Central Texas Technology Solutions
Your Business Partner

Technology Monthly Newsletter
May 2018

Change them often, keep them private, and never share them with anyone!

World Password Day is May 3rd, and seeing as password security is one of the most important parts of using an online account, we wanted to share with you a few tips to keep your accounts and your business secure:

- Use different passwords on different systems and accounts.
- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Use a combination of capital and lowercase letters, numbers, and special characters.
- Don't use words that can be found in any dictionary of any language.
- Develop mnemonics (or spoken memory tricks) such as passphrases for remembering complex passwords.
- Consider using a password manager program to keep track of your passwords.

CTTS is of the firm mind that you should never underestimate the importance of network security best practices--particularly password security. Secure your business today, reach out to us at (512) 388-5559.

This monthly publication provided courtesy of CTTS, Inc.

The Shocking Truth Behind Cybercrime Threats

And What You Can Do About Them Now

Today's technological innovations have empowered small businesses to do things that would have been utterly unimaginable even 15 years ago. To remain competitive in a constantly shifting landscape, we've become more dependent on software and hardware to house even the most basic structures of the companies we run.

Meanwhile, these technologies are evolving at breakneck speed. Every day, there's a slew of new devices to consider, a pile of new updates to install and a new feature to wrap our heads around. Every morning, we wake up and the digital world is thrillingly new.

But all over the world, there's an insidious network of criminals keeping up with this insanely rapid pace of progress. With every new security measure designed to protect our digital assets, there are thousands of hackers working around the clock to determine a new way to break through. An estimated 978,000 fresh new malware threats are released into the world each day. The term "up to date" doesn't mean much anymore in the wake of new developments arriving minute by minute.

There's a price to pay for the increased efficiency and reach enabled by the digital age. We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a crippling large-

scale cyberattack, with criminals lifting millions of dollars in customer data and digital assets. Equifax, J.P. Morgan, Home Depot, Yahoo!, Verizon, Uber and Target – these narratives are so commonplace that they barely raise an eyebrow when we read about them in the news.

Most business owners wrongly assume that these incidents have no bearing on their own companies, but these high-profile incidents account for less than half of data breaches. In fact, according to Verizon's 2017 Data Breach Investigations Report, 61% of attacks are directed at small businesses, with half of the 28 million small and medium-sized businesses (SMBs) in America coming under fire within the last year.

> **"We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a large-scale, crippling cyber-attack..."**

It's hard to imagine how you can possibly protect yourself from these innumerable threats. Statistically, you can be all but certain that hackers will come for your data, and there's no way to know what new tool they'll be equipped with when they do.

You may not be able to foresee the future, but you can certainly prepare for it. With research, education and resources, you can implement a robust security solution

into the fabric of your business. That way, you can send hackers packing before they get their hooks into the organization you've spent years building from the ground up.

One huge leap you can make right now for the security of your business is to simply realize that cyber security isn't something you can install and leave alone for years, months or even days. It requires regular updates and the attention of professionals to ensure there's no gap in your protection. There are new shady tactics being used by criminals every day, but there are also fresh protocols you can use to stave them off.

Small business owners assume that since they don't have the resources of a Fortune 500 company, they don't have the means to invest in anything but the barest of security. Obviously, hackers know this and target SMBs in droves. The bad news is that most businesses' paper-thin barriers won't save them in the event of a crisis. The good news is that it doesn't take thousands upon thousands of dollars to implement a security system that will send the hackers packing.

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

978,000 NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious reputational damage, 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.CTTSonline.com/Security

How to Spot Three Forms of Phishing Attacks

Do you have ways to secure your business? Phishing attacks come in various shapes and forms. Here are some of the most common ways that hackers will use elaborate phishing attacks to scam your business, including phone calls, normal emails, and social media.

Phishing Calls
These messages are designed to target specific employees within your organization to coax information out of them. You should always cross-check contact information before giving up any information to anyone. When in doubt, simply don't give away anything important.

Phishing Emails
You should look for spelling errors or incorrect grammar, falsified information, and just about anything else that doesn't necessarily belong. Still, phishing messages have become more elaborate than ever before, so make sure to consult security professionals like CTTS if you have any doubts.

Phishing Accounts
A hacker can take on any identity they want, which makes phishing accounts even more difficult to identify--particularly if they have taken the identity of someone you might know. In general, just try to avoid messages that come out of the blue, and use your previous interactions with the sender to see if they are (or aren't) who they claim to be.

Overall, just ensure that you approach potential phishing incidents with skepticism. To learn more about how you can secure your company, reach out to CTTS at (512) 388-5559.

The Top 3 Business Lessons I Learned from Robert Herjavec

By Josh Wilmoth

Recently I had the privilege to meet the leading shark on ABC's Shark Tank, Robert Herjavec, and hear him speak on his experiences that lead him to be the entrepreneurial leader he is today. Herjavec's motivational business advice has inspired me and so I'd like to share with you my top 3 takeaways:

1 KNOW YOUR NICHE

As you build your customer base, you'll find that your selling value proposition varies from customer to customer. In order to know the value proposition, one must understand the customer and their needs inside and out. What are their values? What are their long-term and short-term plans? When you continually add more value to the services or products offered, it creates a deeper value within the company itself. Your company's niche is defined by the types of Clients you have and how you help them meet their goals.

