PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions October 2018

4 Social Engineering Scams To Watch Out For

Hackers are preying on gullible victims to circumvent network security systems and steal sensitive information. If you don't want to be the next victim, read about the most common social engineering scams here:

www.palmtech.net/scam-watch/

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.

How To Make Sure You Never Fall Victim To Ransomware

Late last March, the infrastructure of Atlanta was brought to its knees. More than a third of 424 programs used nearly every day by city officials of all types, including everyone from police officers to trash collectors to water management employees, were knocked out of commission. What's worse, close to 30% of these programs were considered "mission critical," according to Atlanta's Information Management head, Daphne Rackley.

The culprit wasn't some horrific natural disaster or mechanical collapse; it was a small package of code called SAMSAM, a virus that managed to penetrate the networks of a $371 billion city economy and wreak havoc on its systems. After the malicious software wormed its way into the network, locking hundreds of city employees out of their computers, hackers demanded a $50,000 Bitcoin ransom to release their grip on the data. While officials remain quiet about the entry point of SAMSAM or their response to the ransom, within two weeks of the attack, total recovery costs already exceeded $2.6 million, and Rackley estimates they'll climb at least another $9.5 million over the coming year.

It's a disturbing cautionary tale not only for other city governments, but for organizations of all sizes with assets to protect. Atlanta wasn't the only entity to buckle under the siege of SAMSAM. According to a report from security software firm Sophos, SAMSAM has snatched almost $6 million since 2015, casting a wide net over more than 233

continued on page 2

victims of all types. And, of course, SAMSAM is far from the only ransomware that can bring calamity to an organization.

If you're a business owner, these numbers should serve as a wake-up call. It's very simple: in 2018, lax, underfunded cyber security will not cut it. When hackers are ganging up on city governments like villains in an action movie, that's your cue to batten down the hatches and protect your livelihood.

The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?

1. Back Up Your Stuff

If you've ever talked to anyone with even the slightest bit of IT knowledge, you've probably heard how vital it is that you regularly back up everything in your system, but it's true. If you don't have a real-time or file-sync backup strategy, one that will actually allow you to roll back everything in your network to before the infection happened, then once ransomware hits and encrypts your files, you're basically sunk. Preferably, you'll maintain several different copies of backup files in multiple locations, on different media that malware can't spread to from your primary network. Then, if it breaches your defenses, you can pinpoint the malware, delete it, then restore your network to a pre-virus state, drastically minimizing the damage and totally circumventing paying out a hefty ransom.

2. Get educated

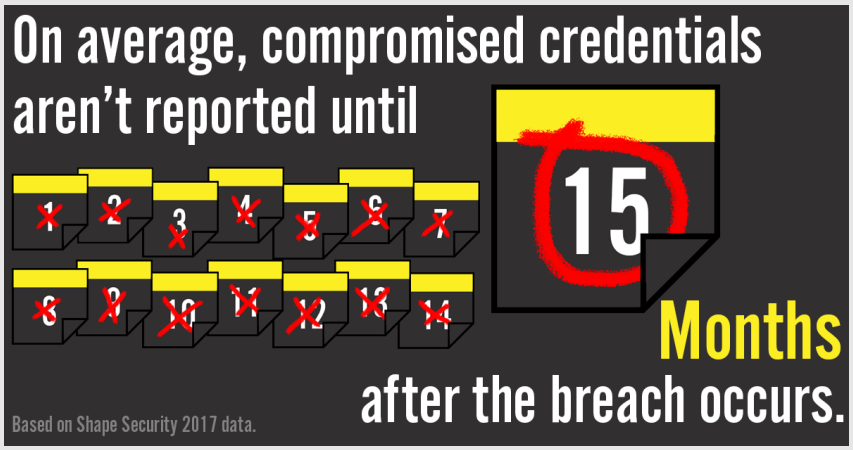
We've written before that the biggest security flaw to your business isn't that free, outdated antivirus you've installed, but the hapless employees who sit down at their workstations each day. Ransomware can take on some extremely tricky forms to hoodwink its way into your network, but if your team can easily recognize social engineering strategies, shady clickbait links and the dangers of unvetted attachments, it will be much, much more difficult for ransomware to find a foothold. These are by far the most common ways that malware finds it way in.

3. Lock It Down

By whitelisting applications, keeping everything updated with the latest patches and restricting administrative privileges for most users, you can drastically reduce the risk and impact of ransomware. But it's difficult to do this without an entire team on the case day by day. That's where a managed services provider becomes essential, proactively managing your network to plug up any security holes long before hackers can sniff them out.

The bad news is that ransomware is everywhere. The good news is that with a few fairly simple steps, you can secure your business against the large majority of threats. Call us at (561)969-1616 for a **FREE Network Security Assessment** so we can ensure your business is protected.

