The Tech chronicle

Creative Consultants Group, Inc. October 2018

Sign Up To Receive CCG's Free Report on Cybercrime and Our Weekly Cyber Security Tips!

Visit Here To Sign Up Today for Our Weekly Tips and Our Report, The 7 Most Critical Security Protections Every Business Must Have In Place Now!

TIPS

October 2018

This monthly publication provided courtesy of Bill Hinson, CEO of Creative Consultants Group, Inc.

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

How To Make Sure You Never Fall Victim To Ransomware

Late last March, the infrastructure of Atlanta was brought to its knees. More than a third of 424 programs used nearly every day by city officials of all types, including everyone from police officers to trash collectors to water management employees, were knocked out of commission. What's worse, close to 30% of these programs were considered "mission critical," according to Atlanta's Information Management head, Daphne Rackley.

The culprit wasn't some horrific natural disaster or mechanical collapse; it was a small package of code called SAMSAM, a virus that managed to penetrate the networks of a $371 billion city economy and wreak havoc on its systems. After the malicious software wormed its way into the network, locking hundreds of city employees out of their computers, hackers demanded a $50,000 Bitcoin ransom to release their grip on the data. While officials remain quiet about the entry point of SAMSAM or their response to the ransom, within two weeks of the attack, total recovery costs already exceeded $2.6 million, and Rackley estimates they'll climb at least another $9.5 million over the coming year.

It's a disturbing cautionary tale not only for other city governments, but for organizations of all sizes with assets to protect. Atlanta wasn't the only entity to buckle under the siege of SAMSAM.

According to a report from security software firm Sophos, SAMSAM has snatched almost $6 million since 2015, casting a wide net over more than 233 victims of all types. And, of course, SAMSAM is far from the only ransomware that can bring calamity to an organization.

If you're a business owner, these

continued on page 2

numbers should serve as a wake-up call. It's very simple: in 2018, lax, underfunded cyber security will not cut it. When hackers are ganging up on city governments like villains in an action movie, that's your cue to batten down the hatches and protect your livelihood.

The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?

1. Back Up Your Stuff

If you've ever talked to anyone with even the slightest bit of IT knowledge, you've probably heard how vital it is that you regularly back up everything in your system, but it's true. If you don't have a real-time or file-sync backup strategy, one that will actually allow you to roll back everything in your network to before the infection happened, then once ransomware hits and encrypts your files, you're basically sunk. Preferably, you'll maintain several different copies of backup files in multiple locations, on different media that malware can't spread to from your primary network. Then, if it breaches your defenses, you can pinpoint the malware, delete it, then restore your network to a pre-virus state, drastically minimizing the damage and totally circumventing paying out a hefty ransom.

2. Get educated

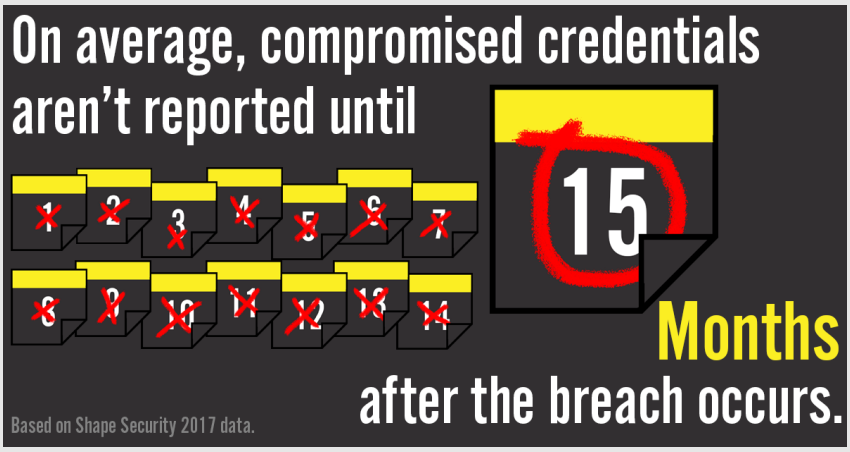
We've written before that the biggest security flaw to your business isn't that free, outdated antivirus you've installed, but the hapless employees who sit down at their workstations each day. Ransomware can take on some extremely tricky forms to hoodwink its way into your network, but if your team can easily recognize social engineering strategies, shady clickbait links and the dangers of unvetted attachments, it will be much, much more difficult for ransomware to find a foothold. These are by far the most common ways that malware finds it way in.

3. Lock It Down

By whitelisting applications, keeping everything updated with the latest patches and restricting administrative privileges for most users, you can drastically reduce the risk and impact of ransomware. But it's difficult to do this without an entire team on the case day by day. That's where a managed services provider becomes essential, proactively managing your network to plug up any security holes long before hackers can sniff them out.

The bad news is that ransomware is everywhere. The good news is that with a few fairly simple steps, you can secure your business against the large majority of threats. Call us at (843)234-9980 for a FREE Network Security Assessment so we can ensure your business is protected.

> **"The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?"**



Are Your Credentials For Sale On The Dark Web? Contact us before December 1st for a FREE Dark Web Analysis. For more information, visit www.getccg.com/darkweb/!

