PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions

May 2020

Security Awareness Training For Your Staff

Human-error; we talk about it all the time, but what exactly do we mean? Human-error occurs when an individual performs a task or does something with an unintended outcome. It's easy to point the finger at employees as being an organization's weakest link, but without appropriate security awareness training provided by the employer, how can employees truly know what to watch out for?

Call us at (561)969-1616 regarding our **FREE security awareness training** for your staff to ensure your organization is protected.

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.

3 Ways To Stop Cybercriminals Cold In Today's Crazy Times

You've seen it. You've probably even experienced it. For what feels like forever now, just about everyone has been forced to modify priorities. As a business owner, you've probably been focused on shifting your business to accommodate this world crisis. You may even be investing more of your time in retaining customers and generating new cash flow. If you're like most people out there, you've barely even had time to think about cyber security and protecting your important data.

Maybe you've heard the saying "Never let a crisis go to waste." It's as if cybercriminals wrote it because that's exactly what they're thinking right now. In fact, they're probably working overtime right now to craft new malware while our lives have been turned upside down. Yes, as you're focused on your business, hackers are finding new ways into your IT network. Their objective is to steal data and passwords, compromise your clients' private information and even demand large ransoms.

Did you know that cybercrime is expected to cost $6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021? But, now is when hackers are expected to do their absolute most damage.

Here are three strategies you can use right now to help protect your business data, money and productivity during these unusual times.

1. Guard Your Inbox. People aren't paying as much attention as they usually do, which makes it the perfect time for cyber-attackers to send e-mails

continued on page 2

with dangerous malware, worms and viruses. Always carefully inspect every e-mail received and make sure you know the sender.

Here's another tip: avoid clicking links in the e-mail unless it's abundantly clear where they go. Also, don't ever download an attachment unless you know who sent it and what it is. While it takes a few extra seconds, double check by calling the person who sent you the attachment. Better safe than sorry. Make sure you communicate these safeguards to everyone on your team, especially if they are working from home.

2. Secure Your Company-Based Technologies. During crises like this one, your passwords are a critical first line of defense. Don't wait for your company's finance data to be compromised. Make a point now to reevaluate your passwords and direct your team to create stronger passwords. Too many employees are guilty of using the same password across multiple applications. Use a unique password for every single application. Finally, as an added measure, please turn on Multi-Factor Authentication by using your cell phone as a password authenticator. This one features makes it exponentially more difficult for a hacker to compromise your systems.

Your team may tend to save your passwords in their web browser. Don't do this. A skilled hacker can bypass the PIN required to access your saved passwords. Once they have the password or PIN to access your web browser, they can steal as much as they want – credit card information, customer's private data and more!

> **"Did you know that cybercrime is expected to cost $6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021?"**

We recommend our clients use a password manager. It's convenient, but more importantly, it's far more secure.

3. Secure Your Home-Based Technologies. With the coronavirus pandemic, far more businesses are encouraging their employees to work from home. That means a lot of people are working from the living room or kitchen without giving a second thought to security. This negligence is an invitation to new cybercrimes.

Here are a few tips to ensure your work-from-home employees are keeping your network and data secure: make sure your employees and contractors are not using their home computers or devices when they are working from home. Add a firewall to ALL computers and devices that will be utilized at home. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network).

There's no need to invite in more problems by letting your computer and network security slide during these times. We would be happy to help you create or even improve your work-from-home environment.

While this coronavirus scare has negatively affected countless businesses, we are proud to say we are open and continuously servicing our customers. If you need additional security advice or would like to have a consultation to discuss how to keep your data safe or how we can help you work more effectively, simply connect with us today at (561)969-1616.

Cybercriminals Are Counting On You Letting Your Guard Down During This Global Pandemic – Here's How To Stop Them

The world has been slowing down during the COVID-19 pandemic. Wall Street has been hit hard. People stopped going out as often, if at all. We're still being told to quarantine or self-isolate and not engage in groups.

You can bet there's one group that's not slowing down at all. In fact, they're probably working overtime while the rest of us have our lives turned upside down. Cybercriminals and hackers know there's no better time to strike than during a global crisis.

I've put together some solutions you can implement now to help protect your business data, money and productivity. Visit www.palmtech.net/onguard/ to read more.

How To Quickly Shift To A Work-From-Home Business Model To Maximize Productivity In Today's Coronavirus Environment

As a business owner today, you are now facing unprecedented challenges to help deal with the coronavirus pandemic. You are asked to self-isolate and practice social distancing to "flatten the curve." You are asked to allow your employees to work from home to reduce possible exposure and slow the spread of COVID-19.

These are all reasonable requests. However, as a business owner you also need to maximize productivity, bring in revenue and try to grow your business in these demanding times. How can you accomplish these goals when your office is now a ghost town and productivity has fallen off a cliff?

