PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions July 2018

Is Your Firm Prepared For Hurricane Season?

Visit www.PalmTech.net/prep-now to download PalmTech's Severe Storm Prep Checklist.

Don't wait to prepare. Contact us before August 31st for a FREE *in-depth analysis* of your disaster preparedness.

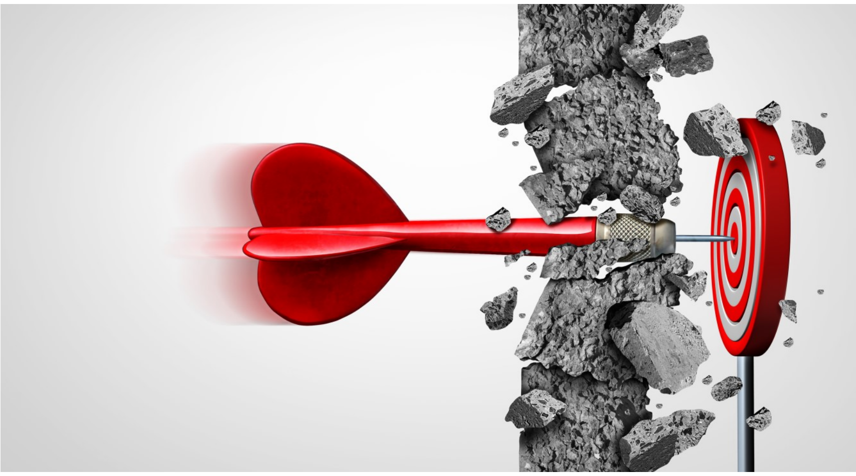
Don't be a statistic. Contact PalmTech at (561)969-1616!

July 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.



Top 4 Ways Hackers Will Attack Your Network

And They Are Targeting You Right Now

Most small and midsize business (SMB) owners exist in a bubble of blissful ignorance. They focus on the day-to-day operations of their organization, driving growth, facilitating hiring and guiding marketing, without a single thought given to the security of the computer networks these processes depend on. After all, they're just the little guy – why would hackers go to the trouble of penetrating their systems for the minuscule amount of data they store?

And eventually, often after years of smooth sailing through calm seas, they get hacked, fork out thousands of dollars to malicious hackers and collapse beneath the weight of their own shortsightedness.

The facts don't lie. According to Verizon's annual Data Breach Investigations Report, a full 71% of cyber-attacks are aimed squarely at SMBs. And while it's unclear exactly how many of these attacks are actually successful, with the sad state of most small businesses' security protocols, it's a safe bet that a good chunk of the attacks make it through.

But why? As Tina Manzer writes for Educational Dealer, "Size becomes less of an issue than the security network … While larger enterprises typically have more data to steal, small businesses have less secure networks." As a result, hackers can hook up automated strikes to lift data from thousands of small businesses at a time – the hit rate is that high.

Today, trusting the security of your company to your son-in-law, who assures you he "knows about computers," isn't enough. It takes constant vigilance, professional attention and, most of all, knowledge. Start here with the four most common

continued on page 2

ways hackers infiltrate hapless small businesses.

1. PHISHING E-MAILS

An employee receives an e-mail directly from your company's billing company, urging them to fill out some "required" information before their paycheck can be finalized. Included in the very professional-looking e-mail is a link your employee needs to click to complete the process. But when they click the link, they aren't redirected anywhere. Instead, a host of vicious malware floods their system, spreading to the entirety of your business network within seconds, and locks everyone out of their most precious data. In return, the hackers want thousands of dollars or they'll delete everything.

It's one of the oldest tricks in the hacker toolbox, but today it's easier than ever for an attacker to gather key information and make a phishing e-mail look exactly like every other run-of-the-mill e-mail you receive each day. Train your employees to recognize these sneaky tactics, and put in safeguards in case someone messes up and clicks the malicious link.

2. BAD PASSWORDS

According to Inc.com contributing editor John Brandon, "With a $300 graphics card, a hacker can run 420 billion simple, lowercase, eight-character password combinations a minute." What's more, he says, "80% of cyber-attacks involve weak passwords," yet despite this fact, "55% of people use one password for all logins."

As a manager, you should be bothered by these statistics. There's simply no excuse for using an easy-to-crack password, for you or your team. Instead, it's a good idea to make a password out of four random common words, splicing in a few special characters for good measure. To check the strength of your password, type it into HowSecureIsMyPassword.net before you make it official.

