



Executive IT Insider

The *Exclusive Edge* to Today's Technology

Published and Distributed by IT Support RI

Contents:

Phishing, Blackmail, and Sextortion; A Triple Threat1

Refer-a-Friend.....2

Technology Spotlight: Google Home Hub.....3

90 Ways To Be Better.....3

Expert of the Month: The Team at Vision Associates4

These Recent Phishing Attacks Can Cause Your Business Serious Harm4

Follow Us

 www.facebook.com/ITsupportRI

 www.twitter.com/ITSupportRI

December 2018



Provided By:

Paul Riendeau

Owner of *IT Support RI*

Season's Greetings!

With the end of the year upon us, **now** is the time to *wrap up* loose ends and

any end of year projects!

Don't forget to take advantage of the **Section 179 Tax Deduction**.

Remember, *any* equipment **purchased in 2018** qualifies for the deduction. Finish this year **strong** and get a **head start** on **2019!**

Contact your account manager or give us a call to learn **more!**



Phishing, Blackmail, and Sextortion; A Triple Threat

Phishing scams are **on the rise again!** Phishing is a type of scam where hackers or cyber criminals send you an email that seems to be from a legitimate company. The email contains a link that directs you to a page that *appears* to be the company's website.

A phisher's **ultimate goal** is to trick you into entering *sensitive information* such as passwords or usernames. Today, phishers are working harder than ever to trick you.

Unfortunately for many people, phishers are taking things up a notch. Now, phishers are using your **real passwords** to get your attention!

Sextortion Emails; A New Twist on Phishing

In this new email scam, the sender claims to have installed a virus on your computer. This virus allegedly monitors

your website traffic, accesses your webcam, and remotely records you watching explicit videos. The sender then demands that you pay a ransom to avoid having these videos leaked to your entire contact list.

This new type of scam email is known as **sextortion**. The FBI defines sextortion as being "a serious crime that occurs when someone threatens to distribute your private and sensitive material if you don't provide them...money."

Besides being blackmailed and threatened, there's **more**. What's the worst part about this email? The sender uses one of your real passwords to **increase the authenticity** of their threat. Suddenly the threat seems much more credible because the sender presented you with a real password. When you're presented with one of your passwords, you're **more**

Continued on pg.2 >

Get More Free Tips, Tools and Services At Our Web Site: www.ITsupportRI.com

(401) 684-3036

likely to comply with their demands and pay the ransom because you don't know what other information then sender *could* have.

How'd They Get A Real Password?

Are you sitting there frantically wondering how they got your real password? Are you afraid they installed a virus? **Don't worry**; the chances of the someone recording you through your webcam or accessing your computer are *highly* unlikely. Even though the sender has a real password, there's a good chance that the password is **old** and **not in use anymore**.

In the deepest part of the internet, known as the **Dark Web**, there are "data dumps" where hackers and cyber criminals buy and sell usernames and passwords. These credentials were either *stolen* or *leaked* from some of the worst database breaches. Breaches like Equifax, Yahoo, and other big companies left *millions* of people vulnerable. Unfortunately, if you were a victim of a company breach, some of your old passwords *may* be floating around on the internet.

How Can You Protect Yourself?

Do Not Recycle Old Passwords

Are you one of those people that repeatedly uses the same few passwords? Do you use the same password but add different numbers or symbols to the end, for example: Password, Password1, Password2, and so on? If you're guilty of this, **stop immediately**.

Use Unique Passwords For Every Account

Do not use the same password for multiple accounts. If a hacker gets that one password, they can access and control all your online accounts. Think of all the information or credit card numbers they'd obtain!



Use Two-Factor Authentication

Two-factor authentication gives your accounts an **extra layer of security**. Even if a hacker gets your password, they can't get very far. Think of two-factor authentication as being your PIN number for your debit card. Without that PIN number, you can't access your money.

The **number one thing to remember** is that if you receive a threatening blackmail or extortion email, **you are not alone**. After a quick internet search, there's a very good chance you'll see *numerous* articles describing this scam and others like it. Don't be afraid or embarrassed to tell someone about the email.

If you have the *slightest suspicion* that your account could have been compromised, **change your passwords immediately**. The sooner you update your passwords, the less likely you are to be a victim. Remember, you should **never** click on any links in the email, download attachments, or enter your information. If you have *any* questions or you're worried about your cyber security, contact us today!

Refer-a-Friend and Get Free Gifts!



We **love** having customers like you and honestly, we wish we had more just like you! So, we are doing an ongoing "Refer-a-Friend" event.