> **"The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?"**



Are Your Credentials For Sale on the Dark Web? Contact us before November 15th, 2018 and we will provide a FREE Dark Web Analysis. For more information and to sign up, visit:

www.PalmTech.net/darweb/

SHINY NEW GADGET OF THE MONTH

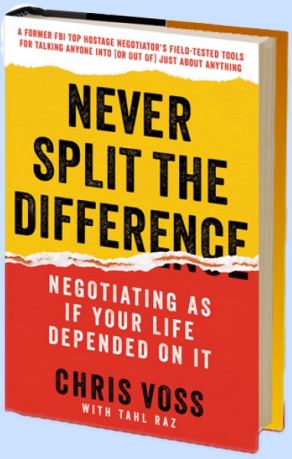
CLOCKY: The Alarm Clock On Wheels

Waking up can be difficult. Even the most driven people occasionally struggle to get out of bed in the morning, pounding the snooze button ad infinitum until we finally force ourselves upright, dazed and groggy from interrupted sleep.

That's where Clocky, the alarm clock on wheels, comes in. Clocky is an adorable little digital timekeeper to keep by your bed; it will be your best friend until it comes time to rise in the morning. By default, it'll give you a single press of the snooze for free, but once you hit snooze for the second time, it'll speed off and start wheeling around your room, beeping and making a racket until you catch it and send it back to sleep. If you or someone you know struggles to get out of bed in the morning, Clocky will be a trusted ally in your mission to start the day.

Never Split The Difference
By Chris Voss

In today's business world, everyone is a negotiator. But hopefully, you've never had to wheel and deal your way out of a hostage situation where lives were on the line.



But that's exactly what ex-FBI kidnapping negotiator Chris Voss used to deal with all the time in his old job. In his best-selling book, *Never Split The Difference*, Voss outlines the tactics that expert negotiators employ to achieve their desired outcome, invaluable strategies that any business leader could stand to master.

2 Sneaky Ways Hackers Will Rob You Blind

We've said it before and we'll say it again: cyber-attacks aren't limited to big corporations and government organizations. Verizon's 2018 Data Breach Investigations Report states that 58%of data breaches in 2017 occurred at small businesses. And according to Verizon's data, there are two specific hacking techniques on the rise today that small businesses should know about.

The first technique is point-of-sale (POS) system hacking. If you're in the hospitality industry, this should definitely be on your radar. Verizon recorded 368 POS incidents in 2017, most instigated by hackers penetrating the system rather than employees making mistakes that opened up vulnerabilities. Usually, hackers will steal credentials directly from a POS service provider, which enables them to exploit the POS systems used by that provider's customers.

The second is called financial pretexting. Instead of phishing a business and installing malware, attackers impersonate a high-level employee within an organization — often using a legitimate but compromised e-mail account — to steal funds or sensitive information from the company's finance or HR department. As always, forewarned is forearmed. Equip your teams with the know-how to avoid these scams and you will be ahead of the game.

SmallBizTrends.com, 5/1/2018

PalmTech's Referral Program

At PalmTech Computer Solutions we believe that referrals are the greatest form of flattery. If you know someone who is worried about any aspect of their business technology, do them a favor and put them in touch with us. For More information, visit www.palmtech.net/referral-program/!

Forget These Disaster Recovery Myths

Disaster recovery (DR) isn't what it used to be. Long gone are the days when a DR solution cost over a hundred thousand dollars and relied predominantly on tape backups. Cloud computing has dramatically changed the DR landscape. Unfortunately, there are still many misconceptions about DR. Here are a few of the myths that no longer apply.

Tape backups are the best DR solution
Backup tapes are physical objects that deteriorate over time. Don't believe us? Try listening to a cassette tape from the '90s. Over time, tape backups become distorted and stop working. Deterioration is slow and may only affect some files in the early stages, so don't settle for a mere cursory check.

Aside from backups in your office, another set of tape backups needs to be stored outside your premises. In case a natural disaster damages your office, not all your data will be wiped out. But if your storage space isn't safe from the elements, this could also be a problem.

Unlike tape backups, a cloud-based backup saves you time. Data is automatically backed up online, and you don't need to spend time managing boxes of tapes. Your time is better spent on your assigned tasks, not IT management.

The RTO you want will be too expensive
Recovery time objectives (RTO) are essential to any DR plan. You need to get everything up and running again as quickly as possible to avoid serious losses. In the days before the cloud, a swift recovery time could cost you well into six figures. Today, cloud and virtualization solutions have made this much more affordable, and faster than ever before.

Most DR providers can back up your critical data in an hour or two. And if you ever need to recover it, most services can do so in less than a day. That's the power of the cloud. And when it comes to DR, it truly has changed everything.

Disaster recovery is for big business, not SMBs
The cloud has made this valuable service affordable for businesses of all sizes. From dental offices to small retail operations, SMBs can now take advantage of the best DR solutions on the market. Advances in IT and the cloud have eliminated the obstacles of complexity, costs, and insufficient IT resources.

We hope that by dispelling these myths, we've convinced you that disaster recovery is more affordable and efficient than ever. If you'd like to learn how our DR solutions can safeguard your business, send us a message at info@palmtech.net or call us at (561)969-1616 and we'll gladly fill you in.

Are Your Credentials For Sale On The Dark Web?

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

"I heard she has eyes in the back of her head, but I suspect more likely it's some combination of Google Glass and a smartwatch."