Creative Resources Technology Group

"Insider Tech Tips and Strategies at Your Fingertips"

March 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.*

The #1 Mistake Your Employees Are Making Today That Lets Cybercriminals Into Your Network

In the wake of unprecedented rates of digital crime, with the cost and frequency of data breaches constantly skyrocketing year after year, companies all over the world have been forced to scramble for solutions. There's an arms race running behind the scenes of every piece of technology we use in business today, as cyber security companies shore up their clients' defences against increasingly sophisticated digital threats. Billions of dollars are now poured into batting away would -be intruders from the most precious assets on global networks: most of the money directed toward the software that keeps everything afloat, just out of reach of the bad guys.

But even as each day brings a new technological apex for security solutions, data breaches continue. Despite the fact that the tools hackers use to make money are more or less the same as they were three years ago, nobody seems to question why companies are still being hacked at record levels. It's easy to imagine a crack team of infamous hackers hammering away at a keyboard into the late hours of the night, feverishly computing the one piece of code that will break them into a system.

This may be the process behind the high -profile breaches you read about in the news each week, but in reality, most cybercrime takes much less effort. The average hack succeeds not because of overt vulnerabilities in the structure of business networks, but because of a mistake made by you or your employees. According to IBM's X -Force Threat Intelligence Index, more than two-thirds of breaches arise from what they call "inadvertent insiders," folks who accidentally left the network vulnerable from one action or another without even realizing it.

Continued from pg.1

Most of the human error that becomes the root cause of catastrophe can be traced back to phishing. A criminal spends some time researching your organization, maybe learning a bit about an employee or two, and decides to masquerade as someone worthy of trust either within your team or from a company you contract with, or just a stock person offering something pretty much everybody wants. They mock up a somewhat convincing email and send it off to 10 people within your business. Somebody clicks the included link without thinking, and there you go – you've got ransomware. If you haven't backed up your data, you're looking at a hefty fee to get everything back, if they even give it back at all.

In other cases, your team may actively duck around your previously implemented security measures or avoid the procedures you've put in place to keep the business safe. That can mean visiting unsavoury websites, ignoring a vital security patch or another minor transgression. But when every mistake spells a potentially massive vulnerability, you can't afford people who aren't conducting business to the highest standards in cyber security.

Regardless of how it happens, most hacks occur because employees just don't know better. Even in 2019, when cybercrime runs rampant and virtually everyone is

"Somebody clicks the included link without thinking, and there you go — you've got ransomware."

constantly at risk on the Internet, most of us just aren't well-versed in ways to protect ourselves, much less the companies we work for.

The good news is that this problem is pretty easy to prevent through education. To keep everyone abreast of the latest threats to their livelihood, it takes a thorough set of rules, guidelines and general savvy to steer them through the troubled waters of modern cyberspace.

Of course, this will take more than a 30-minute crash course in the break room one afternoon. It'll take a concerted effort and dedicated resources. Luckily, we can help. With a trusted partner dedicated not only to keeping your organization protected from the latest digital threats, but to keeping your employees alert and ready to spot anything phishy, you drastically decrease the chances of your business becoming another statistic in the war on cybercrime. Work with us and secure the future of your company for the long haul

Free Report: Why SaaS Isn't Backup

Why SaaS Isn't Backup
Yes, you need to backup your cloud data.

Storing data in cloud applications is far safer than storing data on most on-premise storage systems - but "safe" does not equal "invulnerable." In fact, 1/3 of SaaS users report losing data in the cloud. Yes, the cloud is safe, but it's not infallible and today's cloud vendors lack the incentive to point out their vulnerabilities.

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

The Self-Made Myth: All Business Leaders Had Help Along The Way

I'm about to share an unpopular opinion: the self-made CEO is a myth. No successful entrepreneur or business leader is a self-made man or woman. If you think you are, you need to take a long, hard look in the mirror. Behind your success are countless contributions from family, friends, teachers, mentors and coaches. If you can't see that, you're not looking hard enough.

As a business coach, I've seen countless companies grow from kitchen tables to $100 million enterprises and then collapse because the owners thought they knew everything. In contrast, the world's most-effective leaders know they didn't get to where they are by themselves. They recognize that ideas can come from anywhere, and they actively seek out people who can help them on their journey. Here are three ways to harness that inspiration.

1. RELY ON YOUR TEAM, AND SHOW YOUR APPRECIATION.
The most effective leaders are always the first to admit that they don't have all the answers. They ask themselves tough questions to understand their own strengths and weaknesses, and they don't let ego or pride get in the way of building their companies.

One of the biggest mistakes I see business leaders make is thinking they can't learn anything from the people around them. It's essential to recognize your limits, seek others' help and opinion to patch holes in your expertise, and give credit where credit is due.

2. RIP OFF AND DUPLICATE — THE OTHER R&D.
Some of the best ideas I've had for my businesses are ones I've borrowed (and modified) from others. In my experience as an entrepreneur and coach, I've seen first-hand how ideas that are considered standard practice in one industry can be innovative when applied to another.

Of course, it's about how you adapt those ideas to your business, not necessarily just copying what your competitors are doing. Instead, use the existing base of knowledge to provide a novel solution.

3. CROWDSOURCE IDEAS FROM FELLOW BUSINESS LEADERS.
Finding new solutions to business challenges is a never-ending and often exhausting task for entrepreneurs and business leaders. One source that I've used to help me solve problems has been a business advisory group (BAG) comprised of professionals in business operating in non-competitive markets. Peers in a BAG can relate to the daily challenges you face running your company, managing teams and growing the business. BAG members can provide you with valuable insight into how they are running their own companies and how business solutions they've implemented may apply to your business.

Business is a team sport. No great company has ever been built solely atop the efforts of a single person. The entrepreneurial spirit will take you far, but eventually you have to recognize that you need to rely on the ideas and contributions of others. When that happens, you'll become a greater leader, and you'll see your business and company culture grow exponentially.

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 appeaer 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*

■ 3 Ways To Make Your Customers Love You

1. Be available.

Today, when customers expect products to be available on-the-go, businesses must do the same. Set up reliable resources to update and manage customer experience, for example, by setting up an automatic callback system. Instead of waiting on hold, callers get added to a list, then receive the call when the service team is ready. Live chat, an informative online FAQ and other handy resources can go a long way toward avoiding frustration.

2. Surprise customers by actually being convenient.

We've all had interactions with customer service that made us want to pull our hair out. Avoid this by reducing friction wherever possible. Make sure the people in charge of customer experience, whether it's a front-desk person or a team of dedicated service professionals, are friendly and transparent about the service process. Make signing up for appointments abundantly easy and pleasant, and you'll see the benefits in no time.

3. Put your money into the most important investment.

We all know that acquiring new customers costs seven times more than keeping existing ones. That makes the numbers pretty clear: you need to invest in your existing customers or risk going under.
Inc.com, October 4, 2018

■ Can You Afford To Lose $80,000 A Year? If Not, Read This:

According to the Better Business Bureau's 2017 State of Cybersecurity Among Small Businesses In North America report, SMBS lost more than $79,000 to cybercriminals. Honestly, this shouldn't surprise anyone; after all, as even the smallest businesses digitize more and more of their processes, the costs of breaking those systems will continue to skyrocket. If you're a small-business owner in 2019, you need to start making cyber security a priority – now. Make a list of clear goals and objectives, and prepare your business for threats coming from all directions, rather than relying on a single defensive strategy that's prone to fail when things get tough.
SmallBizTrends.com, 12/3/2018

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*