

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.*

THE TRUTH ABOUT CYBERSECURITY

Every Business Leader Should Know.

There are many common myths when it comes to cybersecurity, and unlike harmless stories, these myths can leave you with gaping holes in your company's cybersecurity defenses. Here are five common myths and the truth behind them.

Myth #1 – “It Won’t Happen To Us”

There's a common belief among small and medium-sized businesses that they are too small to be a target for attackers. But this isn't the case; in fact, some cybercriminals target SMBs specifically, with the knowledge that SMBs are less likely to have the resources for reliable cybersecurity.

Cyberattacks happen to organizations of all sizes, in all verticals and geographies, and hit 80% of businesses. The global financial toll? A projected \$9.5 trillion. And while large corporations can take the hit and recover, a single ransomware attack has the potential to put an SMB out of business.

So, regardless of what type of business or organization you have, you must protect yourself from cyberattacks and reduce your exposure. Always assume you are a target – because you are one.

Myth #2 – “If It Worked Then, It’ll Work Now”

It's very common for decision-makers to reason that since they've never been breached in the past, they won't be breached in the future either. However, that belief doesn't account for the rapid pace at which technology – and cybercrime – are evolving.

The threat landscape is constantly changing and there is a very real game of cat-and-mouse at play. If you're not moving forward, you're moving backward. Effective security is a cycle of anticipation, adaptation and action.

What's New:

THE DANGERS OF OUT OF OFFICE AUTOMATIC REPLIES

A simple OOO auto-reply is more than just a courtesy, it's a treasure trove of useful intel for hackers looking to plan a well-timed, highly targeted phishing or business email compromise attack.

Best Practice: Keep the auto-reply generic. Do not include dates of absence, locations, or internal contact names.

Instead of this:

“Hi! I'm out of the office until [date]. For anything urgent, please contact [coworker's name and email].”

Try this:

“I'm currently out of the office. For immediate assistance, please contact our office at [main phone or general email].”

...continued from cover

Myth #3 – “Once Secure, Always Secure”

Unfortunately, technology is fluid – just like your business. Every time you bring on a new staff member and add new devices, your technology’s configuration shifts. As it does, it creates new avenues of attack from cybercriminals.

That’s why continuous monitoring and management are necessary to maintain security integrity. The attack surface stretches beyond common focus areas. Because of this, strong cybersecurity demands a holistic, proactive, continuous approach.

Myth #4 – “Business Optimization Is Hindered By Security”

Many organizations still assume that security initiatives create operational friction – delaying releases, adding red tape and increasing costs. This outdated thinking frames security and business optimization as mutually exclusive, as if improving one compromises the other.

While these perceptions may have roots in the past, they don’t reflect modern practices. Today, security enables optimization. That means minimizing both waste and risk – including security risk.

In the end, secure systems are more resilient, predictable and cost-effective. This makes security a driver of business performance, not a barrier.

Myth #5 – “A Strong Password Is All I Need”

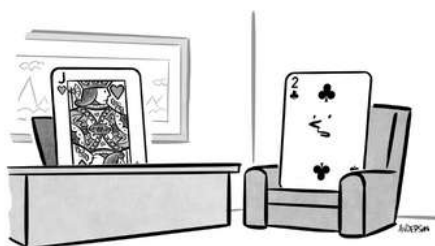
Creating a strong password (at least 16 characters long and a blend of letters, numbers and special characters) for each account is important, but it’s not the only step needed to keep your data secure.

For one, every account and device needs a unique password. If you reuse passwords, it means that if one of your accounts is hacked, all of your other accounts are at risk. To store all your unique passwords, we recommend a password manager!

Enabling MFA for every account will double your protection. The few seconds required to enter a code sent to your phone is well worth the extra security.

That said, there are plenty of other vulnerabilities that savvy hackers can exploit to attack your business’s data. That’s why working with an MSP is a critical component of maintaining your company’s cybersecurity.

Cartoon of The Month!



"Where do I see myself in five years?
Maybe a 5 or 6."

Know Someone Struggling With IT? GET MONEY By Sending Them Our Way!

At Alexaur Technology Services, we believe referrals are the greatest compliment - and they come with **real rewards**.

When you refer a business that becomes a client, we'll thank you with a **CASH REWARD**. It's our way of saying thank you for spreading the word.

You already know the peace of mind that comes with reliable, worry-free IT support. Why not help someone else experience the same- and enjoy a little something in return?

Share the peace of mind. **Get rewarded!**

 alexaur.com/referral-program/

Helping others has never been more worthwhile!

Dr. Phil **PUSHES BUSINESS OWNERS TO "OWN IT" –IN LIFE AND IN BUSINESS**

In a recent interview, Dr. Phil McGraw, celebrity psychologist and talk show host, gave frank advice on what it really means to be in business—and how business owners stay true to themselves while doing it.

