PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions May 2021

What's New?

As the CEO of PalmTech, I understand how managing the operations of a business can be overwhelming. With technology constantly evolving, it can be frustrating trying to keep up.

With this in mind, I began writing blog articles with the intention educating and informing our readers.

My hope is that this helps provide clarity and understanding.

I'd love your feedback, so please email me at info@palmtech.net, along with any topics related to technology that you'd like more information on.

I look forward to hearing from you!

www.palmtech.net/blog/

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.

How To Make Cyber Security An Ingrained Part Of Your Company Culture

Your employees are your first line of defense when it comes to protecting your business from cyberthreats. Human error is one of the single biggest culprits behind cyber-attacks. It comes down to someone falling for a phishing scam, clicking an unknown link or downloading a file without realizing that it's malicious.

Because your team is so critical to protecting your business from cyberthreats, it's just as critical to keep your team informed and on top of today's dangers. One way to do that is to weave cyber security into your existing company culture.

How Do You Do That?

For many employees, cyber security is rarely an engaging topic. In truth, it can be dry at times, especially for people outside of the cyber security industry. It boils down to presentation. That isn't to say you need to make cyber security "fun," but make it interesting and engaging. It should be accessible and a normal part of the workday.

Bring It Home For Your Team. One of the reasons why people are often disconnected from topics related to cyber security is simply because they haven't had a firsthand experience with a cyber-attack. This is also one reason why many small businesses don't invest in cyber security in the first place – since a cyber-attack hasn't happened to them yet, they don't think it will. Following that logic, why invest in cyber security at all?

The thing is that **it will eventually happen**. It's never a question of **if**, but **when**. Cyberthreats are more common than ever. Of course, this also means it's easier to find examples of these threats you can share with your team. Many major companies have been attacked. Millions of people have had their

continued on page 2

personal data stolen. Look for examples that employees can relate to, names they are familiar with, and discuss the damage that's been done.

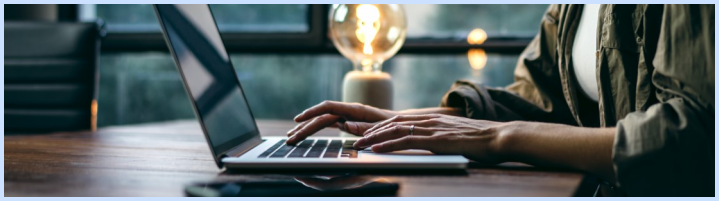
If possible, bring in personal examples. Maybe you or someone you know has been the victim of a cyber-attack, such as ransomware or a data breach. The closer you can bring it home to your employees, the more they can relate, which means the more likely they will listen.

Collaborate With Your Employees. Ask what your team needs from you in terms of cyber security. Maybe they have zero knowledge about data security and they could benefit from training. Or maybe they need access to better tools and resources. Make it a regular conversation with employees and respond to their concerns.

Part of that can include transparency with employees. If Julie in accounting received a phishing e-mail, talk about it. Bring it up in the next weekly huddle or all-company meeting. Talk about what was in the e-mail and point out its' identifying features. Do this every time phishing e-mails reach your employees.

Or, maybe Jared received a mysterious e-mail and made the mistake of clicking the link within that e-mail. Talk about that with everyone, as well. It's not about calling out Jared. It's about having a conversation and not placing blame. The focus should be on educating and filling in the gaps. Keep the conversation going and make it a normal part of your company's routine. The more you talk about cyber security and the more open you are about it, the more it becomes a part of the company's culture.

> **"For the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture."**



Keep Things Positive. Coming from that last point, you want employees to feel safe in bringing their concerns to their supervisors or managers. While there are many cyberthreats that can do serious damage to your business (and this should be stressed to employees), you want to create an environment where employees are willing to ask for help and are encouraged to learn more about these issues.

Basically, employees should know they won't get into trouble if something happens. Now, if an employee is blatantly not following your company's IT rules, that's a different matter. But for the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company's' culture.

Plus, taking this approach builds trust, and when you and your team have that trust it becomes easier to tackle issues of data and network security – and to have those necessary conversations.

Need help creating a cyber security company culture that's positive? Don't hesitate to reach out to your managed services provider or IT partner! They can help you lay the foundation for educating your team and ensure that everyone is on the same page when it comes to today's constant cyberthreats. If you don't have a managed services provider, call us at 561-969-1616 and we'll be happy to answer any questions you may have.

Are Your Employees' Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!

How Much Could A Ransomware Attack Cost You?

Have you ever thought about how much your data is worth? Information is possibly the most valuable part of your business – there's your client database, accounting software and inventory management, and of course, any intellectual property you may own.

When ransomware hits, businesses are suddenly forced to re-assess the value of their data: is it worth saving, and what's the deeper cost of the attack?

Most ransomware attacks cost $150-$600 to get your files released, but that's only IF the cyber-criminals honor the payment and actually give you the decryption key. Meanwhile, new client calls are still coming in and you may find yourself unable to operate with your systems down. Paying the ransom or restoring from an unaffected backup seems like a quick fix, but it doesn't end there. There's still the downtime involved to restore all your data – possibly days – and that's a lot of lost productivity.

