9 Quick Tips To Protect Your Business From Cyber -Attack

Cyber security is more important than ever, but it doesn't have to be complicated.

Just follow the rules we've posted on our blog **here** and you'll be well ahead of the game.

Visit:

www.getccg.com/9quick-tips/

TIPS

August 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.

Employees Keeping Your Data Safe? Don't Count On It.

One morning late last year, an unemployed man was making his way across London, heading to the library to continue his job search. But on the way, he encountered something peculiar: a USB stick, peeking out among the fallen leaves and shining in the morning sun. Not thinking much of it – and perhaps afflicted with a morbid curiosity – he popped the device into his pocket and continued on his way. Once he made it to the library, he connected the USB to a computer to check out its contents. As he clicked around, he realized with a shock that this was a treasure trove of security information for the Heathrow International Airport: 174 folders packed with maps detailing CCTV camera locations, labyrinthine tunnels snaking below the building and even the exact route the Queen takes when she uses the airport.

Understandably worried, the man quickly ejected the device and brought it – for some reason – to local tabloid the Daily Mirror. Today, despite a full-scale security investigation by the airport and the scrutiny of dozens of police and security experts, it's still unclear just where this extremely sensitive data came from. However, all signs point to the USB drive being dropped by either a hapless employee carrying around a national security concern in their pocket or a less-hapless employee looking to instigate a national security crisis.

Either way, the story hammers home a vital point: whether you're an international airport hosting more than 70 million travelers each year or a small business with less than $10 million in annual revenue, your biggest security risk isn't some crack team of hackers –

it's your employees.

Sure, you may chuckle at the idea that any of your employees would actively wish your organization harm. But we're willing to guess that you probably underestimate the wrath of an employee scorned. Even if you treat your team better than any boss in the world, they are still human – which, of course, means they're going to make mistakes from time to time. And when considering the cyber security of many SMBs, "time to time" actually means every day, leaving huge openings in your digital barriers. These errors don't much matter, really – until the day that a hacker turns an eye toward your business and immediately realizes the laughable security gaps your team is leaving for them to exploit.

The thing about cyber security is that it's a lot more complicated than most people are willing to admit. Today's digital landscape is fraught with hazards, a thousand little mistakes to be made at every step, resulting in a million workarounds for cyber criminals to use. Even the most tech-savvy among us probably don't know everything about cyber security, and very few have as much knowledge as the hackers on the other end of the equation. When you consider the uncertainty and

> ## "Your biggest security risk isn't some crack team of hackers – it's your employees."

potential miseducation of your employees, many of whom probably know next to nothing about cyber security, you might start to feel a little panicked.

The battle against digital threats can seem like an endless slog – a war that the good guys seem to be losing – but luckily, when it comes to the security of your business, there are ways to batten down the hatches without dropping a ton of cash. For instance, start with your biggest vulnerability: your team. When a new employee joins your organization, they should go through a thorough cyber security training. Their welcome forms should include comprehensive rules about security policies, from using strong passwords to how they should respond to potential phishing attempts. Deviating from these policies should come with serious consequences.

As for your existing employees, train them up! We can help you build a robust education program to get every single member of your organization up to speed on the most imminent cyber security threats. But even then, cyber security isn't a one-and-done kind of thing; it requires constant vigilance, regular updates on the latest trends and a consistent overall commitment to protecting your livelihood. Without training and follow-up, even the most powerful of cyber security barriers are basically tissue paper, so put some thought into your team in addition to your protections, and you can drastically increase the safety of the business you've worked so hard to build. Contact us for assistance at (843)234-9980.

An Indoor, No-Hassle Cookout: The Kenyon City Grill

As we draw close to the end of summer, many of us are stowing our grills in preparation for the cooler months. Others never had a grill in the first place, banned by their lease from ever doing any sort of grilling. Regardless of the reason, pretty much everyone bemoans a grill-free existence, even if it's only for a few months.

Enter the Kenyon City Grill, a handy grill for those of us who need to stay inside to cook up a hot dog or hamburger. With some complicated engineering tricks, the grill can cook anything you throw at it with virtually no smoke, far exceeding the requirements of city fire codes and preventing you from getting smoked out of your kitchen. Its $475 price tag may seem a little steep, but consider the convenience of grilling right from your kitchen, all year long – even if you're in an apartment! – and you can quickly see the benefits.

