PALMTECH
I.T. SOLUTIONS FOR BUSINESS

THE LEGAL TECH TIMES

PalmTech Computer Solutions October 2019

Join Us For a CyberSecurity Breakfast Seminar in November or December!

Wake up and have breakfast with us!

Visit **www.palmtech.net/events/** for more information and to register for this free educational seminar.

This monthly publication provided courtesy of Chuck Poole, President 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.

3 Ways To Prevent Your Employees From Leaking Confidential Information

A lot of businesses need to come to terms with the fact that their employees are their greatest IT threat. As a business owner, you may be aware of cyberthreats to your business, but your employees might not be. They might not know about the threat of cyber-attacks or malware. They might use unsecured WiFi on company equipment. As a result, your employees may be putting your business at serious risk.

What can you do to change that?

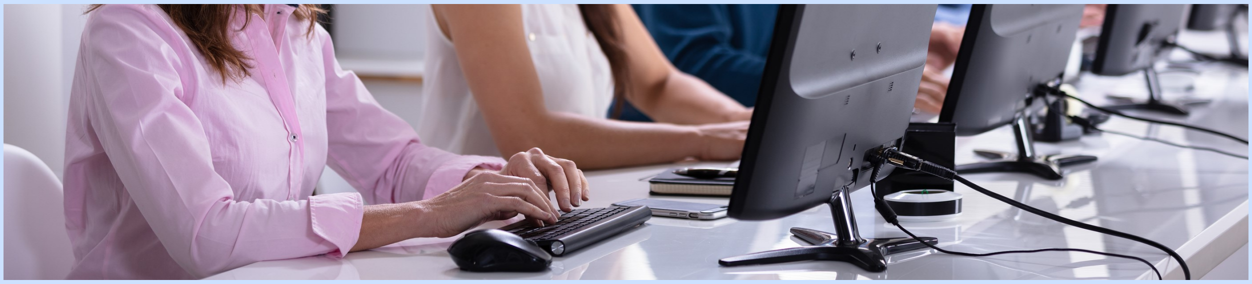
1. IT ALL STARTS WITH EDUCATION. One of the biggest reasons why employees put their employer at risk simply comes down to a lack of education. They don't know about the threats targeting businesses or that small businesses are a major target of hackers and scammers.

You need to do everything you can to train your employees. Give them the education and resources to be a line of defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you aren't sure. Professionals can answer your questions and make sure you and your employees have everything you need to know to keep your business secure.

Another important thing is to ***hold this training regularly.*** Threats evolve, and you need to stay ahead of the curve. Keep IT security on the minds of your employees. When they forget about it, that's when the risk is highest.

2. SAY NO TO UNSECURED, PUBLIC WIFI. This is a big problem for

continued on page 2



businesses with remote employees, employees who work from home or employees who use company technology outside of the business walls. According to a Spiceworks study, 61% of employees said they have connected to unsecured WiFi while working remotely This is cause for concern. Connecting to public WiFi is like leaving the front door of your home wide-open while posting on social media that you're going to be out of town for a week. You never know who is going to let themselves in and snoop around. Hackers use public hot spots to circulate malware and steal data. Sometimes they even set up fake hot spots with the same name as a legitimate hot spot to trick users into connecting to their WiFi, which makes data theft *even easier.*

Discouraging your employees from using unsecured, public WiFi is a good step to take, but don't be afraid to take it further. Don't let them connect company equipment to unsecured WiFi *at all.* And place a bigger focus on endpoint security – make sure your equipment has up-to-date software, malware protection, local firewalls, as well as a VPN (virtual private network). The more layers of security, the better.

3. PROTECT ALL OF YOUR DATA. Your employees should never save personal or business data on portable/external hard drives, USB drives or even as printed material – and then take that data out of the office. The theft of these types of devices is a real threat. An external hard drive is a tempting target for thieves because they *will* search the drive for sensitive data, such as financial or customer information that they can use or sell.

If you have remote employees who need to access company data, put a method in place to do just that (it should be discussed as part of your regular company IT security training). They need to know how to properly access the data, save the data or delete it, if necessary. Many businesses go with a secure cloud option, but you need to determine what makes the most sense for your business and its security.

While these three tips are great, nothing beats helping your employees develop a positive IT security mindset. It's all about understanding the threats and taking a proactive approach to security. Proactivity reduces risk. But you don't have to go it alone. Working with experienced IT security professionals is the best way to cover all your bases – and to ensure your employees have everything they need to protect your business. Call PalmTech at (561)969-1616 to discuss how we can assist you.

> **"It's all about understanding the threats and taking a proactive approach to security."**

Shiny New Gadget: The Philips Somneo Sleep and Wake Up Light

Research suggests that when you wake up naturally (that is, you aren't jolted awake by an alarm or radio), you feel more refreshed and energized during the day.

The Philips Somneo Sleep & Wake-Up Light puts this research to the test. It's designed to simulate a natural sunrise right in your bedroom. You can set it to your specific needs, and it will slowly and steadily brighten when you need to wake up. It can also simulate a sunset for the opposite effect when you're going to bed! You can even use the light as a reading lamp — and it has a built-in radio, too!

The Philips Somneo Sleep & Wake-Up Light is a versatile device, perfect for anyone who wants to get a better night's sleep. Find it at Amazon and many other electronic retailers.