Plus, if word gets out that your data has been compromised, you may find confidence in your business plummets and your existing clients head elsewhere. That $150 ransom may end up costing well over $150,000!

Prevent Ransomware Attacks on your Business

Keep your systems up to date: Many ransomware attacks take advantage of flaws in older versions of Windows, ones that have since been patched by Microsoft. But to be protected, businesses must be up to date with their patches AND be running a supported version of Windows. Delaying patches and updates puts your business at risk - we can help you update automatically.

Lock down employee computers: Very few staff will require full administrator access to your business network. The higher their level of permissions, the more damage a person can do – either accidentally with a whoopsie click, or by inadvertently installing malware. By locking down your employee computers, you have a better chance of containing a malware attack to non-vital systems. Our experts can design an access management plan that gives you best of both worlds: **flexibility PLUS security**.

Educate your workplace:

Most employees believe they're being cyber-safe but the reality is quite different. Many malicious links and embedded malware have become hard to spot in an instant – which is all it takes to click and regret. We can work with your staff to establish procedures around checking links for authenticity before clicking, awareness around verifying the source of attachments, and the importance of anti-virus scanning. We'll help get the message through!

Have a solid backup plan:

When ransomware hits, a connected backup = infected backup. Unfortunately, synced options such as Dropbox immediately clone the infected files, rendering them useless. The only safe backups will be the ones both physically and electronically disconnected, with systems designed to protect against attacks like this. Our experts can set you up with a backup system that makes recovery a breeze.

Be proactive:

The best way to avoid the financial cost of a ransomware attack is to prevent it from happening in the first place. Smart businesses are the ones watching these widespread ransomware attacks from the sidelines, completely unaffected and seizing opportunities while their competitors are down.

Our managed services can help protect your business against the next cyber-attack. Call us today at 561-969-1616.

"I DIDN'T KNOW"

Unfortunately, that excuse doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

Sign Up For Our FREE "Cyber Security Tip Of The Week" and Always Stay One Step Ahead Of Hackers and Cyber Attacks!

Visit: www.palmtech.net/weekly-tips/

You Must Constantly Educate Yourself On How To Protect What's Yours!

A Few Tips To Stay Safe On Facebook and Twitter

Never let your guard down when you're on social media! Malicious hackers are becoming better at stealing your personal information, so keep these reminders and tips in mind to remain safe while you're on platforms like Facebook and Twitter.

Lock screens exist for a reason

Always lock all your devices as soon as you stop using them. This way, you are safe from the simplest hack of all: someone opening a social media site on your browser while you're still signed in.

In case you didn't know, here's how to lock your computer:

On Macs:

- Press *Ctrl + Command + Q*.
- Click the Apple logo on the top left corner of the screen, and click *Lock screen*.

On Windows devices:

- Press *Windows Key + L*.
- If there are multiple users using the device, click the Start button on the bottom left corner of the screen, then select *User > Lock*.

Strong passwords aren't out of fashion — yet

A six-digit passcode may be enough to secure your phone, but you'll need something much more complicated for your social media account passwords. Create a password that you don't use for any other account because with the regular occurrence of data breaches, hackers probably already have a long list of your favorite passwords from other websites and platforms.

It is best to use a password manager like 1Password, LastPass, or Dashlane. These allow you to generate, save, and retrieve complex passwords.

You can also enable multifactor authentication, which requires users to fulfill at least one more identity verification step after entering their username and password. The extra step or steps can be getting your fingerprint scanned or entering a one-time passcode on an authentication app. Even if hackers have your password, they won't be able to log in without the additional authentication requirements.

Make use of social media features

Facebook can help you monitor who's accessing your account and from where. On a Mac or Windows computer, click on the down arrow located at the upper right corner of your Newsfeed and select *Settings and Privacy*. Then click *Settings > Security and Login* to get more information.

Under the section **Where You're Logged In**, you'll see a list of the places and devices you're logged into. If you don't recognize a particular location or device, that means someone else has logged in as you and is likely doing things you do not approve of. You need to log them out forcibly (by clicking the ellipsis on the row indicating the malicious login and click *Not you?*) and then report the incident immediately.

Then, under **Setting Up Extra Security**, turn on *Get alerts about unrecognized logins*. Unfortunately, as of this writing, Twitter doesn't have the same option. This makes implementing multifactor authentication even more necessary.

Hackers can also take over your Facebook and Twitter accounts through third-party services to which you've given access to your profiles, so make sure to double-check what you have approved. Here's what you need to do:

- **Facebook**: Go to *Settings > Apps and Websites* to view and manage third-party services that use Facebook to log you into the accounts you have with them.
- **Twitter**: Go to *Settings and Privacy > Apps* to check and edit the list.

Lastly, check the permissions Facebook and Twitter have on your smartphone or tablet.

- **Android**: Go to *Settings > Apps > App permissions*.

iOS**: Go to **Settings > Privacy to manage which service can access which parts of your phone (such as the camera and speaker).

Less personal info, fewer problems

These steps are just the beginning of what you should be doing. You should also limit the personal data you share on your social media accounts and avoid oversharing.

By following these tips, you can significantly prevent Facebook and Twitter hacking.

Cybersecurity is a sprawling issue — and social media privacy is but one of the many things you need to stay on top of.