TechTelegram
powered by neoRhino

What's New

On May 31st & June 1st, 2017, neoRhino IT Solutions will be exhibiting at the Women's Business Enterprise Alliance (WBEA) Expo in Houston! Come by our table and learn about how we can help your business succeed and see what's coming from us soon.

Also, click any of the links below to follow us on social media, where we provide daily updates of what's new in tech & security as well as what's going on in our world. Be sure to subscribe to our YouTube channel to see our videos once they are uploaded. Thank you & enjoy!

May 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!"

No matter how "bomb-proof" we make your network, you and your employees can still invite a hacker in if you click on a link or open an attachment in an e-mail sent by a cybercriminal. Some spam is obvious (can you say, "Ray-Bans at a discount"?) but others are VERY cleverly designed to sneak past all the filters and trick the recipient into opening the door.

A "Phishing" email is still the #1 way hackers circumvent security. It is critical that you and your employees know how to spot a threatening email. Here are four types of e-mail ploys you should be on high alert for.

The Authority E-mail. The most common phishing e-mails are ones impersonating your bank, the IRS or some authority figure. The rule of thumb is this: **ANY** e-mail that comes in where 1) you don't PERSONALLY know the sender, including e-mails from the IRS, Microsoft or your "bank," and 2) asks you to "verify" your account should be deleted. Remember, ANY important notification will be sent via old-fashioned snail mail. If it's important, they can call you.

The "Account Verification" E-mail. Any e-mail that asks you to verify your password, bank information or login credentials, OR to update your account information, should be trashed. No legitimate vendor sends e-mails asking for this; they will simply ask you upon logging in to update or verify your information if necessary.

The Typo E-mail. Another big warning sign is typos. E-mails coming from overseas (which is where most of these attacks come from) are written by people who do not speak or write English well. Therefore, if there are obvious typos or grammar mistakes, delete it.

The Zip File, PDF or Invoice Attachment. Unless you specifically KNOW the sender of an e-mail, never, ever open an attachment. That includes PDFs, zip files, music and video files and anything referencing an unpaid invoice or accounting file (many hackers use this to get people in accounting departments to open e-mails). Of course, ANY file can carry a virus, so better to delete it than be sorry.

Call Us To Cut Down On 99% Of The Spam E-mails You're Getting.
We can perform a spam-protection analysis remotely or on site for your business. Simply contact us today at info@neorhino.com or call us at (281) 779-4850 to reserve yours.

Do it now... before a ransom demand -or worse - shows up in your inbox.

Continued pg.2

10 Million Passwords Became Public; The Findings Were Astonishing

Keeper Security, a company specializing in secure password management, conducted a review of the 10 MILLION passwords that became public in 2016 from various hacker attacks. What they found was shocking.

One of the most common passwords used was "*123456*" with the second being *QWERTY*, which are the top keys on a keyboard - and these were used by webmasters to "protect" the digital keys to your website's kingdom!

Another very common mistake was that many passwords were six characters or shorter, which any brute-force password-cracking software can descramble in SECONDS. So while remembering all those passwords and changing them is a major pain in the butt, getting your website hacked or your bank account wiped out is even worse.

One of the most common passwords used was "123456" with the second being QWERTY, which are the top keys on a keyboard – and these were used by webmasters to "protect" the digital keys to your website's kingdom!

Our advice is to create a password that:

1) Is AT LEAST 12 characters long,
2) Contains uppercase and lowercase letters,
3) **And** contains numbers and characters such as ! or #.

Of course, if you need help in remembering and organizing your passwords, there are several very good password management software tools such as LastPass and RoboForm.

These password keeper services, as well as following those three strong password requirements, can keep all the passwords secure AND make it easy to cut off an employee's access to various passwords and sites easily if they are let go or they quit.

Microsoft Office Zero-Day Attack Hides Malware Inside Fake Word Documents

In April, an exploit that used fake versions of Office files such as Word documents made its way around the world, potentially affecting all versions of Office including Office 365.

