



# INTEGRATION TECHNOLOGY TIMES

*“Insider Tips To Make Your Business Run  
Faster, Easier, And More Profitably”*



“As a business owner, I know you don’t have time to waste on technical and operational issues. That’s where we *shine!* Call us and put an end to your IT problems finally and forever!”  
- Karen Bowling, Integration

ISSUE 1 ■ VOLUME 8  
■ JULY 2018

## *What’s Inside:*

**5 Free Apps You Must  
Download Today**  
PAGE 2

**Funny Quotes and Jokes**  
PAGE 3

**Back To Basic**  
PAGE 3

## **Security Alert! Hackers And Cybercriminals Are Now Concentrating Their Attacks On Your Business Is Your Cyberprotection Up-To-Date?**



Technology exists in a state of constant flux. The most popular gadgets turn obsolete within a year or two, the sophistication of the hardware and software we use increases exponentially with each passing month and the digital foundations of modern society are almost continuously supplanted. Every day, there’s a new device to contend with, a fresh update and an addendum to the already dizzying array of features at our fingertips.

It’s a thrilling world full of possibility and potential, but our dependence on these ever-changing technologies comes at a price. The overlay of the Internet on all aspects of our lives is fraught with vulnerabilities that criminals are eager to exploit. Though new protective measures are developed at the same breakneck speed as the software they guard, so are new ways to penetrate and circumvent these defenses. It’s estimated that 978,000 new malware threats are released with each passing day. It’s clear that “up-to-date” can no longer be an accurate descriptor; it always describes a system one step behind the newest development.

Today, cybercriminals are casting a wider net and catching more hapless victims than ever before. We read about

the most costly of these breaches in the news each morning, including Equifax, J.P. Morgan, Home Depot, Yahoo!, Verizon, Uber and dozens more.

But these high-profile incidents don’t even comprise the majority of attacks. According to Verizon’s 2017 Data Breach Investigations Report, 61% of breaches occurred at small businesses, with half of the 28 million small businesses across the United States succumbing to a digital strike. Even scarier is the fact that UPS Capital reports that 60% of these businesses shut down within six months of a breach.

It’s a bleak reality to come to terms with if you’re a business owner. The truth is that it’s almost a statistical certainty that hackers will come for your data, and when they do, they’ll likely be using techniques nearly unrecognizable from today’s malicious flavor of the month. How can you possibly prepare for something that is constantly changing?

The answer is sustained attention, vigilance and resources directed toward protecting all that you’ve worked so hard to build. While it may be impossible to foresee exactly how hackers will try to penetrate your business, it’s well

Continued page 2 .....

Continued from page 1 ...

within the means of most businesses to implement comprehensive security solutions to give your organization a fighting chance.

It's vital to realize that, unfortunately, security protocols aren't a set-it-and-forget-it proposition. To respond to the evasive and increasingly sophisticated tools being shared throughout the enormous hacker community, you need an equally sophisticated and regularly updating security system. For nearly every one of the 978,000 fresh new malwares developed daily, there are patches and updates designed to address them – strategies and techniques to outsmart even the most devious of criminals.



Just because you don't have the resources of a massive corporation doesn't mean you need to be low-hanging fruit for well-funded and highly organized cybercrime rings. Hackers assume that a business like yours is too tiny and ill-informed to prepare for even a simple phishing scam, and they're usually right. But if every business owner put just a little more effort into securing their data, you can bet attacks would be curbed. And if every small business pledged to implement a professionally managed security protocol, we would see the frequency of these hacks diminish drastically.

There's a lot for business owners to think about during a year as chaotic as 2018, but your top priority should be the basic security of your company. Invest your time and resources into building a foundational blockade for potential threats, and you can rest assured that your livelihood is safe from digital collapse.

## Back To Basics

**Everyone worries about the newest scams and cybercrimes, but if you and your team can remember the basics, you'll have a big head start. Document your security policies, such as strong password requirements, requiring a VPN to connect remotely and Internet usage guidelines, and make them a part of every employee's training. You also should include strict penalties for violating this protocol.**

**“Remembering the essentials is the best thing you can do to protect yourself and your company.”**

**A couple more basics: It's not a good habit to save files onto your computer if there is a location on the network or server where they can be saved. If you use websites or software that does not require regular password changes, set a calendar reminder to change the password yourself every other month. As with anything, a little prevention goes a long way. Remembering the essentials is the best thing you can do to protect yourself and your company.**



## Funny Quotes and Jokes



Have you heard of that new band “1023” Megabytes? They’re pretty good, but they don’t have a gig just yet.

