RMS ASSOCIATES, INC.

Your RMSCare Package

July 2016
Issue 2707

What's Inside

As you can see from the photo, Claudia and I started out the summer with a bang! Most of you know we are avid tandem bikers and while on our annual BRAG (Bicycle ride across Ga), we had a front tire blow out as we were going down a hill. Needless to say, we are forever thankful for the helmets we were wearing which probably saved our lives. Claudia had multiple bruises and scrapes and I broke my collarbone requiring surgery but it really could have been a lot worse. We appreciate all the calls, texts and prayers!

Our RMSCARES article this month concerns keeping your children safe online which we thought was appropriate since they are out of school and have more time than normal on their various mobile devices.

Have a great summer, be safe and remember to wear your helmet when biking!!

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

Cont. on Page 3

RMS
Smart IT For Smart Business

RMSCARES:

KEEP YOUR CHILD SAFE ONLINE

Children are using online resources to socialize which have benefits but also risks. Adults can help reduce these risks by having open communication with their children discussing responsible online decision making. Below are a few suggestions to help keep your children safe:

1. Use filters and monitoring tools. These can be helpful but know they are not foolproof and can sometimes allow inappropriate materials as well as sometimes block materials a child may need access to. It is smart to monitor a child's browsing history even when using these tools.
2. Discuss with child what technologies they are using and have them show you. This is a good opportunity to check permissions on each to ensure they do not have access to address and phone number or any other personal information.
3. Make sure all photos children are using are appropriate.
4. Make sure your child knows they are never to have face to face meetings with people they have met on the internet.
5. Have your child tell you about any inappropriate, obscene or suggestive messages and immediately notify the National Center for Missing and Exploited Children at 800-843-5778.

6. Have your child tell you about any messages that hurt their feelings so you are aware of any cyber bullying. Children's feelings are so fragile and you need to be supportive and non-judgmental.
7. Make sure your child knows not to click on any links sent to them from strangers in emails or messages as this is one of the main ways devices receive malware and viruses.
8. Consider using a contract with your child for online usage. There are many samples online.

ICE (In Case of Emergency) on Cell Phones

In light of recent tragedies, we thought it a good time to make sure you have your contact and medical information on your cell phones. Many times, police and medical personnel do not even know a person's name when responding to an emergency situation and since most people always have a cell phone on them, this is the perfect place to find this information. But most of us have a password protected device which makes it impossible to get to this information. Did you know that you can put this information on your phone which is accessible even when your phone is locked?

On iPhones go into your Health App which is the white one with a red heart. Go to the tab for Medical ID and put your information in there. Then allow it to be shown on the emergency screen. You can then go to your password screen and hit emergency which will take you to a screen which says Med ID which will give any information you have saved such as emergency contacts and allergies.

There are similar features on other cellphones as well as apps such as ICE you can purchase. Check your device and make sure your emergency information is readily available!

Shiny New Gadget Of The Month:

What If Your Smartphone Had Wings

Video streaming from the air is about to get a whole lot more affordable.

It just so happens that the brains, gyroscope, GPS and camera aboard all those new drone cameras you may have seen can also be found in your smartphone...

Slip your smartphone into a PhoneDrone Ethos, and you have your own flying camera at a fraction of the cost of a fully equipped camera drone.

Worried about your smartphone taking a hit in the event of a crash landing? For about $50 you can buy a cheap smartphone with all you need to fly the Ethos.

Built-in mirrors enable you to shoot down, forward or to the side. You can preprogram it, or fly it manually from the ground. You can even control it with an Apple Watch.

It's scheduled to start shipping in September 2016, and "early-bird" discounts may be available at xcraft.io/phone-drone.

5 Ways to Spot a Social Engineering Attack

Cont. from Page 1

drive is plugged in, the person's or company's computer is infected, providing a point of access for the criminal.

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.

Don't let your organization be caught like a sitting duck!! For more on social engineering as well as other similar cyber threats you need to protect your network from, contact us at 770-988-9640.

Hootsuite, Buffer…or both?

Keeping in touch with new and current customers via social media can suck up your time. Social media apps Buffer and Hootsuite both aim to help you achieve more impact in less time. So which one is right for you? While Hootsuite offers a full-featured social media dashboard, Buffer focuses simply on prescheduling your content. When it comes to managing posts and tracking which ones perform best, Hootsuite is the way to go. Yet Buffer gives you more timing flexibility by allowing you to pick when your posts get published, regardless of when you add them to the queue. Choose either of these apps based on your posting and tracking needs – and consider using them both.

buffer

hootsuite

RMS Associates, Inc.

1850 Lake Park Drive
Suite 200
Smyrna, GA 30080
www.rmsatl.com
Phone: 770.988.9640
Fax: 770.988.9695

RMS

Smart IT For Smart Business

Services We Offer

- Cloud Solutions
- Technology as a Service
- Total Business Continuity Protection
- Proactive Network Maintenance/Monitoring
- Network Design & Implementation
- Network Security
- SPAM & Virus Remediation & Prevention
- 3CX VOIP Phone System

Happy Birthday, USA!!

"Like" RMS Associates, Inc. on FaceBook to get the latest IT news, tips, and even an occasional laugh at facebook.com/RMSAssociates

Like Us On facebook

Blog

Check out our blog at mysupportguys.com/blog

We Would Love To Hear From YOU!

If you have noticed an RMS associate going above and beyond the ordinary for you either on-site or over the phone, please let us know so we may reward them! Please e-mail me at rrowe@rmsatl.com. Thanks!

Subscribe to our RSS feed at mysupportguys.com/feed.

This newsletter is printed by Imagers, a long time client and friend. If you need quality specialized printing, please call them at 404-351-5800 or see them on the web at www.imagers.com.

IMAGERS Since 1947