innovations to future-proof your business and simplify your life in 2025!