TechTelegram
powered by neoRhino

What's New

This fall, neoRhino is thrilled to announce that for its second year we will be participating in Extra Life: an annual gaming charity event to support children's medical foundations across the country.

We will be announcing the dates of when we will be streaming online for donations, as well as swag you can get for helping us reach our goal to help sick kids as all proceeds will go to the Texas Children's Hospital. Be sure to follow our social media pages and website for details or you can click the link below to donate!

neoRhino IT SOLUTIONS + Extra Life

September 2017

This monthly publication provided courtesy of David Pense, Network Engineer of neoRhino IT Solutions.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

7 Critical IT Security Measures Every Business Must Have In Place NOW

Are You a Sitting Duck?

You, the CEO of a small business, are under attack. Right now, extremely dangerous and well-funded cybercrime rings are using sophisticated software systems to hack into thousands of small businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account.

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot?

In fact, the National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing and mobile devices, and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these 7 security measures in place.**

1. The #1 Security Threat To ANY Business Is... You! Like it or not, almost all security breaches in business are due to an employee clicking, downloading or opening a file that's infected, either on a web site or in an e-mail; once a hacker gain's entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (e-mails cleverly designed to look like legitimate messages from a web site or vendor you trust) is still a very common occurrence – and spam filtering and anti-virus cannot protect your network if an employee is clicking on and downloading the virus. That's why it's CRITICAL that you educate all of your employees on how to spot an infected e-mail or online scam. Cybercriminals are EXTREMELY clever and can dupe even sophisticated computer users. All it takes is one slip-up; so constantly reminding and educating your employees is vital.

2. Require STRONG passwords and passcodes to lock mobile devices. Passwords should be at least 8 characters and contain lowercase and uppercase

Continued on pg.2

letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

3. Keep your network and all devices patched and up-to-date. New vulnerabilities are frequently found in common software programs you are using, such as Adobe, Flash or QuickTime; therefore it's critical you patch and update your systems and applications when one becomes available. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

4. Have An Excellent Backup. This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

5. Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT resource. The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is a known username and password. Employees are now even asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything.

But this trend has DRASTICALLY increased the complexity of keeping a network – and your company data – secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility); your biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud application. So if you ARE going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

But here's the rub: Most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your company. Our suggestion is that you only allow employees to access work-related files, cloud applications and e-mail via company-owned and monitored devices, and never allow employees to access these items on personal devices or public WiFi.

6. Don't Scrimp On A Good Firewall. A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance.

7. Protect Your Bank Account. Did you know your COMPANY'S bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account!) Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

Set up e-mail alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. If you discover even 24 hours after it's happened, you may be out of luck. That's why it's critical that you monitor your account daily and contact the bank IMMEDIATELY if you see any suspicious activity.

Second, if you do online banking, dedicate ONE computer to that activity and never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc. with that PC. Remove all bloatware (free programs like QuickTime, Adobe, etc.) and make sure that machine is monitored and maintained behind a strong firewall with up-to-date anti-virus software. And finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account.

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit."

Give us a call at (877) 85-RHINO and let us prevent your business from being a victim.

Services We Offer:

- On-Site Help Desk Support
- On-Site Network Engineering including:
  - Cisco
  - Microsoft
  - Hyper-V & VmWare
- Disaster Recovery & Business Continuity
- Remote Managed Services
- Network Cabling
- Architecting and Implementing Enterprise Level Hardware Solutions

Give us a call today at 281-779-4850 to discuss your needs.

Free Report: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…

This report discusses in simple, non-technical terms the pros and cons of cloud computing, data security, how to choose a cloud provider, as well as three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated.

Even if you aren't ready to move to the cloud yet, this report will give you the right information and questions to ask when the time comes.

Receive your FREE report today by sending us an e-mail at info@neorhino.com or call our office at (281) 779-4850.

What Should Come First?

Success Or Happiness?

Sonja Lyubomirsky, psychology professor at the University of California and expert on the psychology of human happiness, recently analyzed the results of 211 different studies. She investigated these questions: "Are happy people more successful?" and "Does happiness precede success?" The results of their extensive research showed that, indeed, happiness tended to lead to greater success.

This shouldn't come as a surprise for most of us. After all, happy people have more positive moods, and positive moods motivate us to work actively to reach new goals. This results in happy people being more productive, more innovative, better communicators, more respected, more appreciated, more optimistic, energetic, likable, confident, and sociable — quite the impressive list! Not only that, but happy people experience less stress. With approximately 1 million workers per day missing work due to stress, it's evident that there are a lot of unhappy people out there.

When companies downsize their staff, a greater workload is placed on the employees who stay. The greater the demand placed on employees, the greater the potential for even more stress, leading to decreased happiness. At some point, the priority of trying to be happy takes a distant second place to that of merely surviving. "I don't have time to worry about being happy," we say. "I'm too busy working."

I remember, years ago, when the eccentric billionaire Howard Hughes died, a reporter asked someone in the know, "How much money did Mr. Hughes leave behind?"

"All of it," the person replied.

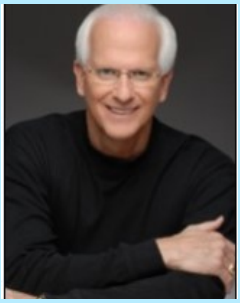
What a great answer. No matter what we accomplish in our lives, we don't get to take any of it with us when we go. That's why, if there's one thing I could possibly share with you today, it's to stress the importance of your own happiness. If you maintain a positive attitude and strive to be truly happy, it will energize you in everything you do. Work on it daily and lighten up a little. Laugh more. Make a point, daily, to count your blessings. Catalog the things that go right in your life. Be grateful and optimistic. If you can manage to consciously make the choice to be happy, your stress levels will decrease, your productivity will increase, and everyone around you will be better off, more eager to talk to you, and motivated to do their own work with a smile.

