RMS ASSOCIATES, INC.

Your RMSCare Package

September 2019
Issue 2832

What's Inside

RMS
Smart IT For Smart Business

September already?! I guess this means the leaves are about to begin falling soon enough and everyone will need to start pulling their sweaters out from the back of their closets. We hope you've all enjoyed the sunshine and warm weather and you're preparing for bonfires and corn mazes.

This is the second month of the new RMS newsletter format. We have begun emailing our monthly newsletter to our contacts. If you know anyone who would like to receive our newsletter, they can subscribe by reaching out to us at newsletter@rmsatl.com. Thank you!

Georgia Hit Again

It's getting hard to keep track of how many times Georgia's been hit with ransomware in the last year. The most recent? Attackers preyed on the Georgia Department of Public Safety (DPS). The DPS encompasses the Georgia State Patrol, Georgia Capitol Police, and the Motor Carrier Compliance Division, which carries out safety inspections. The DPS was forced to bump all servers offline while the Georgia Technology Authority investigated the attack.

State troopers have had to resort to old-school law enforcement. If a trooper is writing a ticket, they might be doing it with a pen and paper instead of a tablet. Or if they're looking up a license plate, they would radio it into a dispatcher. Georgia State Police, Georgia Capitol Police, and Department of Motor Vehicle Safety have all had to switch to an older radio and phone system.

It's hard working in IT for Georgia these days. **It's been a mad scramble of attacks and costly mop-ups for the state.** The first attack hit the city of Atlanta in March 2018 and destroyed years of police dashcam video and froze their systems. They were rescheduling court dates, police and other employees were writing out reports by hand, and residents couldn't go online to pay their water bills or parking tickets.

This attack was only one out of **a crime spree that hit 200 victims**, including hospitals, municipalities, and public institutions. In Georgia's court systems, the government of Henry County in Georgia – the second fastest growing county in metro Atlanta, and the police department in Lawrenceville, Georgia were all hit by malware in July too. **So how do you protect yourself?**

- Pick strong passwords. And don't re-use passwords, ever.
- Make regular backups. They could be your last line of defense against a six-figure ransom demand. Be sure to keep them offsite where attackers can't find them.
- Patch early, patch often. Ransomware like WannaCry and NotPetya relied on unpatched vulnerabilities to spread around the globe.
- Lock down RDP. Criminal gangs exploit weak RDP credentials to launch targeted ransomware attacks. Turn off RDP if you don't need it, and use rate limiting, 2FA or a VPN if you do.
- Use anti-ransomware protection. Firewalls are designed to combat ransomware and its effects.

Who's Listening In?

@NakedSecurity

Have you ever asked Apple's personal voice assistant, Siri, if it's always listening to you? If so, you presumably got one of its cutesy responses. *"I only listen when you're talking to me."* Well, not just when you're talking to Siri, actually. **These voice assistant devices get triggered accidentally all the time**, according to a whistleblower working as a contractor with Apple.

The contractor said that the rate of accidental Siri activations is quite high – most particularly on Apple Watch and the HomePod smart speaker. Those two devices lead to Siri capturing the most sensitive of all the data that's coming from accidental triggers and being sent to Apple, where human contractors listen to and analyze all kinds of recordings that include private utterances of names and addresses.

There have been countless instances of Apple's Siri voice assistant mistakenly hearing a "wake word" and recording **"private discussions between doctors and patients, business deals, criminal dealings, sexual encounters" and more.** Those recordings often reveal identifying information: "*These recordings are accompanied by user data showing location, contact details, and app data."*

If you aren't muttering, "So, what's new?" by this point, you haven't been paying attention to the news about how much these devices are overhearing and how little the vendors are worrying about the fact that it's a privacy violation. **First, it was Amazon listening to us. Next it was Google, and now Apple has made it a trifecta.**

Client Spotlight:

Kingsley Franek LLC

Julie Kingsley was a senior in college before she declared her major, but she had never taken a semester without a math class, so she knew she wanted to do something with numbers. Stephanie Franek's mother worked in accounting, so she would always help her at work and grew into that career. She says that although taking the CPA exam wasn't fun, it has been rewarding.

This dynamic duo knew each other personally before they began working together professionally. Stephanie was working at a large regional firm before she decided to leave and work with Julie at a smaller firm. In June 2018, the two left the firm they were at and started their own together. Since then, they've been growing more than they could have imagined and all by word of mouth. They haven't done any marketing or advertising; everyone just rallied behind them.

Julie deals more with the business clients, while Stephanie works with estates and trusts, and they both deal with individuals. During the tax season, they power through the day every day to try to get all the tax returns completed. Once tax season is over, they deal with offsite CFO services and work on strategy with businesses and owners to stay on top of things. Tax planning helps prevent clients from being shocked in 2019 when they owe money.

They have decided to keep their company smaller so that they can remain involved and keep the personal touch that they have developed. Once you get too big, you lose the intimate aspect that people are looking for. Julie says that there are clients she's had since she started in her 20's. "We've had kids at the same time and grown our businesses together through the years, so it's been really cool to develop those friendships. It makes you more invested when you have personal relationships. We definitely care about our clients and want them to be successful."

RMS has been a life saver and godsend to Kingsley Franek. In less than a week, they were completely up and running with their IT. Julie says, "It's been completely painless, and IT has never been painless for me in my entire life."

(Julie Kingsley pictured right, Stephanie Franek left.)