Why did the computer show up at work late? It had a hard drive.

Some things Man was never meant to know. For everything else, there’s Google.

I love the F5 key. It’s so refreshing.

Why are programmers no fans of the outdoors?

There are too many bugs.

What does a baby computer call its father?

Data

## Master These 3 Roles To Become SUPER Successful

Everybody is eager to offer business owners free advice, but as a leader, your success will come down to how well you fill three key roles: leader, manager, and executor. First you need to lead. Start by accepting that any success or failure within your company lies squarely on your shoulders and that everything depends on your vision, strategy and understanding of your target demographic.

Then you need to manage. Surround yourself with people who are dedicated to making your business grow. Everyone should know the organization’s goals and how you plan to achieve them. Transparency is vital to building trust and cohesion within your team.

Finally, you have to execute. Run through the individual steps on the path to your goal. Your employees should focus on the day-to-day tasks so you can cultivate the big-picture direction of your company. Inc.com 2/21/18

## Ways Technology Can Make Your Business Meetings More Productive

Every entrepreneur knows how difficult it can be to run an efficient meeting. But most of them aren’t leveraging new technologies designed to do just that. Rather than treating meeting participants like audience members, use a tool like GoWall to empower your team to contribute without disrupting your meeting’s flow, keeping them engaged and on topic. Meanwhile, solutions like ParticiPoll equip any meeting with a poll that can provide useful feedback to implement at your next gathering. This is especially valuable for organizations that frequently host remote events, providing a quick breakdown of your meetings’ strengths and weaknesses.

Speaking of remote contacts, Google Hangouts has made it easier than ever to set up video conferences where participants can move from chat to file sharing to video chat with no fuss whatsoever. And if you’re unable to stand in front of your team with a whiteboard, consider implementing a whiteboard app like Cisco Spark Board, which uses shared screens to create a cohesive brainstorming session between you and your team. SmallBusinessTrends.com 2/21/18

## Two-Factor What?

Two-factor authentication (2FA for short) is a system in which you must verify your identity in two separate ways to access an account. Sound confusing? It’s not. Here’s an example:

After enabling 2FA on a Gmail account, you have to enter your password each time you log in. Then you are asked to enter a six-digit code that you pull from your phone, a jump-drive-sized key fob or a program on your computer.

Only then do you have access to your account. That way, if someone steals your password, they still can’t get in.

If you aren’t currently using two-factor authentication with your most sensitive data and systems, look into whether it might be an option. The extra 15 seconds it takes to pull up that second code is laughably short compared to the time you’d spend dealing with a hacked account.



## Computer Service

- ⇒ Pro-Active Customer Care
- ⇒ Onsite Computer Service/Support
- ⇒ Network Management/Support
- ⇒ Network & Server Installations
- ⇒ Network Security & Firewalls
- ⇒ Cloud Solutions & Hosted Email
- ⇒ Secure Remote Access / VPNs

## Healthcare Services Provided

- ⇒ Medical, Dental, Radiology
- ⇒ Software & Hardware Integration
- ⇒ Security Solutions

## Ask us about — Managed Services

How would you like to pay a flat rate and have us take 100% responsibility?

How would you like new equipment, service and support for a flat rate and refresh every 3 years?

## Backup & Disaster Recovery

- ⇒ Business Continuity
- ⇒ Secure & Compliant Offsite Backup
- ⇒ HiTech BDR

## Email, Web & Archiving

- ⇒ Spam Filtering
- ⇒ Email Hosting
- ⇒ Email Encryption & Archiving
- ⇒ Website Hosting
- ⇒ Customer Hosting Server

## VOIP (Hosted)

.....

How would you like the security of knowing that your data is safe and protected?

How would you like a VOIP phone system that is cost effective, saves you money, and you can take it home or vacation and work as in the office?



## INTEGRATION

Po Box 5526  
DECATUR, AL 35601  
PHONE: 256.536.5805

