PALMTECH
I.T. SOLUTIONS FOR BUSINESS

THE PALMTECH TIMES

PalmTech Computer Solutions October 2022

Password Hygiene

Your password is the key to your online identity and personal information.

Just like you wouldn't share your toothbrush with anyone, you shouldn't share your passwords. Keep them protected by choosing a good one — long, complex and unique.

Also, saving passwords in your browser is a huge security risk! If your browser is ever compromised, all your passwords will be exposed. Try maintaining good password hygiene by using a password manager and other such solutions.

Need help finding the right password manager? Contact us today at 561-969-1616.

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Keep Your Information Secure

By Using Strong Passwords

We use passwords for just about everything. Most of us must enter a password to get into our computers and then enter other passwords to access our email, social media profiles, databases, and other accounts. Even our cell phones and tablets can and should be password protected. In fact, if you aren't securing all of your devices and accounts with passwords, you should start. It could help prevent your business and personal information from becoming compromised.

Why Passwords?

We use passwords to ensure that those who don't have access to our accounts, can't get access. Most of our devices hold large amounts of personal information. Think about the potential harm someone could do if they gained access to your cell phone. They would immediately be able to see your contacts, pictures, and applications. They might even be able to log in to your email where they could obtain your banking information. If this type of access falls into the wrong hands, it could be detrimental to your life. Passwords offer the first line of defense to prevent others from obtaining sensitive information.

This becomes even more important if you own a business. Each of your employees should be utilizing strong passwords to access company information. If your business is not using passwords – or is using simple passwords – you could be opening yourself up to hackers and cybercriminals. If a cybercriminal gains access to your company's private information through a weak password, they will gain access to customer information, damaging your reputation and opening you up to lawsuits. That being said, everyone within your business needs to utilize complex and unique passwords.

Making A Strong Password

Not all passwords are created equal. When it comes to making a strong password, you must think about it. If you use a password that you can't remember,

continued on page 2

then it’s essentially useless. If you use a password that’s too easy to remember, your password probably won’t be strong enough to keep cybercriminals out. Your password should be long, have a mix of lowercase and uppercase letters, use numbers and special characters, have no ties to personal information, and should not be a word from the dictionary.

In the grand scheme of things, it’s not enough to just create complex passwords. They also need to be unique. In addition to this, you should use a different password for each and every one of your accounts to help maximize effectiveness. Think about it this way: If you use the same password across your business email accounts, social media accounts, and bank accounts. If someone decrypts the password for your Facebook page, they now have the password for more valuable accounts. The cybercriminal could try to use that same password to gain access to more critical accounts. It’s a dangerous game that can be avoided by using unique and complex passwords for every account you use.

Remembering All Of These Passwords

You may be worried about remembering all of your passwords if you have to create a unique one for each of your accounts. Your first thought may be to write them down, but that might not be the most secure option. If someone gets their hands on your little black book of passwords, they’ll immediately gain access to all of your accounts with a handy directory showing them exactly where to go. Instead, you should utilize a password manager to help keep track of all of this sensitive information.

> **“You should use a different password for each and every one of your accounts to help maximize their effectiveness.”**

With a password manager, you only have to worry about remembering the master password for your password manager. All of your other passwords will be securely hidden. Password managers also give you the option to create random passwords for your accounts to bolster their security. That way you can have the most complex password possible without worrying about forgetting it. Additionally, password managers can also help you remember the answers to security questions and more so that you never get accidentally locked out of one of your accounts. They’re easy to use, convenient and secure.

Passwords are an important part of your cyber security plan. Make sure you and your employees are using complex and unique passwords. It can also help to implement some training so your employees understand the importance of secure passwords. When used correctly, passwords will help deter any would-be cybercriminals from accessing your sensitive information.

If you need more information on cybersecurity best practices, contact us at 561-969-1616 or info@palmtech.net!

PALMTECH
I.T. SOLUTIONS FOR BUSINESS
TREAT YOUR PASSWORD LIKE A TOOTHBRUSH.
CHOOSE A GOOD ONE, DON’T SHARE IT AND CHANGE IT OFTEN.
KEEP UP WITH
#CYBERHYGIENE
www.palmtech.net
561-969-1616

The Secret To Job Happiness Might Be Who You Work With

If I were to ask you where job happiness comes from, how would you respond? Conventional wisdom says that your happiness at work comes from one of these four sources:

- “follow your passion” (what)
- “play to your strengths” (what again)
- “do something with purpose” (why)
- “live your values” (how)

It’s also true that 95% of career-success books follow one of these lines of advice – but what if they’re wrong?

What if your job happiness comes not from ***what*** you do, ***why*** you do it, or ***how*** you do it … but instead comes from the people around you? Your bosses, peers, and subordinates all can play a huge role in your job happiness. Let me give you a few examples that support this idea.