Staying True To Passion And Standing Out

"I don't do anything that I'm not a hundred percent passionate about. And I never wanted to be a member of the herd. I didn't want to be a face in the crowd," McGraw said. "I wanted to market my education in a way that set me apart from the rest of the industry. I think you have to do that [in business]."

Define And Articulate Your Differentiator

"You have to know what separates you from everybody else that thinks they do what you do. What do you bring to the table that nobody else does? What do you do that's different than everybody else? If you don't know what your differentiator is, if you can't articulate it and don't market it in an easily perceptible way, then you aren't really in business yet."

You Are Your Own CEO

"I think every one of us is a company of one," said McGraw. "I don't care if you work for the United States post office. Every one of us is a company of one—and you are your own CEO. Then the question becomes: how are you doing in managing your career? How are you doing in managing your stock?"

How are you advancing your game? What is the world willing to compensate you for? If you can't articulate that with clarity and precision, then you're not really in business yet. You haven't gotten the courage."

Define, Commit And Own Your Brand

"No one is going to confuse me with anyone else, just like you're not going to confuse McDonald's with a great steakhouse. That's important to me," he said. "Define your brand, decide what it is, make a commitment to it and ride that horse to the finish line. You've got to decide what it is that you're selling and own it. Be who you are on purpose. Don't just get up and react to the world. Decide who you are and do that on purpose. Don't apologize for it. Own it."

Authenticity Is Key To Facing Criticism

"In the pursuit of that, you will face criticism. Not everyone will like you and your brand. But that's exactly why you have to believe in what you're doing passionately," says McGraw. "You can't just put it on. You have to believe it. A lot of people don't like some of the things I do. And I get that. But how boring would this world be, if we were all the same? We have a divisive world, in terms of ideas. But you have to believe what you believe. Then when somebody disagrees with you, if you're authentic in your position, you won't have a problem standing with it."



SHINY NEW GADGET OF THE MONTH *BenQ ScreenBar Halo Monitor Light*

The BenQ ScreenBar Halo is a sleek USB-powered LED monitor light designed with an asymmetric optical system that directs soft, glare-free illumination onto your desk while avoiding screen reflection. With adjustable brightness and color temperature, you can dial in the perfect lighting using the wireless controller. It even has a backlight to reduce contrast with your surroundings. Plus, the auto-dimming feature adapts to your room's lighting, so it's always just right. No messy cords or mounts – just clean, functional lighting that protects your eyes and keeps your setup looking sharp.

Five Signs

YOUR DUE FOR A TECH UPGRADE

At first, hanging on to old technology for as long as possible seems like a great way to stretch your IT budget. However, the cost of doing so is much higher than simply replacing the tech.

Continuing to use old hardware and outdated software can cost your business in productivity, budget and security.



The Real Cost

There are a few ways that outdated technology is costing your business. First, old systems move slower, causing your team to move slower and impacting productivity. These systems can also fail completely, causing unexpected downtime and putting a major dent in your deliverables.

There's also the risk factor to consider.

Outdated software and hardware are more vulnerable to cyberattacks, because they are no longer being patched to protect against known vulnerabilities.

Hackers are able to exploit these vulnerabilities and access your business's data. Because of this latent risk, your business also runs the risk of failing compliance audits. That's why it's so important to update to the latest software or hardware to stay secure.

Here are a few signs it's time to upgrade your technology:

1) Your Systems Are Still Running On Windows 10 Or Older

Windows 10 is rapidly approaching end of life; Microsoft will end support for it on October 14th. This means any new vulnerabilities will no longer be patched by security updates. Continuing to use Windows 10 past its end-of-life date is a major cybersecurity and compliance risk. To keep your business protected, plan your upgrade path now and make the switch to Windows 11.

2) You Frequently Call IT For The Same Tech Problems

Frequent crashes and lagging systems aren't just annoyances, they're also indicators that your technology is failing. Slow systems, crashes, frustrated team members and constant tech support add up – and mean a significant impact on your productivity.

3) Your Existing Software Isn't Compatible With New Tools

If you're still using legacy software, it may not integrate with mobile apps or cloud platforms. This limits your ability to adopt new technologies, serve clients efficiently and scale your business.

4) Your Devices Are Slowing Down Your Team

If your team's computers are taking ages to boot up, or freeze or crash during video calls, they're slowing down your entire workflow. At the end of the day, time is money. Inefficient systems harm both. Devices more than three to five years old should be audited for performance and energy efficiency to ensure they aren't having a negative effect on your productivity and energy consumption.

5) You're Relying On Outdated Security Mechanisms

If your business's firewall or antivirus hasn't been updated in years, you're taking serious risks with your data. Cyberthreats evolve quickly; to keep your business safe, your defenses need to evolve too. Outdated systems are often the first point of entry for ransomware attacks.

If you're worried that upgrading tech will break the bank, we hear you. But hanging on to slow, outdated systems can cost more in lost productivity, security gaps and patchwork fixes. The good news is there are plenty of affordable, strategic upgrade paths to keep your business running smoothly without blowing your budget.