According to McAfee, who reported the critical attack, once the fake Word doc is opened by the user, an HTML application is downloaded from the attacker's server, then executed as a cleverly disguised malware file. Once the file has sunken deep into the computer, the hacker receives full code execution on your computer. Microsoft has since issued a patch for the vulnerability, but this incident shows the heavy importance of keeping your Office programs up-to-date as well as the best practice of the prevention of opening files from untrusted sources. McAfee's full report can be found here.

neoRhino's Microsoft-Certified Consultants and Engineers can absolutely assist in keeping your Office 365 accounts managed, secured and up to date. Give us a call at **(281) 779-4850** or email us at info@neorhino.com and we can strengthen your business' Office 365 infrastructure to its full potential.

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.

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

How To Get Your Employees To Commit To Achieving BIG Goals

By Dr. Nido Qubein

How do great leaders inspire others to commit themselves to their goals? It's not just that they have charismatic personalities, or that they give a lot of high-energy motivational talks. What they do is communicate their vision so effectively that other people adopt it as their own.

Inspiring people is what great leaders like John F. Kennedy did best. In the early '60s, President Kennedy set his sights on putting a man on the moon and told the American people, "We can do it!" He said it with such conviction that people believed it and committed themselves to making it happen. And, sure enough, we made it to the moon. That's the formula for any leader to inspire commitment: clear goals, a solid plan of action and a strong conviction.

Of course, leadership takes more than inspiration. One of the most insightful tips I learned about leading others is that **people do things for their reasons**, not for your reasons or for mine. So how can you move past the empty rhetoric and translate your vision into concrete actions your people can identify with and get excited about? Let me suggest seven proven techniques for building a solid team:

Recognize outstanding performance.

Everyone likes to look good in the presence of their peers. When you find someone doing something right, make sure you give them public recognition. If they do really well, throw in a tangible benefit, bonus or gift. It will boost the whole team's mood and productivity.

Constantly ask for input and ideas.

People are usually much more enthusiastic about supporting decisions and plans they helped create. So get ideas and input from any person whose job will be affected by any upcoming decision. When your team quits talking about the company, and starts talking about our company, you know you've got a team.

Give them proper coaching and training.

If you're lucky, you'll have one or two people who can plow into almost anything with little to no instruction from you. But most people need a lot of training, mentoring, coaching and guidance in the beginning. Without that, people can become frustrated quickly and lose interest in hitting a big goal.

Just be a nice person.

Make people feel valued and important by treating them with dignity and respect. If you have to correct someone's mistake, do it privately, and counter it with a sincere compliment. Attacking someone and belittling them is never a useful way to get the most out of a team member.

Get rid of underperformers fast.

You've heard the phrase "Hire slow and fire fast." This is a piece of advice we all need to keep in mind. Make sure you weed out the bad apples before they spoil your culture. That's because keeping someone on the team who is not performing, is not trying and is clearly not doing their job sends a message that it's okay – which is incredibly demotivating to high performers who are striving to hit big goals.

It takes a lot of patience and effort to build a solid team of people who will share and help you fulfill your vision, but the results will be well worth all you put into it.