The answer lies in setting up your office to function remotely. If you've never implemented a work-from-home policy before, it may seem like a whole different world. Managing an entirely remote workforce goes far beyond giving your employees a laptop and reminding them to check in every once in a while. After all, there are many factors most business owners haven't ever had to consider, such as:

- What technologies do I need?
- How can my employees work from home without compromising the security of our network?
- How can I make this new work environment as easy, comfortable and productive as possible?

We understand these are unique times. We know that "business as usual" is going to be quite different for an undetermined amount of time. But together we can help you adjust to today's new normal by giving you the tools, technologies and insights to create a secure and productive work-from-home business environment. Here are three important considerations to getting you set up and running a successful work-from-home business:

1) Don't allow employees to use home computers or devices.

Their mindset may be, "Well, I'm working from home so I may as well use my home computer." This is a dangerous mistake. Our team works hard to ensure your company computers and network are secure and protected from malware, viruses and cyber-attacks. Their home computers and devices could be littered with tons of downloaded music, videos, images and more. Because it's more exposed, it can invite malware into your network. Rather, provide a company-approved and secured computer/laptop for employees to use at home.

2) Secure their WiFi access point.

Without a secure WiFi access point, you're essentially leaving a back door open to hackers. That's because WiFi signals are often broadcast far beyond your employees' homes and out into streets. Yes, drive-by hacking is popular among cybercriminals today. A few tips for securing your employees' WiFi access points:

- Use stronger encryption and a more complex password
- Hide your network name
- Use a firewall

These security measures are not difficult to set up. But if you have any questions or need assistance, we will be happy to help get your employees set up remotely.

3) Use a two-factor authentication VPN.

VPN stands for virtual private network. It's essentially a private, encrypted tunnel that goes direct to your IT network in your office. Ideally, you'll want your VPN to support two-factor authentication. This means it's doubly secure because your employees will need to call in to access the network. If you don't have a VPN for your employees to use, you can consider other services, such as GoToMyPC or Zoho. While these products are not as secure, at least they keep your home network from being exposed.

As business owners ourselves, we too are having to pivot and work differently than we ever have before. However, because we have the technology and infrastructure in place, we are still surprisingly productive.

Our team wants to help your business survive and thrive during today's unique environment. If you and your IT team need extra hands right now…or solutions to help your employees work SECURELY from home…we have software tools, expert staff and resources we'd like to offer you to keep your business as productive as possible. Call us at 561.969.1616 for more information.

if you wish to book a quick 10- to 15-minute call to discuss, call us at (561)969-1616.

Please know that this is not a sales call but simply an outreach to help a fellow CEO stay afloat.

Do These 3 Things To Make Sure You Don't Get Hacked

Train up. Get your entire team trained on IT security fundamentals and best practices. They should know how to create strong passwords, how to safely access the web and how to securely use e-mail – including how to identify phishing scams. They should have a clear understanding of today's threats and how to be proactive in addressing those threats.

Invest in good tech. You should be invested in solid malware protection, including antivirus software and firewalls. All of your data should be backed up to the cloud and expertly secured using encryption software. You should also be invested in threat monitoring.

Establish relevant systems and processes. Have standard operating procedures (SOP) in place to train employees, respond to threats and access networks. For example, are employees connecting with unverified devices from home? Establish rules on what can and cannot happen. Another example: are your cloud backups set up correctly? Is someone checking it? Again, have SOP in place to address these kinds of issues. *Small Business Trends, Feb. 13, 2020*

"I either need a shorter title or a longer desk."

3 Ways To Grow Your Business Without Spending A Dime

Follow a thought leader in your industry. Whether you follow them on social media or their blog, keep up-to-date with the issues they're talking about. Then do further research into those issues. This keeps you in the know and more likely to learn something you can easily apply to your own business.

Use your best testimonials. If someone posts a great review on Google, for example, reach out and ask about using it in your marketing. Or reach out to customers who you already have a good relationship with and ask if they're willing to give you a testimonial. It builds credibility.

Partner up. It pays to develop partnerships with existing vendors or other businesses that are adjacent to yours. That is to say, look for opportunities to share customers. If you have a customer who's looking for a specific service you don't offer, point them to someone who does (your partner). And your partner will do the same. Reach out into your business community and see what kind of relationships you can form. *Business Insider, Feb. 13, 2020*

ARE YOUR EMPLOYEES' CREDENTIALS SAFE?
DON'T RISK THE UNKNOWN
WE'LL MONITOR THE DARK WEB FOR COMPROMISED EMPLOYEE DATA AND NOTIFY YOU WHEN THEY'RE FOUND AT RISK
PalmTech Computer Solutions
561-969-1616
PALMTECH
I.T. Solutions For Business

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

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