



Creative Resources Technology Group

"Insider Tech Tips and Strategies at Your Fingertips"

This Issue's Must-Reads:

Sneaky Ways Cybercriminals
Access Your Network | page 1

Free Report: Why SaaS Isn't
Backup | page 2

Invaluable, First-Rate Team | page 3

Watch Your Doors | page 3

Tech Tip of the Month | page 3

5 Easy Things You Can Do
To Protect Your Business | page 4

February 2019



This monthly publication provided courtesy of Russell Poucher, President of Creative Resources Technology Group.

Our Mission: To make technology work seamlessly with your business and to work for you, not against you. As the leading Apple Consultant in Orange, Riverside, and San Diego County, we pledge to always provide innovative solutions that meets your specific business needs, superior customer service, and expert strategies on how to leverage IT to build your business. *Don't worry, we got IT.*



Sneaky Ways Cybercriminals Access Your Network

And What You Can Do To Prevent It TODAY

Hackers prefer the little guy. The high - profile data breaches you read about in the news — your Facebooks and Equifaxes and T-Mobiles — are only the tip of the iceberg when it comes to the digital crimes being perpetrated day after day, especially against small businesses. Today, according to a report by the National Cyber Security Alliance, 70 percent of hackers specifically target small businesses. Attracted by the prospect of easy money, they search for those organizations who underspend on protection, who have employees untrained to spot security risks, and who subscribe to woefully out-of-date practices to protect their data. As a result, more than 50 percent of small businesses have been hacked, while 60 percent of companies breached are forced to close their doors within six months.

Most business owners have no idea the danger they're putting their livelihood in by leaving cyber security up to chance. According to a survey conducted by

Paychex, 68 percent of small-business owners aren't concerned about their current cyber security standards, despite the fact that around 70 percent of them aren't adequately protected. In the face of an imminent, global threat to the very existence of small businesses everywhere, most CEOs offer up a collective shrug.

The tactics and software available to hackers become more sophisticated by the day, but with so many unwitting victims, most criminals don't even need to work that hard to net a six-figure income. By sticking to two tried-and-tested tools of the trade — phishing, ransomware and the subtle art of guessing users' passwords — they leech comfortably off the earnest efforts of small businesses all over the world.

So, what's to be done? Well, first things first: You need to educate yourself and your team. Protect your organization against phishing by fostering a healthy

Continued on pg.2

Get More Free Tips, Tools and Services At Our Website: www.creativeresources.net
(714) 551-6772

Continued from pg.1

skepticism of any email that enters your inbox. Make it a habit of hovering over hyperlinks to check their actual destination before you click. If an email is coming from someone you know, but the email address is different, verify it with the other party. And never, ever send passwords or personal details to anyone over the internet if you can avoid it.

Speaking of passwords, you probably need to upgrade yours. The majority of folks use the same password for everything from their Facebook account to their business email. The fact that this includes your employees should make you shudder. It may not seem like a big deal — who’s going to take the time to guess SoCcErMoM666?— but aside from the fact that simple software enables hackers to guess even complicated passwords in minutes, that’s not even usually necessary. Instead, they can just look at the data dumps from a recent more high-profile breach — think the Equifax fiasco — pull your old website from there and type it into whatever profile they want to access. If you keep all your passwords the same across sites, it won’t take them long to dig into your most precious assets. To avoid this, implement a strict set of password regulations for your business, preferably incorporating two -factor authentication and mandatory password changes every few weeks.

“In the face of an imminent global threat to the very existence of small businesses everywhere, most CEOs offer up a collective shrug.”



Of course, you can read up on hacking techniques and teach them to your team until you’re blue in the face, and a data breach can still occur. Cybercrime is constantly evolving, and staying abreast of its breakneck pace takes a dedicated awareness of the latest protective tools and measures. That’s why your single best weapon to defend you against the hackers at your door is to find a managed service provider (MSP) with a background in defending against digital threats to partner with your organization. These companies not only regularly monitor your network, they also keep it updated with the latest patches and measures to prevent the worst. And if crisis somehow still strikes, they’ll be able to get your network back up in minutes rather than days, equipped with an expert knowledge of your systems and years of experience in the field.