These Are The Biggest Privacy Threats You Face Online Today

1) Webcam Access – While it's rare, there are known exploits that allow others to access your webcam (such as malicious software or software security flaws). Putting electrical tape over your webcam isn't a bad idea, but more webcams are coming with kill switches and shutters for peace of mind.

2) Phishing Scams – Don't ever expect these to go away. People still fall for them. NEVER click links in e-mails from anyone you don't know (and even if you do know them, verify that they sent you a link — e-mail addresses can be spoofed).

3) Web Browser Plug-ins – Vet every browser plug-in and extension you install. Many extensions collect your browsing history and sell it. Read the terms of service before you click install (a good rule of thumb for software in general).

4) Ad Tracking – Web ads (and web ad providers, such as Facebook and Google) are notorious for tracking users. They want to know what you like so they can cater ads directly to you in the hopes that you'll click the ad, which gives them ad revenue. It's one of the many reasons why people use ad blockers.

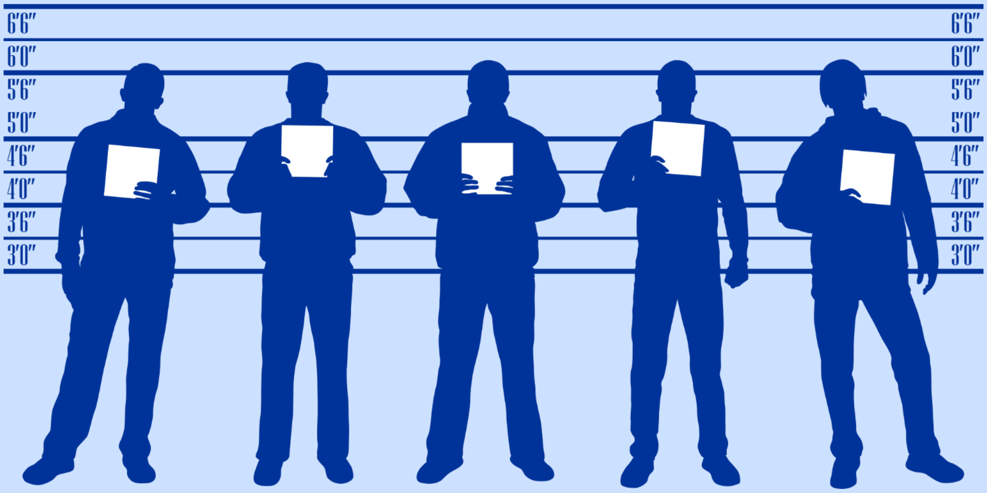
5) Device Tracking – If you have a smartphone, chances are it's being used to track your every move. Again, it comes back to delivering ads that are relevant to you so you'll click on them. For companies like Facebook and Google, users are the product. *Inc., 7/19/2019*

Capitalize On This Strategy To Improve Your Bottom Line

Want to boost your bottom line? The answer may be in cashless payments. It's all about taking your current systems and updating them to current trends.

Outside of the U.S., particularly in Europe and much of Asia, cashless payments are king. More people are relying on smartphones as payment processing tools (both in the consumer and business worlds). Of course, you don't want to rely on cashless — you want to be able to accept any money your customers are spending, whether it's cash, card or electronic.

Look at your point-of-sale system — is it ready for cashless? If not, look into it, research your options, ask around and see what option makes sense for your business (and bottom line). *Small Business Trends, 6/26/2019*



Healthcare Breaches: Data Exposed on 1.5 Million Patient Records

Nearly 1.5 million people had data exposed in healthcare breaches reported to the federal government last month.

That's more than double the roughly 730,000 people who had data compromised in healthcare breaches reported the month prior.

In September, providers, health plans and their business associates reported 29 data breaches to HHS' (Dept. of Health and Human Services) Office for Civil Rights, the agency that maintains the government's database of healthcare breaches. Though fewer people had data compromised in August-reported breaches, there were more overall breach incidents at 49.

Three of the data breaches reported to the OCR in September affected more than 100,000 people each.

Women's Care Florida, an OB-GYN practice, reported a data breach of 528,000 patients to the OCR. The data breach took place at North Florida OB-GYN, a women's health practice that had joined Women's Care Florida in May, and involved an unauthorized user encrypting files on the provider's computer systems, according to a notice posted online.

North Florida OB-GYN discovered the breach in July, but suspects the hacker may have begun accessing its computer systems as early as April.

HHS gives HIPAA-covered entities 60 days from when they discover a breach to notify the department. Women's Care Florida reported the data breach to the OCR on Sept. 25.

North Florida OB-GYN said it has decrypted or recovered "virtually all" of the affected files since discovering the incident.

The two other major breaches reported in September involved ransomware attacks at Sarrell Dental in Alabama and Premier Family Medical in Utah, which compromised the data of 391,000 and 320,000 patients, respectively.

Hacking and IT incidents, like the ones at Women's Care Florida, Sarrell Dental and Premier Family Medical, accounted for 62% of data breaches reported in September. The remaining data breaches resulted from theft, unauthorized access or unauthorized disclosure of patient records. — *Modern Healthcare October 2019*

For information on how PalmTech can help your organization avoid such data risks, contact us at (561)969-1616.

Are Your Credentials For Sale On The Dark Web?

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