TECHNOLOGY TODAY

Save The Date!

January 14, 2020. That's the day Microsoft will end its extended security support for Windows 7. I know from fresh first-hand experience that there are business owners and IT 'professionals' who just don't care. Windows 7 has been extremely popular, and 10 is still not the most stable platform. So what really happens next January 14?

That's the date when there will be no more security patches and updates for 7, which is how Microsoft helps protect your system against new attack methodologies, whether it be simple hacking or new strains of Ransomware.

That's the date cyber crooks are waiting for. Trust me on this: Criminals are paying a lot more attention to that date than most users, because there will be no protection against the next attack. They are poised and ready to pick off the weakest of the herd.

DO NOT fool yourself into ignoring this date. For a free analysis of the best way to make the change, give us a call at 818-797-5300.

July 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.

Top Ways To Protect Your Business From The #1 Security Threat You Face

Today, cybercrime is more than a potential threat facing your business. It's an unavoidable force of nature.

"It's just like preparing for hurricanes, earthquakes or any type of natural or man-made disaster that could create business continuity issues," says Theresa Payton, the Fortalice Solutions CEO and former White House CIO, in an interview with *Cybercrime Magazine*. "[It's the] same thing with a digital cyber-event." For many of us, it's easy to imagine these kinds of things happening to "the other guy" and not us. The problem is that cybercriminals go after everyone. They cast a wide net because that gets results.

In fact, according to Roger A. Grimes, 11-year principal security architect for Microsoft and cyber security columnist and speaker, "Eventually every company is hacked." After decades consulting for many businesses, he's come to the conclusion that "every company is completely and utterly owned by a nefarious hacker or easily could be."

Owners of small and midsize businesses might imagine that – lucky us! – we don't have enough cash to justify some faceless hacker's effort. We'd be wrong. The reality is around half of cyber-attacks go after small businesses. These don't really get reported by the media. They're not as flashy as a cyber-attack against a big bank or retailer. But it's the attacks against small businesses that do the most damage. One 2016 study found that 60% of small businesses hit with a cyber-attack closed within six months.

Thankfully, it's not all bad news. While some business owners have no clue what cyber security they have in place, others are looking for ways to shore up their

Continued on pg.2

Continued from pg.1

businesses. There are steps you can take to keep the bad guys out.

Two of the best ways to do that are to simply keep all your software up-to-date and keep your team educated about the threats. As Grimes puts it, "The two most likely reasons you will get exploited are due to unpatched software or a social engineering event where someone is tricked into installing something they shouldn't … It would be a stretch to claim every other exploit type in the world, added together, would account for 1% of the risk."

How can you keep your software up-to-date? You can actually automate a lot of it. There are several easy-to-use tools built just for this. Many of them also let you manage your software across your entire network from one set location. Say goodbye to jumping around and coordinating updates. Even better, there are many platforms capable of updating themselves. You just want to keep a close eye on them.

> **"60% of small businesses hit with a cyber-attack closed within six months."**

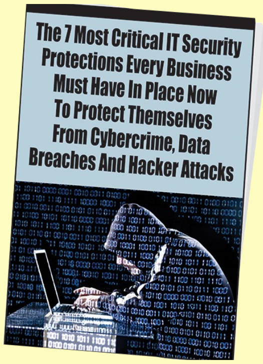
More than that, it's always a good idea to put strong company policies in place. You want to be clear about your security and help inform employees about the dangers posed by malicious files and e-mails, among other things. Take time to educate them on the threats that are out there. And keep the education ongoing, because the threats are ongoing. The bad guys are always looking for new ways to break in.

And don't forget about accountability. Keep the conversation going and talk to your employees about what they know about cyber security. Some businesses go so far as including cyber security training in their onboarding. Education is everything.

Finally, you MUST partner with a highly trained, security-focused managed service provider or other IT organization dedicated to keeping you protected from these constant threats. Some businesses try to do it on their own only to realize they don't have the resources. Others think they need an entire in-house IT team to handle all of these threats.

But the fact is, by outsourcing the work, you save money while keeping out the bad guys optimizing key parts of your network and software. It's a win/win. It's all about being proactive. When you have a group of experts working every day behind the scenes, cyber security stays top of mind in your organization, whether *you're* thinking about it or not. Really, it's one less thing you have to stress about.

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



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

www.itsupportla.com/sittingduck/

Do You Mine?

You may be mining and not even know it. While Ransomware is like an in-your-face armed robbery, the subtle back-door approach is through illicit cryptomining where crooks burrow unnoticed deep into your system and steal your Central Processing Unit's (CPU) power to mine Bitcoins and other online currencies.

Cryptomining is the verification of billions of worldwide monetary transactions. Once a certain block of data is fulfilled, the miner receives cryptocurrency, such as Bitcoins, although the currency of choice for illicit mining is the more untraceable 'Monero'. Since the emergence of the Coinhive malware in 2017, this crime has been on a steady rise.

What you don't know CAN hurt you!

You may think, "If I don't even know it's happening, what's the problem?". The problem is that Time Is Money, and by illegally using up your network's computing power to further *their* success, not yours. This will cause your network to run slower, and as with any machine that is constantly operating at its highest capacity, will shorten the life of your CPU.

Even if that may not seem like a major cause for concern, someone lurking in your network eating up your computing power is like having someone roaming around your house in there middle of the night. While you're upstairs asleep, they're downstairs eating your food, watching your TV and using your phone.

How do these illicit miners get in? It's easier than Ransomware—all you have to do is visit sites on the web, and not even 'shady' websites: In 2016, several Showtime websites were caught running a script that allowed them access to their visitors' CPUs for illicit mining.

