TECHNOLOGY TODAY

Happy Holidays!

We at IT Support LA wish all of our clients, vendors and everyone who takes the time to read our monthly newsletter a joyous and safe Holiday Season.

Whether you travel or welcome your loved ones into your home for celebration, may the Holiday spirit stay with us all as we take joy in those things most important to us: our family, friends and all of the people we encounter as we see to the business of our lives.

Peace and Joy

December 2019

This monthly publication provided courtesy of Yuri Aberfeld, CEO of IT Support LA.

IT Support LA creates the possibility of focusing on business goals and priorities by providing a trusted technology partnership to small businesses.

Cybercriminals Confess:

The Top 4 Tricks And Sneaky 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 into 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 most small-business owners don't invest in security or invest very little. Even if the 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.

Continued on pg.2

Continued from pg.1

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

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

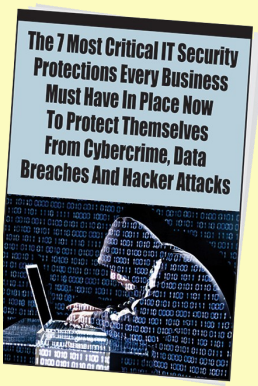
Hackers spend a lot of time looking for vulnerabilities in different types of hardware and software. When they find them, it opens up the general public to those vulnerabilities. In many cases, hardware and software developers work to fix these vulnerabilities and get updates out to users. But these 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.

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 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, you MUST read this report and act on the information we're providing.

Claim your FREE copy today at
https://itsupportla.com/cybercrime/

Insured? Sure You Are...

Insurance is not prevention, of course, but it is also not a cure. At best, it mitigates the damages caused by unexpected and sometimes catastrophic events. We have it for everything these days – even our cell phones. In many ways, it saves us a lot of grief and money. It is very comforting to know that in the event of catastrophe, you are covered.

But ARE you?

Of course, we've all heard of or experienced the horror stories of insurance 'loopholes' designed to protect the insurer, not us. When it comes to cyber insurance, it's still like the Wild West, mostly because people don't understand the policies, or worse and more common, are extremely under-insured. These policies, especially within malpractice insurance, often come with huge deductibles, sometimes double to 4 times the cost of the ransomware and/or data breach fines. Plus, proving your claim can be difficult.

Take the case of Norwegian Aluminum giant Norsk Hydro, which suffered losses between $50 to $71 million following a devastating Ransomware attack. So far, the insurer has paid just $3.6 million, although more claims are pending. But that's a huge multinational corporation with no correlation to your small to midsized company, right?

Not exactly. A company like Norsk Hydro will survive tens, even hundreds of millions in losses. How much loss can your business take before it closes its doors?

If you meet an 'IT Professional' who claims they can keep data breaches and Ransomware from getting in, they are flat-out lying. The true nature of cyber security is to trap the bull in your china shop before it can do much damage, and to immediately execute the plan to repair the damage and restore your operations.

To all of our Los Angeles area readers, we offer a no-strings FREE network security audit. Find out where the weak points in your system are with no obligation. Call us at 818-805—0909 or request your FREE assessment at www.itsupportla.com/free-stuff/free-network-security-assessment/

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. 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. And it seems that these entitlements raised the eyebrows of many around them, all whom – apparently – never challenged them. As time went on, in at least once instance, these little things led to 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 in and outside of business. He's the best-selling author of books like Fred Factor *and* The Potential Principle *and a noted expert on leadership, team building, customer service 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 any of his excellent books, his video series, "Team Building: How to Motivate and Manage People," or his website, marksanborn.com, to learn more.*

3 Ways Your Smartphone Helps You Become Mentally Strong

Sometimes smartphones are a distraction, and other times, they're an amazing on-the-go productivity tool. To get even more out of your smartphone — and to become mentally stronger — try these three things:

Download apps or take online courses to stimulate your brain. There are numerous apps that can benefit your brain. Take Calm, for instance. This app helps you meditate and relax and find your center.

Be smart with social media. A lot of people are focused on building friend lists or mindlessly scrolling through updates. For better mental health, avoid this. Instead, connect with people you genuinely want to connect with — whether it's people in your field or people who inspire you.

Keep it positive. When you're online, keep things positive. Only follow people on social media who contribute positively to your life and the world. Studies show that when we surround ourselves with positivity, we feel much better about ourselves. *Inc., 9/16/2019*

7 Google Search Shortcuts To Save You Time And Make You More Productive

1. Search for specific phrases within quotation marks (""). This way, Google will only return results with your exact phrase in them.

2. Remove certain terms or phrases with a dash/minus (-). This will remove these words from your search.

3. Add a tilde (~) to your keyword to include the keyword AND synonyms of that keyword.

4. Add "site:" followed by a website and keyword to your search to search that keyword only within a specific website.

5. Find out who is linking to any given website with "link:" This is great when you're doing additional research or looking to improve your search engine optimization (SEO).

6. Search within a specific time frame with two periods (..). This can help you narrow down search results to the most timely.

7. Use "related:" to search for terms or websites that are similar to the one you're already searching for. *Small Business Trends, 5/17/2019*

5 Business Trends To Watch Out For In 2020

No AI Just Yet – There's a lot of talk that artificial intelligence is going to take over customer service. While AI support exists, it still cannot match the power of human interaction.

Personalized Customer Service – Coming off that first trend, people don't want to be treated as numbers. Businesses that offer personalized service will find more success.

User Reviews Are More Important Than Ever – This is the first thing people look at before making a buying decision. They want to hear from real people. This is why good, personalized service is so important – it earns you good reviews.

Businesses Recognize Employee Happiness – It's as simple as this: the happier the employees, the more productive they are. More businesses are realizing this and changing their workplaces in response.

More Remote Workers – Thanks to Internet access virtually everywhere, it's easier for people to work from wherever – and this plays a huge role in employee happiness, too! *Freshworks, 8/11/2019*