The Culture Code
By Daniel Coyle

Many small-business owners seek to ape the strategies of their bigger cousins, looking toward the future in every aspect except one: culture. But what these small-minded leaders fail to realize is that, prior to hiring the best employees possible and having them do their best work, prior to nearly everything else, culture must be considered, because it's the driving force that makes successful businesses tick.
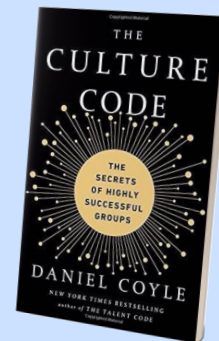
In Daniel Coyle's best-selling book, *The Culture Code*, he unpacks the complicated subject of company culture, starting from the basics and delving into the intricacies of some of the world's best organizations. What he discovers is that, even in teams as disparate as the Navy SEALs and the Upright Citizens Brigade, there are common behaviors and processes that foster work capable of truly changing the world.

The Top 5 Business Apps To Improve Your Productivity

In the light-speed world of modern business, workers need every bit of help they can get. Luckily, new apps are developed every day that make our lives easier. Here are five of the best:

* **Documents To Go** allows users to open and edit Microsoft Office 2007 files from any smart device. While that may seem a simple task, if your company frequently uses the Office Suite, Documents To Go can make a big difference.

* **Evernote** has been making waves for a few years now with its seamless approach to notetaking and file-keeping. It enables users to upload virtually everything they need to the cloud and is especially useful for those quick thoughts you jot down during key work meetings.

* If it's strictly file syncing you need, check out **SugarSync.** A free account gets you 2GB of shared storage between two computers and your phone, accessible from anywhere.

* **Remember the Milk** is one of the premiere apps for to-do listers everywhere, syncing complex lists across multiple platforms with little effort.

* And you can't forget **Skype**, perhaps the best tool for cutting down long-distance charges and communicating via chat, video and audio with far-flung colleagues.

LifeWire.com, 5/17/2018

IT Policies To Protect Your Business

Employees are one of your biggest security holes. There is no foolproof prevention method for human error, which is why employee mistakes are one of the most common causes of a security breach. To reduce potential risks, we've suggested a few IT policies you should implement to protect your business.

Internet

In today's business world, employees spend a lot of time on the internet. To ensure they're not putting your business at risk, you need a clear set of web policies. This must limit internet use for business purposes only, prohibit unauthorized downloads, and restrict access to personal emails on company devices. You can also include recommended browsing practices and policies for using business devices on public wifi.

Email

Just like the Internet policy mentioned above, company email accounts should only be utilized for business use. That means your employees should never use it to send personal files, forward links, or perform any type of business-related activities outside their specific job role. Additionally, consider implementing a standard email signature for all employees. This not only creates brand cohesion on all outgoing emails, but also makes it easy to identify messages from other employees, thus preventing spear phishing.

Passwords

We've all heard the importance of a strong password time and time again. And this same principle should also apply to your employees. The reason is rather simple. Many employees will create the easiest to crack passwords for their business accounts. After all, if your organization gets hacked, it's not their money or business at stake. So to encourage employees to create strong passwords, your policy should instruct them to include special characters, uppercase and lowercase letters, and numbers in their passwords.

Data

Whether or not you allow your employees to conduct work on their own devices, such as a smartphone or tablet, it is important to have a bring your own device (BYOD) policy. If your employees aren't aware of your stance on BYOD, some are sure to assume they can conduct work-related tasks on their personal laptop or tablet. So have a BYOD policy and put it in the employee handbook. In addition to this, make sure to explain that data on any workstation is business property. This means employees aren't allowed to remove or copy it without your authorization.

We hope these four policies shed some light on the industry's best security practices. If you'd like more tips or are interested in a security audit of your business, give us a call at (843)234-9980.

CCG Monthly Trivia -Win $250 Gift Card!

The Grand Prize Winner of last month's Trivia Challenge Quiz is Michelle Schmalfeldt of Ally Management, Inc.! Michelle's name was randomly chosen among those that correctly answered my quiz question from last month: What album is certified as the best-selling of all time with approximately 46 million sales? The answer was c) Thriller.

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

Which 2 Atlantic hurricanes hold the record for the longest time spent as a Category 5 (wind speed of 157 mph or greater)? a) Allen and Maria b) Ivan and Irma c) John & Patricia d) Fred and Wilma
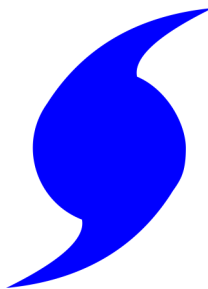
© MARK ANDERSON   WWW.ANDERTOONS.COM

"So you're no good at small talk – just increase the font."