Refer any company with 5 or more computers to our office to receive a **FREE** Computer Network Assessment (a \$300 value). Once we've completed our initial appointment with your referral, we'll send you a **\$50 Amazon gift card**.



Think of it as a small "Thank You" for thinking of us. As an added bonus, if they join and become a client of ours, we will send you a **\$500 Amazon Gift Card** for introducing your friend to us.

Simply call us (401-684-3036), e-mail us (support@itsupportri.com) or visit www.ITsupportRI.com/referral and send us their contact information today!

Get More Free Tips, Tools and Services At Our Web Site: www.ITsupportRI.com

(401) 684-3036

Technology Spotlight: Google Home Hub

The battle between Amazon and Google is heating up! Google's newest device, the Google Home Hub, is the latest device to try and upstage Amazon.



The Google Home Hub is the perfect combination of smart home assistant and touch screen. The Google Assistant, which is Google's equivalent to Amazon's Alexa, can answer questions about the weather, sports, tell you about your Google Calendar, stream music and videos, or act as an alarm clock.

The Google Home Hub can control other smart devices through the Google Assistant. In fact, the Google Assistant works with *most* major smart home device brands. However, before buying, make sure the item is compatible with your Home Hub or other Google devices.

The Home Hub can even help you in the kitchen. It can easily find recipes, display the ingredients list, and play instructional videos to help you make the meal.

In addition to vocal responses through the device's speakers, the answers will appear in text on the screen. When not in use, the Google Home Hub will act as a clock or picture frame, creating a slideshow of pictures stored in your Google Photo Albums.

While the Google Home Hub can perform a lot of tasks, it lacks a web browser, meaning you can't visit any websites.

When compared to other similar devices, the Google Home Hub is simple, small, and affordable. Whether you're familiar with smart devices or just starting to dabble in the sea of smart products, this Google device is a must have.

You can purchase the Google Home Hub at the [Google Store](#) for \$149.

90 Ways To Be Better

Would you believe that there is an organization in America today that lists 90 traits, characteristics and soft skills they want their employees to have? Well, there is. My first thought when I saw the list was, "These folks are nuts!" But, after actually reviewing the list, I changed my tune. All of them are doable and warrant our attention. Success is always all about constantly becoming a better version of ourselves. The question is: What do we have to go by? How do we grade ourselves?

If I gave you a list of things that would help make you more successful, would you do them all? Well, here is an excellent list to start with. Now all you have to do is be really honest with yourself and decide if you live by each of the listed traits.

After reviewing the list several times, you may decide you want to add to it. There's nothing wrong with that!



Personally, I would add "Be nice" to the list. In fact, I would start with that one. But maybe they think "compassionate," "respectful" and "empathic" cover that. I like it stated in simpler terms: be nice!

Good luck with grading yourself. The list sure does make you think. I am working on several of them right now!

Ability to compromise for the greater good • **Accepts criticism constructively**
 Accountable • **Adaptable** • Analytical • **Applies current best practices** • Approachable • **Assertive** • Attentive to detail • **Belief in the dignity of others** • Calming • **Candid** • Community-oriented • **Compassionate** • Confident • **Consistent** • Constant learner • **Courageous** • Customer-focused • **Decisive** • Dependable • **Detail oriented** • Disciplined • **Discreet** • Effective communication skills • **Embraces change** • Emotionally healthy • **Emotionally intelligent** • Emotionally resilient • **Empathetic** • Energetic and enthusiastic • **Ethical** • Flexible • **Focused** • Frustration-tolerant • **Honest** • Humble • **Informed** • Shows initiative • **Innovative** • Inquisitive • **Displays integrity** • Intelligent • **Excellent interpersonal skills** • Judicious • **Knowledgeable** • Leadership • **Learns from mistakes** • Level-headed • **Logical** • Loyal • **Good memory** • Moral fortitude • **Motivational** • Good at multitasking • **Non-impulsive** • Open-minded • **Organized** • Patient • **Perceptive** • Perseverant • **Has perspective** • Is physically fit • **Is prepared** • Preserves confidentiality • **Proactive** • Problem solver • **Professional** • Protective • **Reasoning ability** • Resilient • **Resourceful** • Respect for diversity • **Respect for the individual** • Respectful • **Responsible** • Self-motivated • **Self-restraint** • Good sense of humor • **Sense of service to others** • Skeptical • **Exhibits sound judgment** • Strong work ethic • **Tact** • Teamwork • **Tolerance** • Trustworthiness • Verbal communication skills • Written communication skills



*Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books *How To Soar Like An Eagle In A World Full Of Turkeys* and *52 Essential Habits For Success*, he's shared the podium with esteemed figures from across the country, including former President George H. W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

Expert of the Month: The Team at Vision Associates



For almost 50 years, Vision Associates has been providing patients with quality eye care. Dr. Alan Grossman strongly believed in the phrase “**make your patients come first,**” and instilled this philosophy into his staff. In 1995, Dr. Grossman’s daughter, Dr. Debra Sleight joined the practice. Today, almost 25 years after his retirement, the staff *still* practices this philosophy. Because they are dedicated to their patients and provide each patient with the individual attention they deserve, the team at Vision Associates is our new *Expert of the Month!*

Vision Associates was founded in the early 1970’s by Dr. Alan Grossman. With her interest and degree in biology, studying optometry just seemed like the next, natural step for Dr. Sleight. When Dr. Grossman retired in 1998, Dr. Sleight and Dr. Ara Barsamian took over the practice.

At Vision Associates they specialize in primary eye care. They offer eye exams, complete contact lens services, diagnose ocular disease, and can satisfy all your eye glass needs. In fact, their optical shop is *highly* experienced because *each* optician has **over 30 years of experience** in the field.

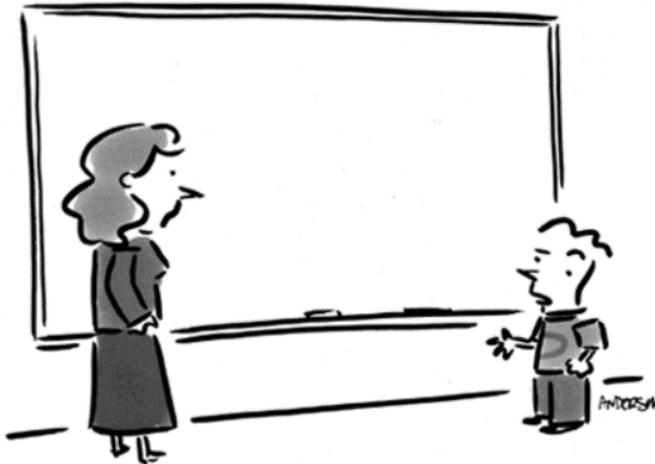
Not only does everyone at Vision Associates love what they do, they love serving the community. Dr. Sleight’s *favorite* part of her job is talking to her patients. She enjoys talking to people, learning about their lives, and hearing their stories. To her, an appointment is more than just checking her patients’ eyes; it’s getting to know them while helping them. To Dr. Sleight, this is the most rewarding part of her job.

At Vision Associates, they’re excited to help you. You get a certain level of customer service and **personalized** attention that you can’t find at the chain stores. Vision Associates has patients who have been going there for years, as well as several generations of family members. Because they provide such **extraordinary care**, many of their patients started visiting when Dr. Grossman was still practicing!

Dr. Sleight is grateful that she hired us. As Dr. Sleight puts it, “everything fell together” when she met us at an optometry conference. She was the IT person in her business, and she was concerned with protecting her patients and their data. We came in and helped Dr. Sleight “move forward take the steps [they] needed” to transform the practice and get everything computerized. Overall, Dr. Sleight states that “you guys have been incredibly helpful, the support has been great, and I couldn’t have made our transition without you!”

Vision Associates is accepting new patients, and they take a variety of health insurance providers. If you’d like to learn more about Dr. Sleight and Vision Associates, visit their website www.vamarlboro.com. The entire team hopes to *see* you soon!

© MAZK ANDEZSON WWW.ANDEZTOONS.COM



“Before I write my name on the board, I’ll need to know how you’re planning to use that data.”

These Recent Phishing Attacks Can Cause Your Business Serious Harm

According to Symantec’s 2018 Internet Security Report, the number of reported blocked phishing attacks increased by 92% over the last year. Many of those were due to Ryuk, a variation on Hermes, the first known ransomware plague. The malware has been targeting law firms, convenience store chains, and even medical facilities, netting hackers as much as \$640,000.

Then there are state-sponsored attacks hitting small businesses across America, funded by hostile governments. In addition, there has been a Facebook e-mail scam going around, masquerading perfectly as an e-mail from the massive company, but leading victims into downloading malware. The same goes for false e-mails from FedEx, as well as Bank of America. Hackers have even begun offering false SEO services to get victims to click a link! Teach your team how to spot phishing attacks and stay vigilant. You never know when they might show up in your inbox.

SmallBizTrends.com, 9/19/2018

Get More Free Tips, Tools and Services At Our Web Site: www.ITsupportRI.com

(401) 684-3036