I know a talented MBA who works for a public-private partnership with a mission that would make any do-gooder proud. He is planning to quit that job because he feels the firm’s leadership disregards the human element of their work, bickers internally, and lacks integrity. I’m reminded of a well-researched fact I learned during graduate school: employees don’t quit jobs, they quit supervisors.

My firm once did a pro-bono project for the US Navy where I observed a grueling exercise routine. I asked one of the instructors why anyone would sign up for that – and honestly, I think I expected a response about patriotism. Instead, he explained that they join to be part of a camaraderie. It was a community where they had each other’s backs.

If the secret to job happiness is who you work with, then that means you should plan your career differently. Rather than meditate for too long on your passion and purpose, you could think about the kinds of people you really want to be around. Who do you want to be your customers? Who do you want to be your colleagues? What sorts of personalities?

Rather than sourcing job titles, you could be sourcing bosses and colleagues you want to work with. I recently told a young job-seeker, “Don’t just go find any old job in your industry. The most important thing you can do right now is to find the right boss – to hire your boss. Hire the best boss in your industry – someone who will teach you, invest in you, tell you the truth, give you real feedback, put energy into helping you discover your ideal path, and then help you achieve it.”

Once you land your new dream job, be mindful of the time you are spending with the people you want to work with. Don’t just track your goals and results, track the time you are spending working with the specific people in your company who you want to work with.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times *best sellers. He stays active in his community and has advised many government officials.*

Watch Out For These 4 Employee Cyberthreat Traits

To succeed in today's modern competitive business landscape, you need to understand the strengths and weaknesses of your employees. This will equip you to identify areas where employees may need further training, including cybersecurity awareness.

Are you sure that your employees can resist threats and prevent cyberattacks? Certain employee traits can indicate a lack of cybersecurity knowledge or awareness. For example, individuals who regularly click on phishing emails or fall victim to social engineering attacks are likely unaware of the dangers of these threats. Similarly, employees who do not adhere to cybersecurity best practices, such as using strong passwords, may also demonstrate a lack of awareness or motivation.

If you notice these behaviors in your employees, you must empower them with the latest cybersecurity training and best practices. By doing so, you can help protect your business against the dangers of cyberattacks. Below, we attempt to categorize the most common employee traits so that you can identify individuals who require additional attention.

Traits To Watch For — Although there are numerous ways to classify employee traits, we believe the four listed below cover the most common character traits.

The skeptic: Skeptical individuals believe that a cyberattack will never happen to them. They don't understand the significance of regularly changing their passwords or using two-factor authentication. This callous behavior is precisely what cybercriminals exploit to attack the organization. They have a high success rate when businesses and employees don't take the necessary safety precautions.

Remember, cybercriminals are out there and are very good at staying under the radar, making it difficult to spot them if you're not actively looking for them.

The procrastinator: Cybersecurity procrastinators know they are critical to preventing hackers from infiltrating systems, but they'll worry about finally connecting to your virtual private network (VPN) or deploying that security patch tomorrow.

Those with the procrastinator cybersecurity trait also have a love-hate relationship with the dozens of red bubbles on their apps and software. They know that if left unchecked, the situation could quickly spiral out of control, but they will prioritize other tasks and wait until "the next day" to take care of the issue.

The naïve: Although naivete is not synonymous with foolishness, those who are inexperienced in cybersecurity might trust too easily.

Do you know people who leave their computers unlocked when they go out for lunch? Or the remote worker who uses the free Wi-Fi at coffee shops? Some individuals even write their passwords on post-it notes.

While it may seem to this type of employee that good people surround them, the threat might be sitting right next to them.

The employee with good intentions: If cybersecurity best practices were an exam, this type of employee would get an A+. They are cautious of emails with links or attachments, use complex passwords to deter hackers, and are always informed of the latest threats. However, even the employees with the best of intentions can be targeted by a cybercriminal without knowing it, which is why providing your team with the latest cybersecurity awareness training is crucial.

Conclusion: It's essential for any business to know its employees well. After all, they are the lifeblood of the company. Moreover, good employees help drive a business forward, whereas careless employees can drag it down.

It's important to remember that each employee is an individual with unique skills, traits, and motivations. It's up to you to ensure that these individual traits are being put to good use and that your employees receive regular security awareness training to help them learn and practice good cyber hygiene.

Don't worry if you don't know where to begin. The experience and expertise of a specialized IT service provider, like us, may be just what you need. Contact us today at **561-969-1616** (info@palmtech.net) for a no-obligation consultation to see how easy we can make security awareness training.

9/25 © 2018 Maria Scrivan Dist. by Tribune Content Agency, LLC.

CartoonStock.com