2 KEEP THREATS IN CHECK

As CEO and Founder of one of North America's fastest growing technology companies, Herjavec Group, we asked Herjavec what he considers the biggest cybersecurity threat. His answer? Ransomware. This malicious software that uses encryption to hold data for ransom is not a new concept and with numerous new variants of ransomware being developed every day, it is a continually growing problem. "The amount of threat at the corporate level is immense, and it's not going away anytime soon," Herjavec says. From attacks on utilities companies to mobile phones, the best course of action in avoiding this devastating reality is prevention. One way to keep this threat in check is to have a Cybersecurity Assessment performed to discover where your business stands. This includes a Dark Web scan to determine whether your domain is on the dark web before any damage is done. For a free Dark Web scan, visit our website: https://www.cttsonline.com/darkweb/. For a free Cybersecurity Assessment call CTTS today: (512) 388-5559

3 RISE ABOVE THE CIRCUMSTANCES

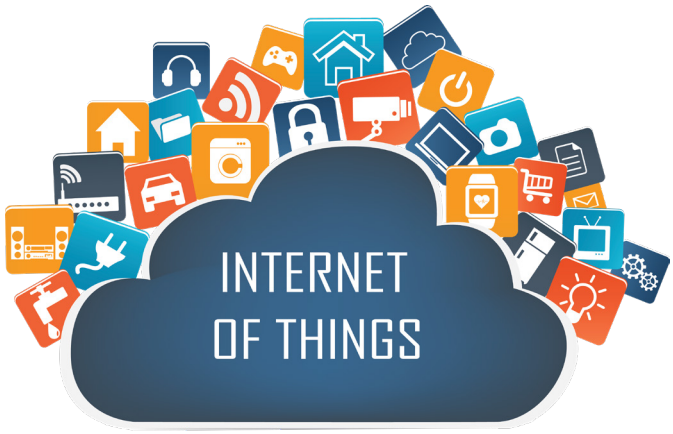
We're all either in a situation, coming out of a situation, or headed into a situation, and you can't always determine which of these your life is in at the moment. What you can do is decide how to react to that situation. You can feel sorry for yourself and do nothing when times get tough, or you can choose to rise above your circumstances. Don't feel sorry for yourself and you won't be a victim. Herjavec says, "A true entrepreneur has the confidence to jump out of an airplane and figure out the parachute on the way down." Be open to change, and though you might need to change quite a bit over the years to be successful, never ever give up.

3 Big Trends Businesses Need To Adopt

When the online publication *Small Business Trends* surveyed nearly 500 small and midsize-business owners across the country last February, they found that technology has become more important than ever in companies of all sizes.

Though CRM is often an expensive and lofty goal for time-strapped businesses, it drastically increases growth once it's implemented and understood. In fact, *Small Business Trends* found that "growing SMBs are twice as likely as their stagnant counterparts to rely on CRM in their daily lives." Along with these cohesive programs, synchronizing business data across platforms is becoming a priority as well, especially when providing a holistic view of key customer information.

Even artificial intelligence has begun to crop up in the small business market, albeit slowly. Still, it's clear that the fastest-growing businesses are using automation and predictive sale forecasting nearly twice as much as their stagnant counterparts. *SmallBusinessTrends.com, 2/14/18*



The Internet Of Things: Are You Okay Playing Offense?

Adjusting your home's thermostat and hot water heater back to normal temperatures as you board a plane on your way home isn't just cool, it's incredibly handy. However, the network of these and other connected devices – often called "the Internet of Things" (IoT) – poses one of the biggest security problems of the modern era. Most people think about changing their computer password regularly and their ATM PIN occasionally, but they almost never consider changing the password the programmable thermostat ships with from the factory, meaning that anyone who can access the manual has access to your thermostat.

Usually, attackers who target IoT devices don't want to cause you a problem. Instead, they use your device along with 20,000 other thermostats as "soldiers" to battle against a website or e-mail server. By flooding these sites with traffic, they can shut them down or stop your e-mail server from delivering your messages.

You should adopt a strict offensive posture against these types of threats in your life and business. If there is even a suspected problem with one of your IoT devices, pull the plug. Your heater may be cold when you get home, but at least your data will be safe.

"How come Lewis and Clark didn't just use MapQuest?"

How Are We Doing?

Let us know what you think of CTTS: bit.ly/CTTS-Experience

Follow us on Social Media!

- Twitter: bit.ly/CTTS-Twitter
- Facebook: bit.ly/CTTS-Facebook
- Instagram: bit.ly/CTTS-Instagram
- LinkedIn: bit.ly/CTTS-LinkedIn
- YouTube: bit.ly/CTTS-YouTube