Remember, happy people have problems, too, they just handle them differently.

There's nothing worse than a person who's a "professional depressor." You know the type, the Debbie Downers who can't seem to find the positive in anything or, even worse, find the negatives in a positive situation. Happiness starts with the words you speak yourself. So, before opening your mouth to whine about the traffic, complain that the store clerk was a total jerk, shout about your aching body or your parking spot or how you missed your flight, understand that you are essentially reliving the bad events that you're complaining about. You've multiplied their effects and given them power over your life. Don't do that! It brings you down again and brings down everyone you're sharing it with. It's not fair to whomever you're talking to.

At the end of the day, our happiness and the happiness of our friends and families are all that matters. Everything else is commentary.

Robert Stevenson, along with being a best-selling author, is among the most successful public speakers in the world.



His years of service-minded experience owning and running numerous companies have given him the real-world knowledge to help fellow business owners thrive.

This App Could Save Thousands of Lives

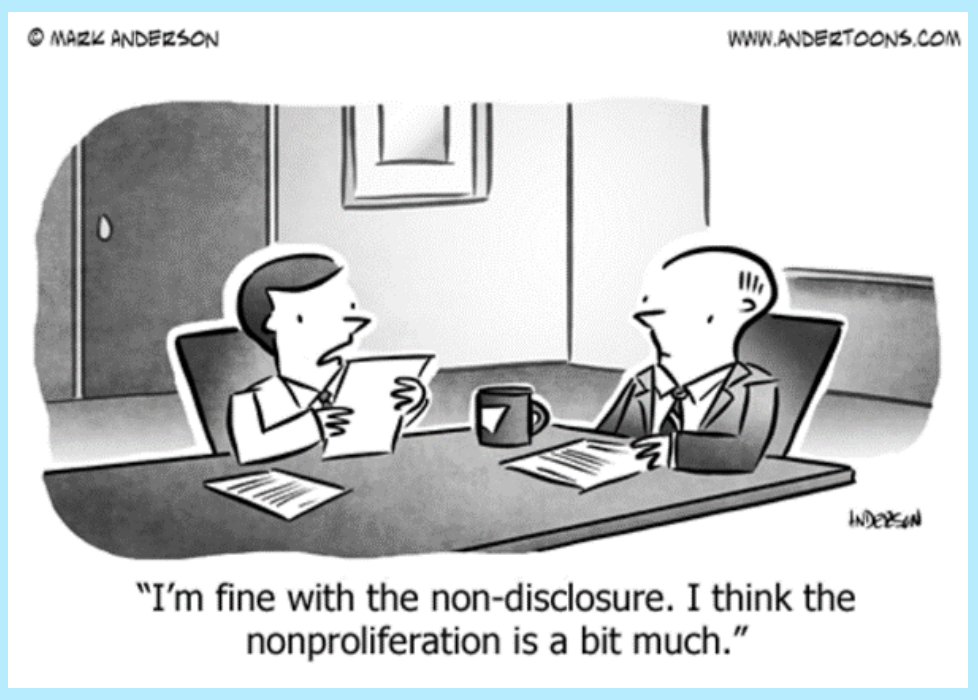
In the event of cardiac arrest, every minute that passes without CPR and defibrillation lowers the victim's chance of survival by 7% to 10% percent according to the American Heart Association. The new First Responder phone app, created by the European Heart Rhythm Association, was designed with this in mind. It uses GPS tracking to locate nearby trained responders to administer aid, notify emergency services, and direct rescuers to the scene of the incident. During trial runs in Lubeck, Germany, 36 percent of cardiac arrests were addressed by an app rescuer three minutes before professional responders arrived on the scene. *Digitaltrends.com 6/23/17*

It's A New Quarter, You Need To Do This Immediately

When it comes to the security of your business, it's best not to take any chances. We recommend changing your password, at least once every three months. Use both lowercase and capital letters in your password along with numbers and symbols. Avoid using the same password for different accounts — you don't want a Facebook hacker to gain access to your Amazon account!

5 Ways You Can Leverage New Technology To Stay Ahead Of The Competition

Use new AI technologies to your advantage. Automate back-office tasks to regain work-life balance. Have your AI sort through unreadable stacks of data to help you expedite important business decisions. Employ machine learning to parse data from your clients in order to create a personalized experience. Use it to identify patterns in customer behavior, giving you ideas about how to improve your product. You can even use an AI-powered personal assistant to handle everything from running your calendar to scheduling meetings. *inc.com 7/6/17*



Do These Simple Steps Throughout The Day To Keep Sitting From "Killing" You

Lately, everyone is abuzz about the latest silent killer: sitting. Wellness coach Roland Denzel recommends breaking up every 25 minutes of work time with a five-minute break, stretching and moving around to get the blood flowing. Lift your arms overhead, lean your body from side to side, and lean far forward. If you can, take a short walk. One way to keep moving throughout the day is, instead of messaging on Slack or picking up the phone, walk over to your colleague's space and talk in person. Jill Henderzahs-Mason, PT at the Mayo Clinic, says, "At the bare minimum, you should get up and change positions for at least a minute or two."