In today’s digital world, leaving your cyber security up to a subpar antivirus and some wishful thinking is more than irresponsible — it’s an existential threat to your company. But with a little savvy, a bit of investment and a second opinion on the circumstances of your company’s security, you can rest easy knowing that no matter what comes, you’re protected.

Free Report: Why SaaS Isn’t Backup

One of the most business-friendly innovations in recent years has been the proliferation of cloud apps like Google Apps, Office 365, and Salesforce. These SaaS apps have fundamentally changed the way we do business, enabling companies to take advantage of economies of scale, reduce infrastructure costs, and expand the boundaries of a cubicle.

In this e-book, we compare 3 of the world’s premier SaaS applications (Google Apps, Office 365, Salesforce) to highlight how they are (and aren’t) protecting your data. Get the facts straight and start backing up before it’s too late.

Download your free copy today at:

<https://www.creativeresources.net/why-saas-isnt-backup/>



What Our Clients Have to Say:



"Invaluable, First-Rate Team"

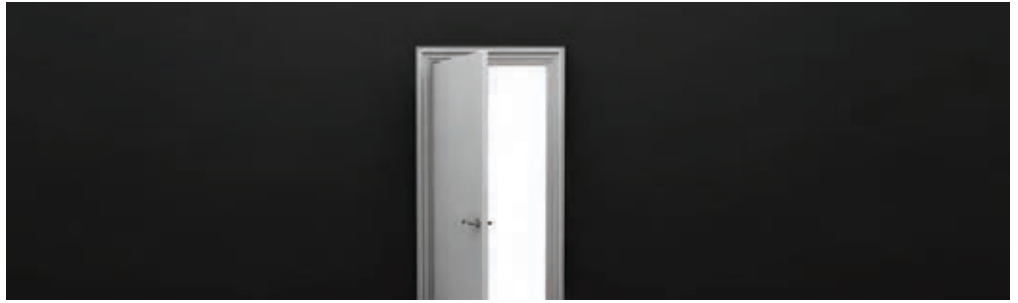
Less than a year ago our company had been experiencing multiple lengthy periods of email downtime due to our previous email hosting provider. The cost to our company in lost productivity, time, monetary damages and our reputation with our clients was getting higher every day. As the sole "IT" person at our company, my days were filled with putting out fires. That all seems like it was in the distant past now. CRTG provides us with online data backups, email archiving, onsite and remote support, and a host of other services that we now find invaluable. Their Apple technical knowledge is first rate. But more impressive than that is their team of engineers, technicians and office personnel. All of them are personable, friendly, responsive, professional and excellent communicators. As much as we would like to keep CRTG a secret for selfish reasons, I hope this review influences some of you to give them a try. We're certainly glad we did!

Jim Hendricks
Project Manager
Riviera Building & Development

We don't like to brag but check out what our clients have to say about us here:

www.creativeresources.net/our-clients

Watch Your Doors



When was the last time you looked at the doors to your business? It isn't just about who comes in; it's also about how.

Let me give an example. A new restaurant opened near my office. It's been very successful, and I eat there regularly. The only problem is the horrendous door you have to go through to get in. Opening it causes an obnoxious grating sound, not unlike a few metal tomcats duking it out in an alley. The pull is hard and inconsistent. At first I thought they'd fix it, but since it hasn't been dealt with in months, it's clear to me that the owners don't give much thought to the first impression it creates.

Actual doors are important, but the metaphorical doors to your business are even more important. These "doors" are entry points, drawing people in or keeping them out. They can welcome or they can warn.

What about the doors to your business?

Your website is your online door. Is it aesthetically pleasing? Easy to navigate? Up-to-date? Can a visitor quickly find contact information? Does it just advertise, or does it make it easy for visitors to actually take action?

Your phone is a door too. Whether answered by a person or a recorded message, it speaks volumes about your professionalism and punctuality.

The way you handle service and support is yet another door. How easy is it for a customer to schedule a repair? Do techs arrive when promised? Are they professional in appearance and friendly in demeanor?

Then there's your social media accounts. What image do your various platforms convey? Does your social media support or detract from your brand?

