PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions JULY 2016

Come See PalmTech at the 23rd Annual HFTP Florida Regional Conference

July 20th - 22nd, 2016

Location: Wyndham Grand Jupiter at Harbourside Place in Jupiter, FL

Visit www.palmtech.net/events/ for details!

HFTP Hospitality Financial and Technology Professionals

JULY 2016

This monthly publication provided courtesy of Chuck Poole, President of PalmTech Computer Solutions.

Our Mission:
To equip small and midsized businesses in West Palm Beach area with a smooth running and seamless IT platform that enhances productivity and efficiency and becomes a competitive advantage.

5 Ways To Spot A Social Engineering Attack

"I'm not going to make payroll – we're going to close our doors as a result of the fraud."

Unfortunately, that statement is becoming more common among smaller businesses, according to Mitchell Thompson, head of an FBI financial cybercrimes task force in New York.

The FBI reports that since October 2013 more than 12,000 businesses worldwide have been targeted by social engineering–type cyberscams, netting criminals well over $2 billion. And those are just the reported cases. Often, due to customer relationships, PR or other concerns, incidents go unreported.

These unfortunate events were triggered by a particularly nasty form of cyberattack known as "social engineering."

Social engineering is a method cyber con artists use to lure well-meaning individuals into breaking normal security procedures. They appeal to vanity, authority or greed to exploit their victims. Even a simple willingness to help can be used to extract sensitive data. An attacker might pose as a coworker with an urgent problem that requires otherwise off-limits network resources, for example.

They can be devastatingly effective, and outrageously difficult to defend against.

The key to shielding your network from this threat is a keen, ongoing awareness throughout your organization. To nip one of these scams in the bud, every member of your team must remain alert to these five telltale tactics:

1. **Baiting** – In baiting, the attacker dangles something enticing to move his victim to action. It could be a movie or music download. Or something like a USB flash drive with company logo, labeled "Executive Salary Summary 2016 Q1," left where a victim can easily find it. Once these files are downloaded, or the USB drive is plugged in, the person's or company's computer is infected, providing a point of access for the criminal.

continued on page 2

2. **Phishing –** Phishing employs a fake e-mail, chat or website that appears legit. It may convey a message from a bank or other well-known entity asking to "verify" login information. Another ploy is a hacker conveying a well-disguised message claiming you are the "winner" of some prize, along with a request for banking information. Others even appear to be a plea from some charity following a natural disaster. And, unfortunately for the naive, these schemes can be insidiously effective.
3. **Pretexting –** Pretexting is the human version of phishing, where someone impersonates a trusted individual or authority figure to gain access to login details. It could be a fake IT support person supposedly needing to do maintenance…or an investigator performing a company audit. Other trusted roles might include police officer, tax authority or even custodial personnel, faking an identity to break into your network.
4. **Quid Pro Quo –** A con artist may offer to swap some nifty little goody for information… It could be a t-shirt, or access to an online game or service in exchange for login credentials. Or it could be a researcher asking for your password as part of an experiment with a $100 reward for completion. If it seems fishy, or just a little too good to be true, proceed with extreme caution, or just exit out.
5. **Tailgating –** When somebody follows you into a restricted area, physical or online, you may be dealing with a tailgater. For instance, a legit-looking person may ask you to hold open the door behind you because they forgot their company RFID card. Or someone asks to borrow your laptop or computer to perform a simple task, when in reality they are installing malware.

The problem with social engineering attacks is you can't easily protect your network against them with a simple software or hardware fix. Your whole organization needs to be trained, alert and vigilant against this kind of incursion.

For more on social engineering as well as other similar cyberthreats you need to protect your network from, get our latest special report on this crucial topic:

The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind

Don't let your organization be caught like a sitting duck! You've worked way too hard to get where you are today to risk it all due to some little cyberhack you didn't know about. Call us at **(561)969-1616,** or complete the form at www.palmtech.net/hackers/ and get your copy of this crucial preventive guide today – before your company becomes yet another social engineering statistic.

It's Time to Disaster-Proof Your Business

When and if disaster strikes, is your business going to continue to operate and cater to customers despite a possible long-term hardware failure or a network disruption? If you answer no or are not even sure what to do, you are part of a majority of business owners who have not considered disaster preparedness and the crucial role it plays in business survival. This post helps small or mid-sized businesses (SMBs) gain some understanding about Disaster Recovery (DR) and how important DR planning is today to protect against unexpected and costly downtime. Visit www.palmtech.net/disaster-proof/ or call us at **(561)969-1616** for assistance with Disaster Recovery!

Shiny New Gadget Of The Month:

Finally - An Easy Way to Control The Family Net

Got kids aged six to 16?