> **"...hackers can hook up automated strikes to lift data from thousands of small businesses at a time — the hit rate is that high."**

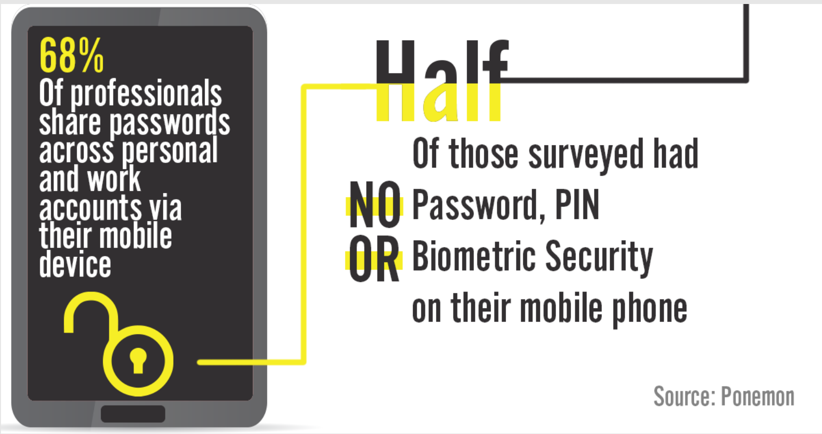
3. MALWARE

As described above, malware is often delivered through a shady phishing e-mail, but it's not the only way it can wreak havoc on your system. An infected website (such as those you visit when you misspell sites like Facebook.com, a technique called "typosquatting"), a USB drive loaded with viruses or even an application can bring vicious software into your world without you even realizing it. In the past, an antivirus software was all that you needed. These days, it's likely that you need a combination of software systems to combat these threats. These tools are not typically very expensive to put in place, especially considering the security holes they plug in your network.

4. SOCIAL ENGINEERING

As fallible as computers may be, they've got nothing on people. Sometimes hackers don't need to touch a keyboard at all to break through your defenses: they can simply masquerade as you to a support team in order to get the team to activate a password reset. It's easier than you think, and requires carefully watching what information you put on the Internet – don't put the answers to your security questions out there for all to see.

We've outlined some of the simplest ways to defend yourself against these shady techniques, but honestly, the best way is to bring on a company that constantly keeps your system updated with the most cutting-edge security and is ready at a moment's notice to protect you in a crisis. Hackers are going to come for you, but if you've done everything you can to prepare, your business will be safe. Call us at **(561)969-1616** for assistance with your organization's security.



Source: Ponemon

Contact us before August 31st, 2018 and we will provide a FREE Cybersecurity Assessment for your organization. For more information and to sign up, visit:

www.PalmTech.net/cyber-secure/

SHINY NEW GADGET THE MONTH

Introducing The Snap SmartCam

Today, the security of your home is more important than ever before. Lawbreakers are constantly getting bolder, and as our technology advances, they switch up their tactics. With that in mind, all of us should be on the lookout for a security camera that's difficult to spot, is intelligent about the footage it collects, and grabs high-quality footage to identify burglars.

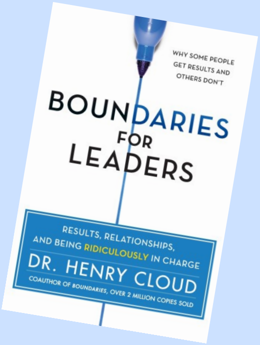
Enter the Snap SmartCam, a tiny little camera that looks — and operates — just like a phone charger. The innocuous-looking device uses motion-detecting technology to pick up when shady activity is going on in your house, and takes high-quality footage to catch a person in the act. If you're interested, the camera will cost you $57.00 at the time of writing, a great deal for a security camera of any type, much less one that seems so useful.

Boundaries For Leaders

By Dr. Henry Cloud

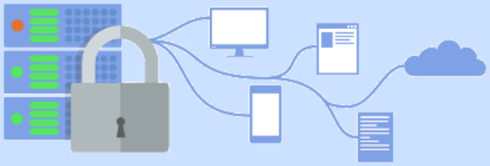
Being an effective leader requires more than tracking employee performance and guiding your team to success. You need to create a business environment that enables your team to function at their highest potential.

In "Boundaries for Leaders," Dr. Henry Cloud breaks down seven "leadership boundaries" that are crucial to maximizing productivity and success throughout your organization, from facilitating employee focus on what matters most, to identifying ways for your team to take ownership of projects in order to drive results. If you're a leader in any capacity, it's a vital read that will give you a big-picture overview of strategies to push your team to the next level.


