The DIGITAL MINDSET

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLE

Our Mission:

Honor God, Serve People, Protect Businesses

This monthly publication is provided courtesy of Sean Priddy, President of Alexaur Technology.

What's New:

Tax Season is here, which means so are the cyber criminals looking to make a quick buck. Hackers are using tax season to steal W-2s, direct deposit details, and even identities.

2 tips to help keep you safe this tax season:

1) Treat every email like it's a postcard. If you would not write something on a postcard and stick it in the mail (i.e. bank account information or social security numbers), then do not put it in an email, unless of course the email is encrypted.

2) The IRS will NOT email you. If you receive an email from someone claiming to be from the IRS, do not respond to the email or click on any links contained in it.

HACKERS HATE THESE 6 SMB Cybersecurity Tricks (AND WHY THEY WORK)

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 two 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Cybercriminals love outdated software because it's full of unpatched vulnerabilities they can capitalize on.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 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 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.

5 Data Encryption

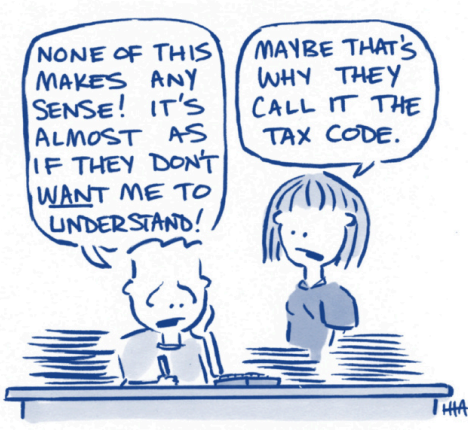
The modern world operates on data, and encrypting this data is the most effective method to protect it. In fact, most cybersecurity insurance policies require it. Encryption is like turning your information into code that only authorized people can unlock. Even if hackers intercept your e-mails or customer 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.

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.

Cartoon of The Month!



Claim Your FREE Microsoft Risk Assessment And Migration Plan.

We'll identify which systems need upgrades and help you transition to remain secure.

Still running Windows 10? Time is running out! After October 14, 2025, no more security updates will leave your systems as a prime target for hackers. Upgrading isn't optional-it's essential. Don't wait for disaster to strike.

Here's why you cannot afford to wait:

- **Your Business Is A Target**
  Cybercriminals are ready to attack businesses still running Windows 10. Don't give them easy access.
- **Compliance Penalties Are Coming**
  Hefty fines are around the corner for businesses using outdated, unsupported software.
- **Downtime Costs You More Than You Think**
  Outdated software drains productivity and money.

Get Started And Claim Your FREE Assessment Now Using This Link:
https://alexaur.com/windows-10-end-of-life/

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 clothed 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.

Ways to Connect With Us

Facebook	LinkedIn	Instagram
@alexaurtech	**@alexaur-technology-services-inc**	**@alexaurtech**