TEKConn

December 2019 NEWSLETTER

MAKE THE MOST OUT OF THE HOLIDAY SEASON

ASK FOR HELP Delegate and communicate what you need to complete end-of-year projects or tasks.

TAKE A BREAK When you need rest, take it. Lack of rest is a major cause of burnout.

EAT HEALTHY Sugar and carbs can seriously bring you down. Focus on healthy foods for a healthy mind.

DON'T GO INTO 'VACATION MODE' TOO EARLY As much as it is tempting, don't get distracted by the upcoming holidays and start to neglect your tasks.

WHAT'S NEW

HAPPY HOLIDAYS!

May the spirit of the Season fill your home with peace, joy and love. TEKConn wishes you a Happy Holidays!

ANNOUNCEMENTS

Congratulations to Christina Adorno, for moving to the Managed Consultant department.

We're giving away a free cyber security assessment! (see page 3 for details)

OUR MISSION

To empower our clients to be successful, by leveraging technology to help achieve their business goals.

This publication is provided courtesy of Stephen Dike, CEO of TEKConn.

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

CYBERCRIMINALS CONFESS

INSIDE THE MIND OF A CYBERCRIMINAL

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.

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.

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.

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!

Learn more and sign up for weekly email security tips at

www.tekconn.com/weeklysecuritytips

HOW A SMARTPHONE HELPS YOU BECOME MENTALLY STRONG

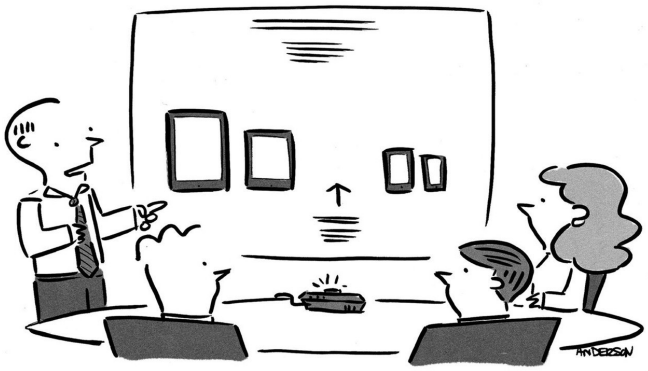
GIFTING YOURSELF A NEW DEVICE?

"Technology can either drain your mental strength or build your mental muscle, depending on how you use it."

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.*



"We believe there's room in the marketplace for a revolutionary new device somewhere between the 7-inch mini tablet and the 6.3-inch mega smartphone."

LAST MONTH FOR WINDOWS 7

TIME IS RUNNING OUT

On January 14, 2020, Microsoft will end support for Windows 7. That means no more updates, security or otherwise, will be offered by the company from that date forward. The clock's been ticking on Windows 7 ever since Microsoft ended mainstream support back in 2015.

Not only will Windows 7 become progressively more unstable as modern hardware outpaces the software, but cybercriminals are certain to flock to the operating system after support shuts down, eager to pick off easy targets left vulnerable by the lack of ongoing security updates. If you're running a business, this is a risk you can't afford. It's time to contact your IT provider and make preparations to upgrade, preferably well in advance of the January 14 deadline.

Whether you're planning on transitioning to Windows 10 or moving on to an alternative operating system, this is a task that needs priority. If you're one of the businesses still on the outdated Windows 7 platform, consider this your wake-up call: time is nearly up for your trusty, tried-and-true operating system.

WIN FREE CYBER SECURITY ASSESSMENT ($5000 Value)

To Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive security assessment to uncover loopholes in your company's IT security.

After the assessment is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast..

Must be a company over 10 users based in New York City, Southern Connecticut, Westchester County, NY or Northern NJ. Winner will be notified 12/30/2019.

Register by Contacting Us by 12/24/2019

Call 800-955-0231 or Email cyber@tekconn.com

HAVE YOU MET SOMEONE WHO'D REALLY VALUE FROM USING TEKCONN?

We appreciate your trust in making an introduction to us and we're happy to compensate you **$250** for each successful referral that becomes a client.

VISIT WWW.TEKCONN.COM/REFERRAL

5 BUSINESS TRENDS TO WATCH OUT FOR IN 2020

1. 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.

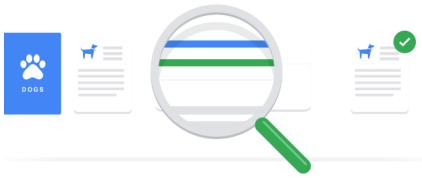
2. PERSONALIZED CUSTOMER SERVICE – Coming off that first trend, people don't want to be treated as numbers. Businesses that offer personalized service will find more success.

3. 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.

4. 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.

5. 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

GOOGLE SEARCH SHORTCUTS TO SAVE TIME & MAKE YOU MORE PRODUCTIVE



- Search for specific phrases within quotation marks (""). This way, Google will only return results with your exact phrase in them.
- Remove certain terms or phrases with a dash/minus (-). This will remove these words from your search.
- Add a tilde (~) to your keyword to include the keyword AND synonyms of that keyword.
- Add "site:" followed by a website and keyword to your search to search that keyword only within a specific website.
- 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).
- Search within a specific time frame with two periods (..). This can help you narrow down search results to the most timely.
- 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