PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions June 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. That's why I have began publishing blog articles to educate and inform our readers.

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

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 AVOID PHISHING SCAMS AND SCAMMERS

Chuck Poole, CISSP

Since the outbreak of COVID-19, there has been a universal trend of an increase in cyber-attacks as more people take their presence online for work and to connect with loved ones. As businesses transition to remote work and operations, cybersecurity and best practices are easily overlooked; creating the perfect opportunity for scammers to strike.

The name of a phisher's game is to deploy a sneaky little trick on you and see if you will take the bait—also known as a Phishing Scam.

Phishing is a type of cybercrime that targets individuals and sends them an email disguised and spoofed to look like it came from a legitimate source in hopes that you will provide them with sensitive information such as your login credentials. Hackers will tempt you to download attachments or go to malicious links that will grant them entry to your data and steal your valuable information.

These phishing scams are popping up at an alarming rate with each passing day—the FBI reported that phishing scams were the most common type of cybercrime in 2020, nearly doubling in frequency from the previous year.

Our expert IT technicians are here to lend a helping hand with a few handy tips to help you spot a phishing scam email:

!. Take note of who the email is from. Look at the sender's email address—most of the time, hackers will make a subtle change to the email address by adding an additional letter to disguise their invalid email. So, if a hacker decided to disguise themselves as your supervisor, Jill Smith, they might add a third L to Jill in the email address making it all too easy for someone to overlook on a day-to-day basis.

2. Keep a wary eye out for attachments. Cyber criminals often send attachments to entice you to open and download spyware, ransomware, or a virus to your device. Make sure you are certain that the sender is someone you know, and the email address is legitimate before opening any attachments.

3. Look before clicking on any links! Scammers are professional criminals;

continued on page 2

disguising a link to look like a genuine website is second nature to them. By briefly holding your cursor over the link, you will see the true URL of where the link will take you to—please, DO NOT CLICK!

4. Read the message clearly and read between the lines. If the email address is identical to someone you know, you are not in the clear yet. It is extremely common for a cybercriminal to pose as someone you know and ask for gift card purchases rather than a set of login credentials because it equates to fast money. If a co-worker or a supervisor asks you to purchase gift cards for the office and request that you send them the information located on the card, just know that this is a textbook scam attempt.

Other signs in the message that point to a cyber-attack are:

- Generic greetings
- Spelling errors
- A sense of urgency
- A call to action

If there is any seed of doubt, ask yourself: *Am I expecting something from this person? Is what they are asking of me out of character for them?*

If you think a phishing scam has been deployed on you:

- Inform your supervisor and IT department immediately
- NEVER respond to the suspected email—by responding to the email, you are informing the cyber criminal that your email address is active and being monitored
- And if you are caught in a ransomware attack, NEVER EVER pay the ransom! There is no guarantee that the cyber criminal will decrypt your files after payment.

What can you do right now?

- Back up all your data and files
- Enable Multi-Factor Authentication on accounts and devices
- Use a password manager
- Keep an eye on Dark Web status (this will alert you if your name and any other personal information has been detected on the Dark Web)

As we've witnessed with the recent cyber-attacks on FireEye and Colonial Pipeline, cyber criminals are working harder than ever to deploy attacks that are more sophisticated than the last. Protecting your devices and your network is critical to safeguarding your data and your livelihood—so in addition to your Anti-Virus, firewalls, and other zero trust applications, make sure you carry out the best practices shared by our IT experts so you don't take the bait when scammers go phishing.

For more information to protect your network, visit us at **www.PalmTech.net** or call us at **561-969-1616** to get a **free cybersecurity assessment for your business**.

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

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

4 Ways Employees Are Putting Your Data At Risk

Your employees are instrumental when it comes to protecting your business from cyberthreats. But they can also become targets for hackers and cybercriminals, and they might not know it. Here are four ways your employees might be endangering your business and themselves — and what you can do about it.

1. They're Not Practicing Safe And Secure Web Browsing. One of the most basic rules of the Internet is to not click on anything that looks suspicious. These days, however, it can be harder to tell what's safe and what isn't.

A good rule of thumb is to avoid websites that do not have "https" in front of their web address. The "s" tells you it's secure – https stands for Hypertext Transfer Protocol Secure. If all you see is "http" – no "s" – then you should **not** trust putting your data on that website, as you don't know where your data might end up.

Another way to practice safe web browsing is to avoid clicking on ads or by using an ad blocker, such as uBlock Origin (a popular ad blocker for Google Chrome and Mozilla Firefox). Hackers can use ad networks to install malware on a user's computer and network.

2. They're Not Using Strong Passwords. This is one of the worst IT security habits out there. It's too easy for employees to use simple passwords or to reuse the same password over and over again or to use one password for everything. Or, worse yet, all of the above.