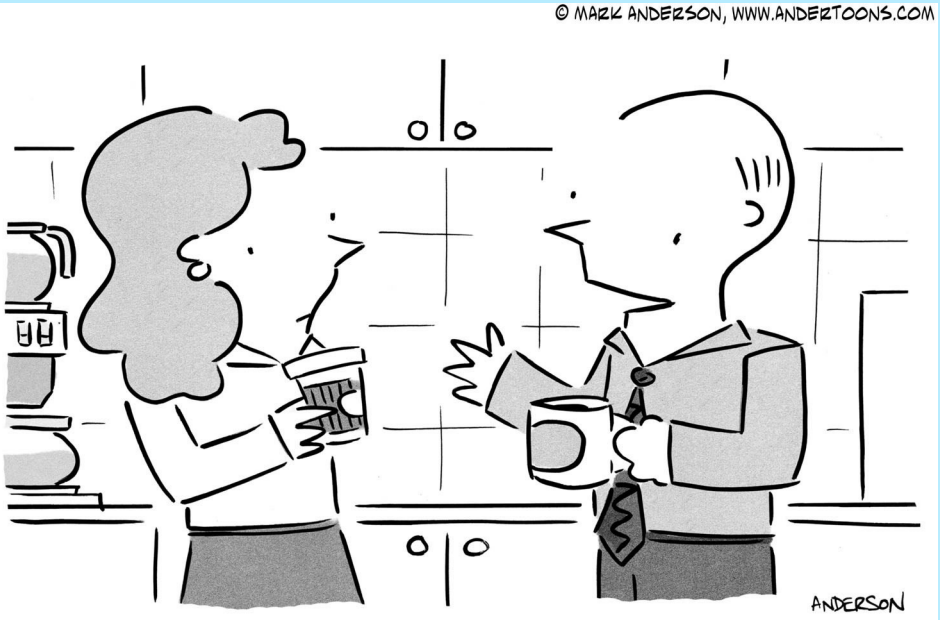
Dr. Nido Qubein is president of High Point University, an undergraduate and graduate institution with 4,300 students from 40 countries. He has authored two dozen books and audio programs distributed worldwide. As a business leader, he is chairman of the Great Harvest Bread Company, with 220 stores in 43 states.

As a professional speaker, Dr. Qubein has received many distinctions, including the Golden Gavel Medal, induction into the International Speaker Hall of Fame and as the founder of the NSA Foundation in Arizona.

Want More Customers? Use This FREE Google Marketing Trick. If you want your business to show up first when potential customers are searching for you or for the services and product you provide, you MUST claim your business on Google. This free service allows you to enter data about your company, products, services and location that will greatly improve your search-engine ranking. Make sure you enter COMPLETE data and information, including hours of business, your phone and photos of your location. You can even post internal photos of your store or office. Remember, Google displays search results based on relevance, so the more specific information you can provide on what you do, the better your chances are of coming up in search-engine rankings.

For more information, just search "Google My Business" to get started.

The Latest Way Hackers Are Stealing Your Identity That You Won't Believe. Researchers at Japan's National Institute of Informatics report that fingerprints can be easily reproduced from photos without using any advanced technology. If the image is clear and well-lit, fraudsters can mimic your fingerprints. Swiping biometric data is nothing new. In 2015 a famous hacker recreated German chancellor Angela Merkel's iris from a photo to unlock a test. The problem is, once biometric data is resold on the dark web, the risk it will be used against you persists for life. New technologies, such as a scanner that also analyzes underlying tissue and pulse, promise to "go deeper," making this type of theft more difficult. Until then, however, think twice before flashing that peace sign on your next selfie.
Telegraph.co.uk, 01.17.17



"Things have gotten a lot easier since I moved everything from my to-do list to my it-is-what-it-is list."

How Businesses Hurt Sales And Their Reputation On Social Media. If you have any type of social media presence – Facebook, Twitter, LinkedIn, YouTube or others – one of the things you must be on CONSTANT alert for is customer complaints. According to a study conducted by Edison Research, consumers post their complaints on social media in order to solicit a FASTER response than going through the normal channels. That's because smart companies don't want an unhappy client's comments hanging out there for the world to see, unanswered and unaddressed. So IF you are going to have a presence on social media, make sure you or someone on your team is constantly monitoring it for client complaints.

New 360 video cameras let you deliver a whole new customer experience. 360 video lets your customers visit a location without actually being there. How you use it depends on your business, but the sky's the limit – literally. Realtors and property managers, for instance, can give prospective buyers or renters a view from the kitchen where they can look in all directions and get a feel for the place that they just can't get from 2-D shots. 360 video cams consist of two back-to-back fish-eye lenses and software that "stitches the seam" between them. Just be sure to position the camera where viewers can see everything all around them. With the right camera and headset, you can now put your customers "on location" – virtually.
Wired, 02.24.17