SHINY NEW GADGET THE MONTH

CLOCKY: The Alarm Clock On Wheels

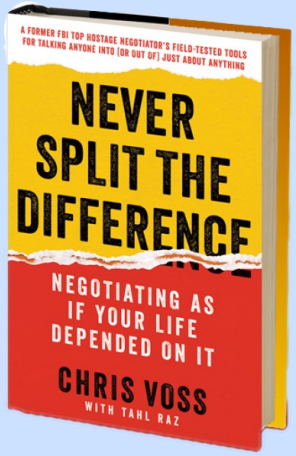
Waking up can be difficult. Even the most driven people occasionally struggle to get out of bed in the morning, pounding the snooze button ad infinitum until we finally force ourselves upright, dazed and groggy from interrupted sleep.

That's where Clocky, the alarm clock on wheels, comes in. Clocky is an adorable little digital timekeeper to keep by your bed; it will be your best friend until it comes time to rise in the morning. By default, it'll give you a single press of the snooze for free, but once you hit snooze for the second time, it'll speed off and start wheeling around your room, beeping and making a racket until you catch it and send it back to sleep. If you or someone you know struggles to get out of bed in the morning, Clocky will be a trusted ally in your mission to start the day.

Never Split The Difference

By Chris Voss

In today's business world, everyone is a negotiator. But hopefully, you've never had to wheel and deal your way out of a hostage situation where lives were on the line.



But that's exactly what ex-FBI kidnapping negotiator Chris Voss used to deal with all the time in his old job. In his best-selling book, *Never Split The Difference*, Voss outlines the tactics that expert negotiators employ to achieve their desired outcome, invaluable strategies that any business leader could stand to master.

4 Types Of Hackers That May Target SMBs

When it comes to cyberattacks, most business owners get hung up on the technical and logistical details, forgetting another important aspect: motive. Why are hackers attacking people and organizations? And whom are they targeting? By answering these questions, you'll have a better understanding of which of your business's resources need the most protection.

Script Kiddies

Skill-wise, script kiddies (or skids, for short) are at the bottom of the hacker totem pole. Their name comes from the fact that they use scripts or other automated tools written by others. Most of the time, script kiddies are young people on a quest for internet notoriety. Or, more often than not, they're simply bored and in search of a thrill. Many never become full-time hackers; in fact, many script kiddies end up using their skills for the greater good, working in the security industry.

Though lacking in hacking know-how, script kiddies shouldn't be dismissed so easily, as they can cause businesses much damage. In May 2000, for instance, a couple of skids sent out an email with the subject line "ILOVEYOU" and ended up causing a reported $10 billion in lost productivity and digital damage.

Hacktivists

Hacktivists are primarily politically motivated, and they often hack into businesses and government…

Read More Here

4 Ways To Keep Your Team Inspired

By Andy Bailey

Entrepreneurs and business leaders often find that motivating team members is one of the most challenging parts of the job. Leaders seldom lack self-motivation — it's so second nature to them that they get frustrated when a team member doesn't appear to have the same level of drive and ambition.

One of the most frequently asked questions I hear from business leaders is "How can I motivate my team?" Imagine their surprise when I tell them, "You can't." My responsibility as a coach is to help company leaders grasp the underlying reasons for their own motivation and ensure that those reasons are consistent with the goals and objectives of their business. In the same way, leaders need to stop looking for ways to motivate and instead find ways to inspire team members to seek out their own motivation.

Business leaders must understand that team members will not always share their outlook or passion. Instead of forcing your will on others, use these four approaches to inspire motivation in your team.

1 Lead by example.

Show your team members how it's done, and dedicate yourself to showing your passion and motivation in everything you do. When your team members see your genuine excitement and enthusiasm, they'll be much more likely to increase their energy levels and get on board.

2 Honesty is the best policy.

It's vital that you be open and honest about the task at hand. You must get your team members to understand why the task is so important to you personally and to the company as a whole. Not every goal, task, or objective will foster the same amount of excitement and teamwork. If what you want is challenging or risky, let your team know. They'll respect your transparency and be more likely to trust you and your leadership.

3 Find balance.

There are two surefire ways to destroy motivation among team members. The first is micromanaging, and the second is being so hands-off that your team doesn't know what to do when problems arise. Give your team the freedom they need to feel empowered, but stay involved so that you can provide the necessary guidance when team members get discouraged.

4 Expect results and celebrate victories.

Before you give your team their marching orders, let them know you have confidence in their abilities. Take time to explain why a successful outcome is important to you and the business. They'll be more likely to meet your expectations, not because they're doing it for your sake, but because they're working harder for the benefit of the team as a whole.

It's crucial to celebrate wins with the team and to express your appreciation. An individual reward can be a great motivational tool, but it's just as important that you celebrate as a team.

CCG Monthly Trivia -Win $250 Gift Card!

The Grand Prize Winner of last month's Trivia Challenge Quiz is Michelle Schmalfeldt of Ally Management! Michelle's name was randomly chosen among those that correctly answered my quiz question from last month: Which NFL coach has the most wins in NFL history? The answer was d) Don Shula.

Now, for October's trivia question. Email your answer to: swoollums@creativeconsultants.net.

What color jersey is worn by the winners of each stage of the Tour De France?

a) black b) yellow c) red d) blue

"I heard she has eyes in the back of her head, but I suspect more likely it's some combination of Google Glass and a smartwatch."