Cybercriminals love it when people get lazy with their passwords. If you use the same password over and over, and that password is stolen in a data breach (unbeknownst to you), it becomes super easy for cybercriminals to access virtually any app or account tied to that password. No hacking needed!

To avoid this, your employees must use strong passwords, change passwords every 60 to 90 days, and not reuse old passwords. It might sound tedious, especially if they rely on multiple passwords, but when it comes to the IT security of your business, it's worth it. One more thing: the "tedious" argument really doesn't hold much water either, thanks to password managers like 1Password and LastPass that make it easy to create new passwords and manage them across all apps and accounts.

3. They're Not Using Secure Connections. This is especially relevant for remote workers, but it's something every employee should be aware of. You can find WiFi virtually everywhere, and it makes connecting to the Internet very easy. A little too easy. When you can connect to an unverified network at the click of a button, it should raise eyebrows.

And unless your employee is using company-issued hardware, you have no idea what their endpoint security situation is. It's one risk after another, and it's all unnecessary. The best policy is to prohibit employees from connecting to unsecured networks (like public WiFi) with company property.

Instead, they should stick to secure networks that then connect via VPN. This is on top of the endpoint security that should be installed on every device that connects to your company's network: malware protection, antivirus, anti-spyware, anti-ransomware, firewalls, you name it! You want to put up as many gates between your business interests and the outside digital world as you can.

4. They're Not Aware Of Current Threats. How educated is your team about today's cybersecurity threats? If you don't know, or you know the answer isn't a good one, it's time for a change. One of the biggest threats to your business is a workforce that doesn't know what a phishing e-mail looks like or doesn't know who to call when something goes wrong on the IT side of things.

If an employee opens an e-mail they shouldn't or clicks a "bad" link, it can compromise your entire business. You could end up the victim of data breach. Or a hacker might decide to hold your data hostage until you pay up. This happens every day to businesses - and hackers are relentless. They will use your own employees against you, if given the chance.

It is critical to get your team trained & educated about current threats. Education is a powerful tool to help protect your business and your employees. **Call us at 561.969.1616 for a consultation!**

"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 "Cybersecurity 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!

Tech Bytes From PalmTech

ELIMINATE WORKPLACE DISTRACTIONS TO MAXIMIZE YOUR PRODUCTIVITY

While most of us accept that distractions will be a part of our day, if your intention is to get things done and to stay productive and focused, you'll need to minimize those distractions. No, we'll never be able to eliminate them 100%, but we can certainly try. Here's what you can do to cut distractions.

- **Block Time On Your Calendar (And Stick To It).** Use your calendar to its full advantage. Mark time off for e-mails, for *all* projects, phone calls, Zoom calls, you name it! If it's part of your normal day, put it on your calendar. Even throw on time for miscellaneous stuff. Then share it with all relevant parties and stick to it. If you're working on a project between 1:00 p.m. and 3:00 p.m., that's the word.
- **Use Sound To Your Advantage.** A common source of distraction is sound: it can be office chatter in the background or even neighborhood sounds (for those working from home). Find a sound that complements your workflow. It might be chill music or the sounds of rain or a babbling brook. Find the right sound that helps you zone in and blocks disruptive sounds. *Forbes, March 15, 2021*

THE 2 BEST INVESTMENTS YOU WILL EVER MAKE

Practically every successful person has something in common with every other successful person. Millionaires and billionaires share these habits – habits that are absolutely crucial if you want to achieve the success that's on your mind.

1. **Read, Read And Read Some More.** Warren Buffett and Bill Gates are prime examples of this, but it's one of the most common traits among the most successful businesspeople in the world ... They are constantly reading: books, blogs, newspapers, magazines and anything else that enriches their personal and professional lives.
2. **Get Educated.** Whether you hire a private coach, take courses (like continuing education) or hire consultants, there are pros who can teach us more about what we do (or want to do) and how to improve ourselves or our businesses. While we may be good at what we do, there is always room for improvement – you just have to be open to it. *Inc., Feb. 24, 2021*

THE #1 WAY HACKERS BREAK INTO SMALL BUSINESS NETWORKS

Cybercriminals always have new ways to break into business networks. However, there is one method of entry in their toolkit that works better than anything else – and it isn't new!

What is this #1 way they break into business networks just like yours?

Social engineering!

It can take many different shapes, from phishing and smishing scams to simple phone calls. According to a 2020 Security Intelligence study, nearly one-third of cyber-attacks start with a phishing e-mail – and the number is rising. This highlights the need for employee education on cyberthreats and how to identify these types of scams. After all, your employees are your first line of defense against these kinds of threats!

"Every time I use my name as my password I get hacked. Maybe I should change my name. Or, change my password."

CartoonStock.com