A thorough security scan will uncover these parasites within your system. IT Support LA offers all of our readers a free scan by calling us at 818-797-5300, or by visiting us at: www.itsupportla.com/free-stuff/free-network-security-assessment/

Learn Like A Leader

Disraeli once said that all other things being equal, the person who succeeds will be the person with the best information. For leaders, learning isn't an academic pursuit. Leaders don't just learn to know more; they learn to be more. Learning is a critical means to this important end and how they find the ideas that fuel their ongoing improvement. Here's how the best leaders do it.

1.They make investigation and inquiry a way of life. In their classic book *Leaders: Strategies For Taking Charge*, Warren Bennis and Burt Nanus famously said that leaders are readers. My friend Bill Byrne was on the cover of *Fortune* magazine as one of America's 1% wealthiest entrepreneurs. He credits much of his success to his 15/15 program: he read 15 hours a week for 15 years.

2. They ask more and better questions of more and different people. The best leaders emulate the ancient city of Alexandria, where no ship was allowed to enter the port without surrendering its books to be copied. They query everyone who passes into their lives, hoping to add material to their learning arsenal.

3. They think for themselves. Just because the best ask lots of questions doesn't mean they accept what they learn at face value. Learn to consider what you learn with a healthy dose of skepticism.

4. They choose critical thinking over the convenience of conjecture. An important characteristic of the best is that they are the people who seek the truth. They want to act on factual information rather than speculation and conjecture. They ask, "How do I know this is true? Who says? How does it affect me?"

5. They learn in future tense. Study for the future, not the past. Develop your learning agenda on what you will need to know to be successful, not what you used to need.

6. They learn the most important stuff the fastest. When an area of knowledge becomes important, a modern expert is able to recognize the importance of that knowledge and glean what's most important from it as fast as possible.

7. They design their own continuing education program. Unlike most people, the best design their own curriculum on an ongoing basis.

8. They listen to their intuition. Intuition is a great bunk detector. As Robert Bernstein, former chairman of Random House Publishing, says, "In an age of information, only intuition can protect you from the most dangerous individual of all: the articulate incompetent."

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.*

Beware! 60% Of Businesses Lose Their Data Through These Breaches

When you're thinking about cyber security, you're usually thinking about your PCs, servers and precious data. But what if your printer is a vulnerability?

Well, it is, according to the Global Print Security Report, stating that 60% of businesses suffered a print-related data breach within the last year. While these breaches may not cost too much, they can still pose quite a problem. Printers are vulnerable not only to all the threats associated with IoT devices but also to those linked to hard-copy output. It's vital that we find ways to secure our print infrastructure for the long haul as we move forward.
SmallBizTrends.com, 2/24/2019

Google Tricks To Make Your Life Easier

The Google search bar is even more useful than most people realize. You can use it as a timer or stopwatch by entering "set timer for X" for instance. If you type "sunrise in X" or "sunset in X," you can pinpoint the exact moment the sun will rise or set in a given location. You can quickly convert between currencies, or use it as a powerful calculator. Type "etymology + word" to discover its origin, or enter "query + filetype:extension" to search for results of a specific file type. Then there are the Easter eggs. Type "do a barrel roll" to see what happens, or "fun facts" or "I'm feeling curious" to learn something new.

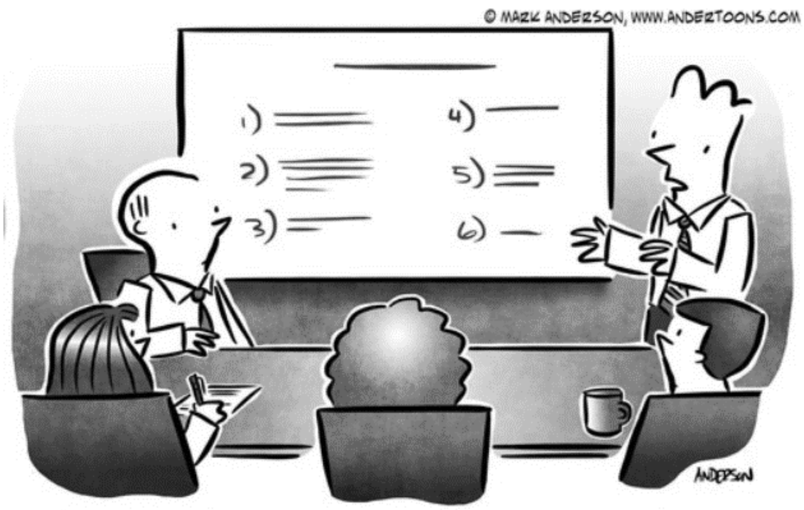
Leadership Lessons Learned From The First Free Solo Climb Of El Capitan

Whether you think Alex Honnold's attempt to scale the massive El Capitan alone and with no ropes is foolhardy or transcendent, we all can learn a thing from his incredible feat. Honnold knew that to cement his legacy, he'd have to top the less intense (but still insane to any normal person) "free solo" successes of his past. So he prepared for two full years to complete the 3,000-foot ascent. As leaders, we should all identify with this – what will we leave behind when we're gone?

We can also learn from his thorough preparation. We need to think beyond "What will it look like to achieve our vision?" We need to think, "What does it mean for us to have a perfect run today?" Take the guesswork out of the equation as much as possible.

Once Honnold had his ideal outcome in mind, he practiced, climbing El Cap over and over and over again. In addition to full routes, he'd drill challenging sections repeatedly until it felt impossible to make an error. For most leaders, making a mistake won't lead to death. But keeping this "deep practice" mentality in mind is essential for doing something truly great. None of us are going to have a Nat Geo documentary made about us, but we certainly can leave our mark on the world before we go. *Inc.com, 3/26/2019*

© MARK ANDERSON, WWW.ANDERTOONS.COM



"You're right, it is easier said than done. That's why I said it; because it's easy. Try and keep up."