RMS ASSOCIATES, INC.

Your RMSCare Package

Mar. 2016
Issue 2703

What's Inside

Happy Spring!

It looks like we've made it through another winter and spring is in the air. We're having beautiful weather, flowers are in bloom, and the pollen hasn't gotten too bad yet. Hopefully your year is off to a wonderful start!

We are starting a new series this month called **RMSCares.** *There will be articles aimed at keeping you, your business, your family and your friends safe out there in the big, bad Internet-connected world. I had a family member's Facebook account get hacked recently, so I thought an article about Facebook security was the perfect way to kick off* **RMSCares.**

I hope you all have a great March!

Introducing RMSCares

Who is old enough to remember the days before the internet? My business, Just like most businesses out there, depends on it. There are times I like a little escape from the digital world, but, unfortunately, as a small business owner of an IT company, I can't afford to disconnect for too long.

Streaming music, movies, news, cat videos, house lights, refrigerators, Fitbits, the thermostat in your home, self-driving cars, cloud computing—the Internet is so entwined in our lives we can hardly ever get away. We can now access just about anything as long as we have WIFI access or a cell phone. Kids grow up today with their heads buried in their devices. They'd rather text than talk.

Face it, the connected world permeates our lives more every day and is the greatest boon to productivity as well as the greatest threat to our security. The threats are never going away and are just getting worse and worse.

We have seen large companies (Hollywood Medical, Target, Scottrade, BlueCross BlueShield, etc.) hit with various cyber-attacks and we see it almost every day with users or clients that get hit with attacks or follow the wrong link.

From stealing our identity to holding our files for ransom, we are ALL targets. Because the threats are constantly changing and there are so many ways the bad guys are trying to steal from each of us, I decided to devote a portion of each month's newsletter to protecting yourself, your family and your business from these threats.

RMS
Smart IT For Smart Business

Relying On A Good Luck Charm?

Carrying a four-leaf clover might work for leprechauns. But when it comes to Internet abuse by employees, you're going to need more than sheer luck…

Did you know that…

- 70% of all web traffic to Internet pornography sites occurs during the work hours of 9 a.m. – 5 p.m.
- Non-work-related Internet surfing results in up to a 40% loss in productivity each year at American businesses.
- According to a survey by International Data Corp (IDC), 30% to 40% of Internet access is spent on non-work-related browsing, and a staggering 60% of all online purchases are made during working hours.

The list goes on, and the costs to your company can be staggering.

What types of web sites present the greatest risk? Categories include abortion, alcohol, dating, death/gore, drugs, gambling, lingerie/swimsuits, mature, nudity, pornography, profanity, proxy, suicide, tobacco and weapons.

Risks these types of web sites expose your business to include malware, viruses, fraud, violence, lawsuits, loss of confidential and/or proprietary data and more. Even social sites, while perhaps not quite as risky, can have a major impact on productivity.

Barriers that once stood at the edges of your office network have been annihilated by digital media.

Web content filtering is now crucial to network security – not to mention employee productivity – in this emerging environment. It can be deployed in a number of ways, but basically they boil down to two: inline and endpoint filtering.

Inline Web Filtering
One way to filter web content is to control it at the entry point or gateway to your network. This technique intercepts all web traffic and applies filters that allow or block web access requests. Because the entire network is filtered, no access to the user's device is required.

With inline web filtering, there's no need to expend resources managing content at each endpoint – your employees and their computers, whether desktop or mobile. Inline filtering not only saves bandwidth, it goes a long way toward mitigating cyber threats. For securing activities that take place within your network, it's a critical and potent strategy.

Yet, with the shift away from traditional office-bound work routines to a work-from-anywhere culture, the effectiveness of inline filtering has diminished. When employees access the web outside your network's gateways – via home networks, hotels, coffee shops, etc. – their devices become vulnerable to attack.

