PALMTECH
I.T. Solutions For Business

# THE PALMTECH TIMES

PalmTech Computer Solutions May 2018

## Take Your Security To The Next Level With PalmTech's Enhanced Security

**We've created an all-inclusive package to address your security needs.**

**Visit www.palmtech.net/enhanced/ for more information.**


**May 2018**

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.

## The Shocking Truth Behind Cybercrime Threats

### And What You Can Do About Them Now

Today's technological innovations have empowered small businesses to do things that would have been utterly unimaginable even 15 years ago. To remain competitive in a constantly shifting landscape, we've become more dependent on software and hardware to house even the most basic structures of the companies we run.

Meanwhile, these technologies are evolving at breakneck speed. Every day, there's a slew of new devices to consider, a pile of new updates to install and a new feature to wrap our heads around. Every morning, we wake up and the digital world is thrillingly new.

But all over the world, there's an insidious network of criminals keeping up with this insanely rapid pace of progress. With every new security measure designed to protect our digital assets, there are thousands of hackers working around the clock to determine a new way to break through. An estimated 978,000 fresh new malware threats are released into the world each day. The term "up to date" doesn't mean much anymore in the wake of new developments arriving minute by minute.

There's a price to pay for the increased efficiency and reach enabled by the digital age. We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a crippling large-scale cyberattack, with criminals lifting millions of dollars in customer data

*continued on page 2*

and digital assets. Equifax, J.P. Morgan, Home Depot, Yahoo!, Verizon, Uber and Target – these narratives are so commonplace that they barely raise an eyebrow when we read about them in the news.

Most business owners wrongly assume that these incidents have no bearing on their own companies, but these high-profile incidents account for less than half of data breaches. In fact, according to Verizon's 2017 Data Breach Investigations Report, 61% of attacks are directed at small businesses, with half of the 28 million small and medium-sized businesses (SMBs) in America coming under fire within the last year.

It's hard to imagine how you can possibly protect yourself from these innumerable threats. Statistically, you can be all but certain that hackers will come for your data, and there's no way to know what new tool they'll be equipped with when they do.

You may not be able to foresee the future, but you can certainly prepare for it. With research, education and resources, you can implement a robust security solution

**"We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a large-scale, crippling cyber-attack..."**

into the fabric of your business. That way, you can send hackers packing before they get their hooks into the organization you've spent years building from the ground up.

One huge leap you can make right now for the security of your business is to simply realize that cyber security isn't something you can install and leave alone for years, months or even days. It requires regular updates and the attention of professionals to ensure there's no gap in your protection. There are new shady tactics being used by criminals every day, but there are also fresh protocols you can use to stave them off.

Small business owners assume that since they don't have the resources of a Fortune 500 company, they don't have the means to invest in anything but the barest of security. Obviously, hackers know this and target SMBs in droves. The bad news is that most businesses' paper-thin barriers won't save them in the event of a crisis. The good news is that it doesn't take thousands upon thousands of dollars to implement a security system that will send the hackers packing. Call us at **(561)969-1616** before June 15th and get a **FREE Network Security Assessment**!


**For a FREE scan, visit www.palmtech.net/darkweb/**

SHINY NEW GADGET THE MONTH

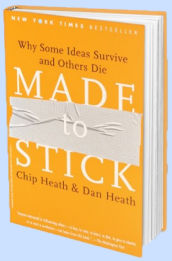
## The Reverse Microwave Can Quick-Freeze Food and Drinks

Way back in 1946, technology gave us the capability to pop some leftovers into the microwave and heat them up within minutes. But if we had a warm beer in our hands or needed a tray of ice quick, we were out of luck. Enter Frigondas's line of new kitchen technologies, which enable users to flash-freeze dishes, rapidly chill beverages and create crystal-clear ice within minutes. Couple this revolutionary feature with Frigondas's host of advanced heating abilities, and you've got a kitchen appliance that's set to change the microwave game for good.