Too Hot to Handle

What do cigarettes, candles, and faulty electrical appliances have in common with one another? They are among the top causes of house fires in the US. However, it seems there is another often overlooked cause that should be near the top of the fear list... hair straighteners.

They get hot (235 degrees Celsius, or 455 degrees Fahrenheit) and are easy to leave turned on inadvertently. Which brings us to one particular expensive hair straightener product, the Glamoriser Smart Bluetooth straightener, which offers up yet another dismal example of how not to implement the Internet of Things (IoT) in an already risky product.

As its name implies, it uses Bluetooth to communicate with a Glamoriser app and, as with a growing number of previously dumb and perfectly satisfactory consumer products, it's SMART – by now most readers will know what's coming next.

Researchers found enough weaknesses to remotely override the product's chosen temperature setting as someone is using it. That is, raise the temperature and keep it at this level for longer than would be realized by its owner.

The log files that are part of its software design were far too open, allowing anybody with a little time on their hands to infer the commands to do dangerous things.

In fact, it seems a hacker might not even need to do that – they could just fire up the app on their own phone and do the whole thing from there as long as the owner wasn't connected or is out of range.

Putting a Stop to Bullies

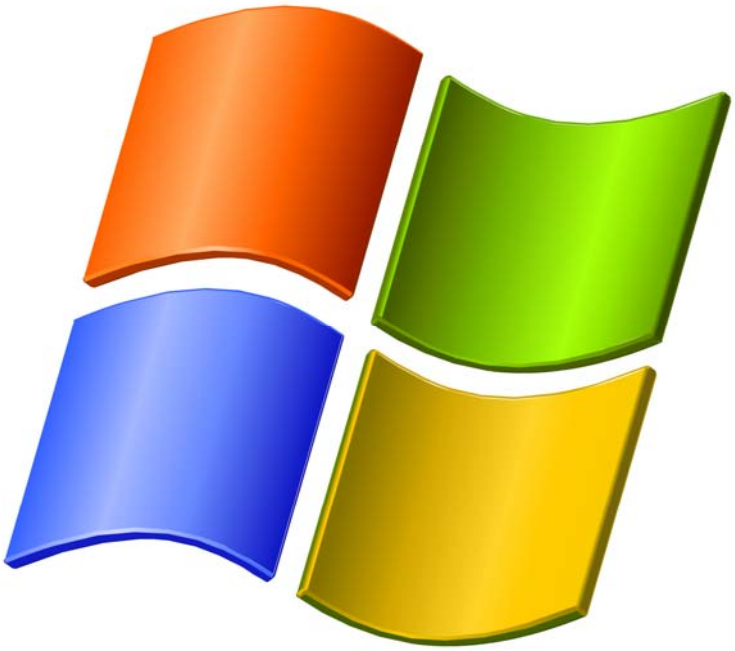
Instagram is now using artificial intelligence (AI) to detect speech that looks like bullying and will interrupt users before they post, asking if they want to stop and think about it first. The Facebook-owned platform also plans to soon test a new feature called "Restrict" that will enable users to hide comments from specific users without letting them know that they've been muted. Think of it as a smarter way to block bullies and trolls.

Instagram chief executive Adam Mosseri said the company "could do more" to stop bullying and help out its victims: "*We can do more to prevent bullying from happening on Instagram, and we can do more to empower the targets of bullying to stand up for themselves. These tools are grounded in a deep understanding of how people bully each other and how they respond to bullying on Instagram, but they're only two steps on a longer path.*"

Can you really reason with bullies? Sometimes. Mosseri said that giving users a chance to reflect has been effective in talking some people out of spewing their bile. "*From early tests of this feature, we have found that it encourages some people to undo their comment and share something less hurtful once they have had a chance to reflect.*"

Any improvement could literally save lives. Instagram has been under pressure for bullying following widely reported suicides, such as that of 14-year-old Molly Russell, who took her own life in 2017. Her family blamed Instagram in part for her death: when they looked into her Instagram account, they found distressing material about depression and suicide. Molly's father said that Instagram "helped kill my daughter."

Since he took over the reins at Instagram in October 2018, Mosseri pledged that he would wage war on bullying. He's said that Instagram wants to lead the industry in the fight. Thus, the announcement of the two new features: the two first steps in this battle. I don't envy Instagram this work. Research makes clear that bullying comprises a tangled web of words, actions, inactions, images, group behavior and subtle slights. Instagram, good for you for stepping up to the plate to deal with these issues and do whatever you can to keep kids safe. Let's hope we see more progress, from more companies, and that this battle moves to and stays at the top of their priority lists.



Time is Running out!

Windows is Flatlining

The year 2020 is fast approaching, and with that comes the end of the Windows 7 lifecycle. "**End of life**" means Microsoft will discontinue all support and all updates, including security updates. What does this mean for you? If you are using Windows 7, 8, 8.1 or Server 2008, you will be severely vulnerable to security and maintenance issues. Contact RMS as soon as possible to upgrade your equipment and ask about next steps.

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
- Cyber Security
- Help Desk
- Hosted Phone Systems

87% of people have back pain.

The other 13% have no computer.

Like us on Facebook to get the latest IT news, tips, and even an occasional laugh.
facebook.com/RMSAssociates

Follow RMS Associates on Twitter at twitter.com/rms_atl for even more content.

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 can reward them! Email me at rrowe@rmsatl.com. Thanks!