WHY SOME PEOPLE GET RESULTS AND OTHERS DON'T
BOUNDARIES FOR LEADERS
RESULTS, RELATIONSHIPS, AND BEING RIDICULOUSLY IN CHARGE
DR. HENRY CLOUD
COAUTHOR OF BOUNDARIES, OVER 2 MILLION COPIES SOLD

What To Do BEFORE You Go To Starbucks

You're in the car on the way home from Starbucks, basking in the glow of your triple-shot, low-foam, extra-hot pumpkin spice latte when you suddenly realize your laptop has gone missing. You drive back to the store like a caffeinated lunatic, only to discover no one has turned it in. What do you do?



Well, first you should notify your IT department (us!) immediately to tell them your device has gone missing. That way, we can change passwords and lock access to applications and data. We can also remotely wipe your device to make sure no one will be able to gain access — a key reason it's critical to back up your data on a daily basis.

Next, change ALL the passwords to every website you regularly log in to, starting with any sites that contain financial data or company data. If your laptop contained others' medical records, financial information, or other sensitive data (social security numbers, birthdays, etc.), you should contact a qualified attorney to understand what you may be required to do by law to notify the affected individuals.

An ounce of prevention is worth a pound of cure, so make sure you're engaging us to encrypt/back up your data and put remote monitoring software on all your mobile devices. Put a pin-code lock or password requirement in place to access your devices after 10 minutes of inactivity, and get in the habit of logging out of websites when you're done using them.

For additional tips on protecting yourself and your data, visit www.PalmTech.net/6-ways. In addition, if you haven't already, be sure to sign up for our weekly cybersecurity tips at www.PalmTech.net/security-tips/.

Regularly Evaluate Your Cybersecurity

Experts estimate that the global market for cybersecurity products this year will exceed that of last year. At first glance, an increase in spending seems necessary and shows that businesses are becoming more aware of cybersecurity issues. But a closer look may prove otherwise. Learn why your company could be investing on cybersecurity products the wrong way.

Uncover threats and vulnerabilities

Every business should evaluate the current state of its cybersecurity by running a risk assessment. Doing so is one of the easiest ways to identify, correct, and prevent security threats. After discovering potential issues, you should rate them based on probability of occurrence and potential impacts to your business.

Keep in mind that risk assessments are specific to every business and there is no one-size-fits-all approach for small business technology. It all depends on your line of business and operating environment. For instance, manufacturing companies and insurance groups have totally different applications to secure.

After tagging and ranking potential threats, you should identify which vulnerabilities need immediate attention and which ones can be addressed further down the line. For example, a web server running an unpatched operating system is probably a higher priority than a front desk computer that's running a little slower than normal.

Tailor controls to risks

Instead of spending time and money evenly on all systems, it’s best that you focus on areas with high risk. You should address these issues immediately after an assessment, but also put plans in place to evaluate their risk profiles more often.

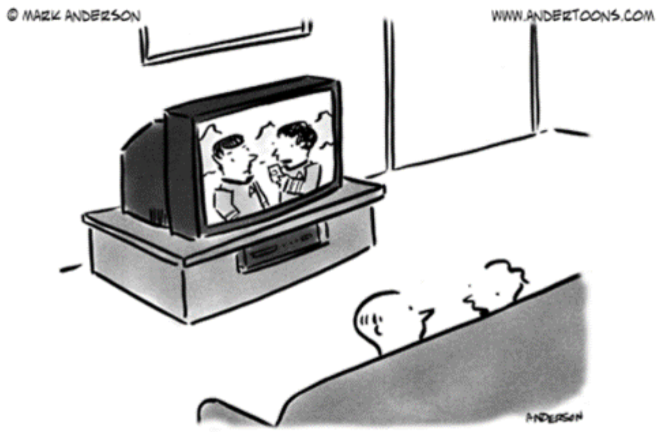
Assess existing products

Chances are, your organization has already spent a great deal of money on security products and their maintenance and support. By conducting risk assessments more often, you can improve the strategies you already have in place and uncover wasteful spending. You may discover that one outdated system merely needs to be upgraded and another needs to be ditched. Remember, your existing products were purchased to meet specific needs that may have changed immensely or disappeared altogether.

It's much harder to overcome cybersecurity obstacles if you're not regularly evaluating your IT infrastructure. Contact our experts at **(561)969-1616** for help conducting a comprehensive assessment today!

Are Your Credentials For Sale On The Dark Web?

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



“If this is the future, how come their phones can’t take pictures?”