The only problem is that the technology isn't yet available for purchase, with no release date in sight. Still, experts expect it to hit the market within a year or two, though it remains to be seen whether it will justify what's sure to be a hefty price tag.

## *Made To Stick*

**By Chip and Dan Heath**




Why, in today's chaotic media climate, do conspiracy theories, abject falsifications and urban legends circulate effortlessly throughout the country while most businesses struggle to make their ideas "stick"? In their popular 2007 book *Made to Stick*, educators and idea collectors Chip and Dan Heath employ a wealth of anecdotes, case studies and data to discover what makes some ideas last and others fade away within the week. Using this information, they create a compelling set of principles that can be used by anyone seeking to make a lasting mark on the world.

# The Internet Of Things: Are You Okay Playing Offense?

Adjusting your home's thermostat and hot water heater back to normal temperatures as you board a plane on your way home isn't just cool, it's incredibly handy. However, the network of these and other connected devices – often called "the Internet of Things" (IoT) – poses one of the biggest security problems of the modern era.

Most people think about changing their computer password regularly and their ATM PIN occasionally, but they almost never consider changing the password the programmable thermostat ships with from the factory, meaning that anyone who can access the manual has access to your thermostat.

Usually, attackers who target IoT devices don't want to cause you a problem. Instead, they use your device along with 20,000 other thermostats as "soldiers" to battle against a website or e-mail server. By flooding these sites with traffic, they can shut them down or stop your e-mail server from delivering your messages.


You should adopt a strict offensive posture against these types of threats in your life and business. If there is even a suspected problem with one of your IoT devices, pull the plug. Your heater may be cold when you get home, but at least your data will be safe.

# Safety Tips For Watering Hole Attacks

Bad news, internet users: Cybercriminals have developed more advanced tricks to compromise your systems. While you may be familiar with attacks involving suspicious emails, the new kid on the block known as watering hole attacks are far more nefarious and effective. Fortunately, there are a few things you can do to keep yourself safe.

**What are watering hole attacks?**
Much like phishing, a watering hole attack is used to distribute malware onto victims' computers. Cybercriminals infect popular websites with malware. If anyone visits the site, their computers will automatically be loaded with malware.

The malware used in these attacks usually collects the target's personal information and sends it back to the hacker's server. Sometimes the malware can even give hackers full access to their victims' computers.

But how does a hacker choose which websites to hack? With internet tracking tools, hackers find out which websites companies and individual users visit the most. They then attempt to find vulnerabilities in those websites and embed them with malicious software.

Any website can fall victim to a watering hole attack. In fact, even high-profile websites like Twitter, Microsoft, Facebook, and Apple were compromised in 2013.

You can protect yourself by following these tips.

**Update your software**
Watering hole attacks often exploit bugs and vulnerabilities to infiltrate your computer, so by updating your software and browsers regularly, you can significantly reduce the risk of an attack. Make it a habit to check the software developer's website for any security patches. Or better yet, hire a managed IT services provider to keep your system up to date.

**Watch your network closely**
To detect watering hole attacks, you must use network security tools. For example, intrusion prevention systems allow you to detect suspicious and malicious network activities. Meanwhile, bandwidth management software will enable you to observe user behavior and detect abnormalities that could indicate an attack, such as large transfers of information or a high number of downloads.

**Hide your online activities**
Cybercriminals can create more effective watering hole attacks if they compromise websites only you and your employees frequent. As such, you should hide your online activities with a VPN and your browser's private browsing feature.

At the end of the day, the best protection is staying informed. As cyberthreats continue to evolve, you must always be vigilant and aware of the newest threats. Tune in to our blog and sign up for our cybersecurity tips and alerts to find out about the latest developments in security and to get more tips on how to keep your business safe: www.palmtech.net/security-tips/.


## Are Your Credentials For Sale On The Dark Web?

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


"How come Lewis and Clark didn't just use MapQuest?"