The Tech chronicle

What's New

With the busy holiday season in full swing we want to remind you to stop and enjoy what makes the season special for you. Perhaps you value time spent with family and friends, much needed days off or maybe just eating holiday cookies! Whatever you enjoy doing, don't let this month go by without engaging in something special which will help restore you and set you up for success no matter what is in store over the next decade.

As a reminder our office's holiday schedule is as follows:
12/24/19: Open until Noon
12/25/19: Closed All Day
12/31/19: Open All Day
1/1/20: Closed All Day

From all of us here at Canon Capital Technologies—Merry Christmas to you and your family!

December 2019

This monthly publication provided courtesy of Craig Covington co-owner Canon Capital Technologies

Our Mission

To enhance our customers quality of life and the health of their business.

Cybercriminals Confess:

The Top 4 Tricks And Schemes They Use To Hack Your Computer Network

Most cybercriminals love their jobs. They get to put their hacking skills to the test. In fact, many of them compete against one another to see who can hack a network the fastest or who can steal the most data. They don't care who gets hurt along the way, and in most cases, it's small-business owners who are getting hurt.

Cybercriminals will do anything to get what they want. Some want to create chaos. Some want to steal data. And others want to get straight to the money. These are the people who will hold your data hostage until you pay up. They install ransomware on your computers, and if you don't pay, they threaten to delete your data. This is one of the many reasons why backing up ALL of your data is so important!

So, how do the bad guys get your data? How do they work their way into your network and find exactly what they're looking for? Well, it's much easier than you might think.

They count on you to have no security. This is why cybercriminals go after small businesses. They know a lot of small business owners don't invest in security or invest very little. Even if a business does have security, it's generally easy for a hacker to break through.

Then, all the hacker has to do is steal or destroy data, install malware on the computers and then wait. Because there are so many small businesses around the world, it's just a numbers game for cybercriminals. When you attack every business, you are guaranteed to eventually succeed in the attack.

They let your employees do the work for them. Most cybercriminals aren't going to "hack" into your

Continued on pg.2

Continued from pg.1

network or computer. All the cybercriminal needs to do is get hold of your company's e-mail list and then e-mail your employees.

This phishing e-mail may include a link or an attached file. The e-mail may be disguised as a message from a bank or retailer – or another source your employees are familiar with. The problem is that it's all fake. The cybercriminal wants your employees to click the link or open the file, which will likely install malware on their computer. Once the malware is there, the cybercriminal may gain access to your network and be able to steal critical data.

They exploit outdated hardware and software. If you haven't updated your equipment in years, you leave it open to attack. This is a huge problem in the health care industry right now. Many hospital-based computers are still running Windows XP. Microsoft ended support for Windows XP in 2014, which means the operating system isn't getting any security patches, leaving users vulnerable.

Hackers spend a lot of time looking for vulnerabilities in different types of hardware and software. When they find them, it opens up the general public to those vulnerabilities. In many cases, hardware and software developers work to fix these vulnerabilities and get updates out to users. But these updates only work if you update your equipment. If your equipment is no longer supported by the developers or manufacturers, that's a good indication that it's time to update. While the upfront cost can be high, it doesn't compare to the cost you'll face if hackers get into your network.

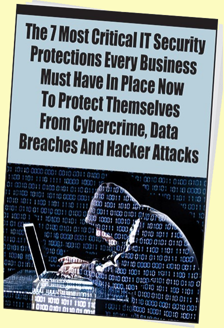
They try every password. Many cybercriminals use password-cracking software to get past your password defenses. The weaker your password, the easier it is to break. In fact, hackers can often break simple passwords in a matter of seconds. This is why it's so important to have strong passwords. Not only that, but all your passwords MUST be changed every three months.

> **"Most cybercriminals aren't going to 'hack' into your network or computer. They'll let your employees do it for them."**

Here's why you need to constantly update your passwords: cybercriminals aren't just going after you. They're going after everybody, including the services you use as a business. If those businesses get hacked, criminals can gain access to countless passwords, including yours. Hackers then can either attempt to use your passwords or sell them for profit. Either way, if you never change your password, you make yourself a target.

Use these four points to your advantage! It is possible to protect yourself and your business from the bad guys. Do everything you can to implement stronger overall security. Prioritize stronger passwords. Keep your equipment updated. And most of all, educate your team about cyberthreats to your business!

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place To Protect Themselves From Cybercrime And Data Breaches


The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the #1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack read this report and act on the information we're providing.

Claim your FREE copy today at www.ccmgtech.com/cybercrime

2 Clues a Leader Is about to Fall

Success may leave clues, but clues often precede failure.

I've been closely following the moral collapse of two different leaders over the past several months and I was struck by how similar the themes are despite the differences in personalities and circumstances.

The situations are tragic for everyone involved, but especially those who trusted these leaders. Those who believed in and supported these leaders are naturally experiencing anger, betrayal and disappointment. The fallout has been ugly, and there is no joy in tracking these moral failures. There are, however, lessons that can help both leaders and those they lead. Two things strike me:

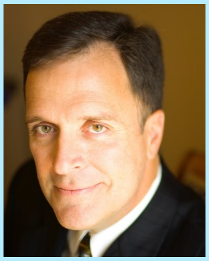
Both leaders were known for having unusual perks and privileges. These weren't the kind of benefits that increased their impact or effectiveness, but that signaled their power and increased their personal comfort. It seems that these entitlements raised the eyebrows of many around them, all whom – apparently – never challenged them. As time went on these little things led to an outright misuse of funds. What started small became a huge problem.

More concerning, the behavior of both was often abrasive or even abusive of those around them. Rage, yelling, name-calling and shaming are examples. I've always wondered why behavior that wouldn't be tolerated by an employee or middle manager is accepted from a powerful leader. The easy answer is that people fear for their jobs and well-being. Ironically, that makes the offending leader think that their behavior isn't that bad. After all, nobody complains, right?

The success or effectiveness of any leader is not a license to privilege or bad behavior. Treating people badly is a major shortcoming of any leader, regardless of skill or success. If it would be unacceptable from someone else in the organization, it should be unacceptable from those in power.

Personal privilege is telling. Although a leader can – because of their schedule, demands and responsibilities – sometimes need resources that others in the organization wouldn't, we should still beware when the infrequent becomes the frequent and then the norm.

While we are often disappointed when a leader fails, we are rarely surprised. In retrospect, there were usually clues. It takes courage for the leader to recognize and change when they are guilty of these things, and it takes even more courage for a friend or colleague of the leader to challenge them to do so.



Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders. He's the best-selling author of Fred Factor *and* The Potential Principle *as well as a noted expert on leadership, team building, and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out his books, his video series, "Team Building: How to Motivate and Manage People," or his website, marksanborn.com, to learn more.*