And any employee can carry an infected machine into and out of your company's building and network on any given day, exposing your entire intranet to infections. And that's why so many companies are moving to endpoint-based web filtering to complement their inline filtering.

Endpoint-Based Web Filtering
Endpoint-based filtering protects employee devices from infections, no matter where they connect to the web. Software at the endpoint – your employee's device – carries a predefined filtering policy from the central server that can be intranet-based or cloud-based.

The endpoint filter is then updated periodically from your company network. This method assures that web filtering is always active, no matter which gateway the machine connects through. The downside is that it must be rolled out and maintained at all endpoints.

That being said, one advantage of endpoint-based filtering is that it addresses stringent employee privacy regulations that are quickly becoming the norm in Europe and elsewhere around the world. Because it keeps browsing-pattern information within the user's device, endpoint-based filtering provides a fairly non-intrusive way to handle employee privacy concerns.

And finally, while endpoint-based filtering really is the only way to protect a network without boundaries, as most companies now have, ideally it works hand in glove with inline filtering.

Forget the Charms – You Can Bet On This

We highly recommend rolling out not only inline and endpoint filtering, but also an effective training program for your staff to encourage best practices and assure compliance with your company's web security policies and procedures.

Want to make sure all gaps are sealed and you won't have to count on a four-leaf clover, a rabbit's foot or knocking on wood to keep your network secure? Contact us today at (770) 988-9640 or rrowe@rmsatl.com for a customized Web Content Filtering Review.

Shiny New Gadget Of The Month:

Keeps You In Touch, Could Save Your Life

If you fly often for business, a satellite messenger may be just the thing to stay in the cloud when you're above the clouds. And if your travels for fun take you into the wild, it could literally be a lifesaver.

Just ask retired Houston firefighter Michael Herrara. After breaking three ribs and his collarbone in a hard fall from his dual-sport bike in a remote area in Alabama, he hit the SOS button on his messenger. Within 40 minutes an ATV was on hand to transport him to a trauma center.

Features to look for in a satellite messenger include data speed, battery life, coverage areas, size, weight and ease of use.

And, of course, an SOS button.

RMSCares:

Keep Your Facebook Safe

As of December 2015, there are 1.55 billion monthly active Facebook users worldwide. 1.01 billion people log in daily and 5 new profiles are created every second. With so many people using Facebook, it is no wonder that hackers are at work to compromise accounts. If it hasn't happened to you, the likelihood is that someone you know has been hacked. So how do you keep hackers off your account? Here are some great ideas to keep you safe!

1. Create a strong, unique password that you only use for Facebook. It should contain capital and small letters, numbers and symbols. (I use a password manager to create and store mine.) To change your current password, go to Settings, General, Password.
2. Attach your mobile number to your account so if the need arises you can use it to reactivate your account. Go to Settings, Mobile to set it up.
3. Activate login notifications AND approvals. Notifications alert you via text whenever you (or a hacker) tries to log into your account. Approvals send you a unique code to enter every time you log in to provide two-factor authentication (something you know, plus something you have). Find these under Settings, Security.
4. Disconnect previous browsing sessions. You can see everywhere you have active browsing sessions by going to Settings, Security, Your Browsers and Apps. You can end all activity for any device you don't recognize.
5. Log out when done. If you don't, anyone that gains access to your device will be able to get into your account without having to log in. And when you login, uncheck the keep me logged in box so that you have to enter your email and password every time.
6. Be Link Aware! Be aware that whether o FB or anywhere else, you must be careful before clicking on any links!! Even if the link appears to come from your friends it may be from a scammer. They send you private messages, links on your timeline, etc. so never click these unless you are sure it is safe!
7. When using your computer to access Facebook, make sure your browser is updated so that it has the latest security updates.

If you use these suggestions, you should be able to enjoy Facebook with the other 1.55 billion users and lower your risk of getting hacked. Above all, stay vigilant. The threats change continuously and you should stay aware of the changing risks.

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

"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