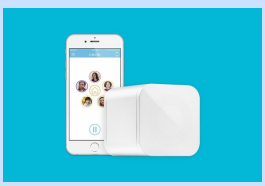
Circle With Disney is a new device that helps make Internet struggles at home a thing of the past. Imagine: no more negotiating with kids to get off the web and come to dinner (or get their homework done).

This 3½-inch white cube with rounded corners (it's not exactly a circle…) lets you control Internet usage around your house with a tap on your iPhone. (Android compatibility coming soon.)

With presets by age group, or custom controls, Circle helps you restrict who in your family surfs what, and when. It also tallies how much time each person spends on any site. You might even want to monitor your own Facebook or Pinterest time (or maybe not…).

Circle also lets you put your whole home network on pause, sets up in about five minutes and works with your router.

Just $99 at MeetCircle.com may be all you need to win your family back from the web – at least for a few minutes a day.



Bloatware Elimination in Two Simple Clicks

If the name wasn't clear enough, 'bloatware' is unnecessary manufacturer software that comes preloaded on new hardware. Just about no one likes it, and now Microsoft is giving us a tool to trim the fat. It may seem like small potatoes to anyone who hasn't spent an afternoon removing apps one by one, but for the rest of us it's a welcome blessing. Let's take a minute to examine Windows' new tool a little more closely here: www.palmtech.net/bloatware.

Microsoft Office 365 Ravaged by Ransomware

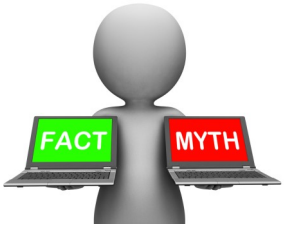
The Internet is a powerful platform that brings people together on a global level while giving them access to a wealth of information anytime they please. With the good, comes the bad - some utilize their skills in committing cyber crimes from the comfort of their own homes. Case in point, the recent Cerber ransomware attack that ravaged millions of Microsoft Office 365 users worldwide.

Visit www.palmtech.net/Ransomware-July/ to read what a security expert and Microsoft had to say about the matter.

I would love to send you a copy of my published IT survival guide entitled **"What Every Business Owner Should Know When Looking For A Professional, Competent, Honest and Dependable IT Service Company"**. To request your free copy, visit www.palmtech.net/#freebook to request your copy today!

Debunking Security Myths

Here are some of the biggest myths that many people believe about cyber security:



1) It won't happen to me; only big companies are targeted. False. Like most crimes, cyber thieves are opportunistic and actually attack the weakest targets. These are generally small businesses who have not invested in cyber security layers and training.

2) I have Anti-Virus software; I am fully protected. False. While, security software is a necessity, it is just one of several strategies that contribute to a layered approach to Cyber Security. The problem with Anti-Virus software is that it is only was good as the last update – which may have been several hours ago. Cyber threats are constantly changing to avoid detection so Anti-Virus software is largely a "reactive" technology that only detects "known" threats.

3) I have strong passwords so even if I get hacked they won't be able to get into my banking and other sites. False. Most Hackers "bug" your computers and install key-loggers as soon as they compromise a PC. They immediately start logging all of your usernames and passwords and everything you type.

4) I only open emails from people I know, so I can't get infected or scammed. False. Many hackers compromise the computers of the people you know and send emails to you to try and infect your computer as well. Training is the only way to better determine what a safe attachment looks like.

5) I only go to web sites that are safe so there is no way I can get infected. False. Websites are compromised every day and programmed to download or inject viruses. In addition, many hackers buy sound-alike names or misspellings of popular web sites in order to make you believe you arrived at the correct destination, only to trick you into infecting your computer.

6) A comprehensive Cyber Security System that includes multiple layers of protection, training, and proactive features that most Fortune 500 companies use is too expensive for my small business. False. The cost of security and training has come down to affordable pricing these days and starts as low as $10 per user.

Cyber-attacks are a constantly changing threat. If you put in the best security measures, they could be irrelevant in a very short time. Keeping up with the best security practices will help your business stay secure and make hacking difficult. The best protection is a proactive, all-encompassing internet security strategy. Contact PalmTech for a complimentary strategy session at **(561)969-1616**.

****Special offer for potential new clients with 15 or more computers. Through a special promotion with our Security training provider, we are able to give away free Cyber-Security training to the first 6 companies that request a complimentary Cyber Security strategy session. Offer good until 8/31/16. This innovative computer-based training will take your staff through a comprehensive program designed to help create awareness and prevent the most up to date and modern Cyber threats. Your staff is the weakest link. This is the single best tool to avoid a security breach and the best part is it's free. ****

"Thank you to you and your team for all your help with our office move. Both Rob and Mike (and of course yourself) are great and so quick to respond to any issues and questions. I enjoy working with everyone at PalmTech and look forward to our continued relationship. Please pass along my thanks to your team."

Molly Bunshaft
Assistant General Manager
City Place Towers

CITYPLACE TOWER

"This is Tom. He creates awareness."