Effective IT for Business
FUSIONFactor

TECHNOLOGY Bytes
Insider Tips to Make Your Business Run Faster, Easier & More Profitably

"As a business owner, 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!"

-Bhavin Mehta, Fusion Factor Corporation

OCTOBER - 2018
Carlsbad, CA

What's Inside

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 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 *(Continued on page 2)*

(Continued from page 1)

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 un-vetted 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.

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

Shiny New Gadget Of 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.

4 Ways To Keep Your Team Inspired

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.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

Top Tricks Cybercriminals Use To Hack Your Computer Network

There's no denying that cybercrime is on the rise. All it takes is a glance at a few big news stories from the past couple years. Equifax gave up the information of over 100 million people, many of them not even users, to a surgical hacker attack. Last May, over 57,000 infections spread from a single ransomware source across 99 separate countries, with damage reaching everything from hospitals and businesses to vital public utilities like the German railway network. And how many high-profile celebrities have had their phone's picture feeds hacked and had to deal with the scandal of some maliciously leaked photographs, some of which they'd deleted years before?

But it's not just massive corporations like Equifax or JPMorgan or actresses like Jennifer Lawrence that are being targeted day in and day out. It's small businesses, many equipped with far less robust security measures in place. In fact, if you're an entrepreneur, it's almost a statistical guarantee that hackers will target your business at some point down the road.

In your company's battle against cybercrime, it's essential to stay abreast of the rapidly shifting digital landscape. Only the most up-to-date security technology can even hope to protect you from the ever more sophisticated thieves pounding at your digital door.

However, it's also important to stay informed. Here are a few of the sneakiest and most common tricks thieves use to snatch your vital data:

Social Engineering Hacking, though it can cost you thousands and thousands of dollars and do just as much damage as its digital counterparts, doesn't require a single line of code. Instead, they find weaknesses in the "human network" of a business. For example, skilled scammers can call your business's cell phone provider, posing as the CEO's spouse, and convince the customer service rep to hand over passwords, Social Security numbers, and sensitive personal information. Many IT departments are susceptible to this same scam.

Often, social engineering is used to gather information that will later be used for a different strategy. Such as …

E-mail Phishing, which hijacks (or fabricates) an e-mail account with trusted authority and sends users an e-mail requesting they click a particular link. Maybe the e-mail looks like it's from the service department of your company's time-tracking software, seeking to remedy an error. But when the link is clicked, ransomware or other malware spreads like wildfire through the system, and the user is at the mercy of the hackers. Usually, this is used to extort exorbitant sums of money out of small businesses or individuals. Symantec reports that just last year, over 7,000 businesses of all sizes fell prey to some form of phishing scam, costing them more than $740 million in total.

Brute-Force Password Attacks Or Password Guessing are just what they sound like. Either a hacker uses a software that, after putting in some data about the target (for example, the name of their dog or their anniversary), runs through potential keys ad infinitum. With sufficient information about the target, it's only a matter of time before the software breaks through. Or, more often than you might think, hackers can simply guess the password. Infiltrators have common passwords that use real words or common structures memorized and can run through hundreds before giving up.

Fault Injection is a different story, usually only used by the most dedicated, sophisticated hackers around the world. Cyberthieves will use a complicated software to scan the source code of their internal software or network, noting every potential weak point in the system. Then, by splicing in strings of code, they can penetrate through and steal data, inject a virus, or employ other digital mischief.

How To Protect Yourself Against These Threats

As they say, forewarned is forearmed, but it's not enough to keep your eye out for common hacker strategies. As the progress of technology marches on, so do the techniques and softwares used by hackers, resulting in an infinite number of permutations of ways they can penetrate your system.

The only way to be truly secure is by utilizing bleeding-edge security solutions to ensure you stay ahead of the breakneck developments in hacker technology. With constantly updating software dedicated to security, along with some know-how, you can rest a lot easier knowing your data is safe.