Your office environment is another. Is it a place customers enjoy or endure? If you serve coffee, how good is it?

Gordon Hinckley said, "Eternal vigilance is the price of eternal development." Paying attention consistently will allow you to develop and achieve success. Ignoring the doors, literal and metaphorical, can be costly.

A good door makes it easy for customers to enter. A great door invites them in and sets the tone for what follows. Make sure yours immediately conveys everything you want others to know about your business.

Tech Tip of the Month



You're working at your computer when all of a sudden - BAM! - you get a pop-up notification that your PC is infected with a virus and you must "click here" to run a scan or install antivirus software. This is a common scareware tactic used by hackers to get you to click and download a virus. You should know that we would never deliver that type of pop-up to you. Often it will appear to be a system alert or a Microsoft operating system alert. Regardless of how legitimate it looks, NEVER click on the site or the pop-up. The safest thing to do is close your browser; do not click on the X, "Close", or "Cancel" button in the pop-up or on the site because clicking anything on the page or pop-up will trigger a virus download. **PRO TIP:** Bring up your task manager (CTRL + ALT + DEL for PC and CMD + OPT + ESC for Mac to "Force Quit").

Want to stay on top of the latest IT updates? Sign up for our Security Tip of the Week here: www.creativeresources.net/tech-tip-sign-up

■ 4 Reasons You Should Move Your Data To The Cloud TODAY

If you're one of the skeptics holding out on incorporating cloud technology into your business, you're in the minority. Today, a full 93% of businesses now use the cloud in their day-to-day operations, according to RightScale. Here's why.

- The cloud increases profits. The nimble, location-flexible nature of the cloud enables lean, remote operation from anywhere in the world, increasing the bottom line of SMBs.
- The cloud boosts efficiency. Without the need for data silos, cloud applications

can drastically reduce bottlenecks and failures.

- The cloud saves money. Instead of paying to maintain unused hardware, the cloud allows you to pay low monthly fees, reducing wasted funds.
- The cloud is more secure. Backups are that much easier to implement and access, meaning that your business can be up and running after a data breach in minutes rather than days. *Smallbiztrends.com, 11/27/2018*

■ Top Tactics To Improve Company Culture

A healthy company culture does more than make work

life bearable – it draws in talent and increases productivity. But contrary to what some CEOs may believe, culture begins with leadership. To bolster a positive, winning environment in your business, make sure that above all, your team embodies the core values of your organization. Hire and fire by the standards you've set, and build an organization that seeks to bring meaning to the business you do.

Also, be sure to maintain transparency at every turn. Nothing erodes trust and good vibes like secrets or the rumors they spawn, yet many leaders struggle to understand that, when faced with a difficult situation, a thorough explanation will win the loyalty and consideration of those you work with.

Finally, keep your vision locked on your organization's long-term goals. With a clear focus in mind for your employees, it's that much easier for everyone to stay on the same team and continue to push forward in earnest. Short-term wins are important, sure, but it's the visionary in you that will become someone to rally around for the long haul.

5 Easy Things You Can Do To Protect Your Business Today

- 1. Review your business insurance carefully.** Most business carry some type of general liability insurance that would pay them if their building and the things in it were damaged. Do you know how much it actually covers?
- 2. Consider cloud computing.** The biggest advantage of cloud computing is that your data and assets are stored off-site in a highly secure, high-availability data center, with failover and redundancy built in.
- 3. Secure your data.** Making sure your data is protected from theft is a never-ending battle you don't want to lose. Companies that get hacked and expose sensitive client and employee data can face severe penalties, lawsuits, and massive loss of credibility in the marketplace.
- 4. Write a simple disaster recovery plan.** The key word here is "simple." If your plan gets too complicated or difficult, you won't do it. But at a minimum, think of the disaster that is most likely to happen and that would have a severe and negative impact on your company's survival.
- 5. Review your employees' Internet Policy.** According to a recent survey by Salary.com, 64% of respondents admitted to visiting non-work related websites every day during work hours.

Not sure if you have all these items checked off? Contact us now for a **FREE Network Assessment** at www.creativeresources.net/freenetworkassessment