

# TECHNOLOGY TIMES

*"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"*

## What's New

It seems the press is full of new cybersecurity attacks and dramatically improved systems risks.

This issue's headline article outlines the risks and the ways you can protect yourself and your business.

There isn't any one solution.

It's about layers of protection; strong tools, security policies, staff, education, and solid multiple backup methodologies to recover quickly if an attack does occur.

Give me a call at 732-792-2021 to set up an appointment to evaluate your security.

**July 2017**



This monthly publication provided courtesy of David Streit, Principal of Stephill Associates, LLC.

Our Mission: To Help Clients STEP over the HILLS of technology. For 15 years we've provided individualized, responsive computer support, network systems, and vertical applications support.



## The Most Common Ways Hackers Access Your Network

You are under attack. Right now, cybercrime rings in China, Russia, and the Ukraine are hacking into small businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses, and half of all cyberattacks are aimed at small businesses. The National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year. It's critical that you protect yourself from the following 10 vulnerabilities.

**1** Poorly trained employees are the biggest risk. It's common for an employee to infect an entire network by opening and clicking a phishing email designed to look like legitimate correspondence from a trusted source. If they don't know how to spot infected emails or online scams, employees can easily compromise your

entire network.

**2** We strongly recommend an acceptable use policy that limits the websites employees can access with work devices as well as work material they access with personal devices. We can easily set up permissions that regulate which websites your employees access and what they do with company-owned devices, even granting certain users more freedom than others. You also need to detail what an employee can or cannot do with personal devices when taking work home.

**3** Weak passwords are bad news; passcodes should be at least eight characters long with both lower and uppercase letters and include symbols and at least one number. On a company cellphone, requiring a passcode makes stolen devices harder to compromise. ➤

Get More Free Tips, Tools and Services At Our Web Site: <http://www.stephillassociates.com>

(732) 792-2021

*Continued pg.2*



Again, this can be enforced by your network administrator so employees don't get lazy and put your organization at risk.

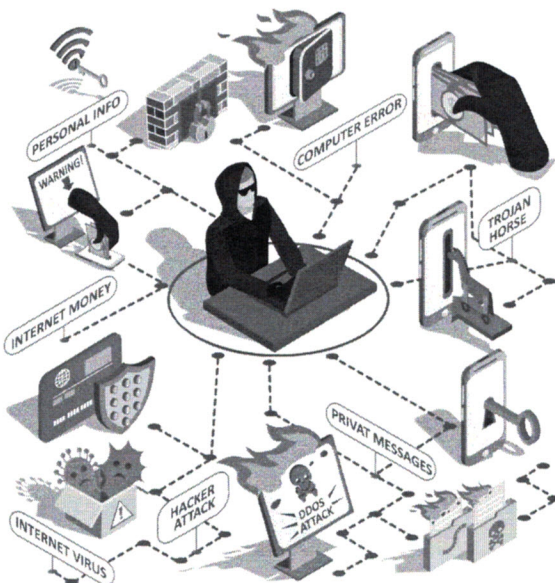
**4** If your networks aren't patched, new vulnerabilities (which are common in programs you already use, such as Microsoft Office) can be exploited by hackers. It's critical that you patch and update your systems frequently. If you're under a managed IT plan, this can be automated so you never miss an important update.

**5** Are you backed up in multiple places? Aggressive ransomware attacks, where a hacker holds files for ransom until you pay a fee, can be foiled by backing up your data. You won't have to pay a crook to get them back. A good backup will also protect you against accidental deletion and natural disasters, and it should be automated.

**6** One of the fastest ways cybercriminals access networks is by duping employees to download malicious software by embedding it within downloadable files, games, or other innocent-looking apps. This can largely be prevented with a secure firewall and employee training and monitoring.

**7** Not all firewalls are created equal. A firewall blocks everything you haven't specifically allowed to enter or leave your network. But all firewalls need monitoring and

maintenance, just like all devices on your network, and a weak one does you little good. This, too, should be done by your IT person or company as part of their regular, routine maintenance.



**8** Many hackers exploit your devices when you connect to public Wi-Fi, getting you to connect to their Wi-Fi instead of the legitimate public one. Always check with a store or restaurant employee to verify the name of the Wi-Fi they are providing. And never access financial or medical data or enter your credit card information when surfing public Wi-Fi.

**9** It may be one of the oldest tricks in the book, but phishing emails still work. The goal is to get you to download a virus by clicking a link or getting you to enter your login information on a clone of a legitimate website.

**10** In 2009, social engineers posed as Coca-Cola's CEO, persuading an executive to open an email with software that infiltrated the network. Social engineering is another old-school tactic, but, like phishing, it works well. Hackers pretend to be you, and people often fall for it.

If you are concerned about cybercriminals gaining access to your network, then call us to learn more about implementing a managed security plan for your business. You've spent a lifetime working hard to get where you are and have earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, reputation, and data are protected.

## Free Cyber-Security Audit Will Reveal Where Your Computer Network Is Exposed and How to Protect Your Company Now



At no cost or obligation, we will come to your office and conduct a comprehensive Cyber Security Audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

**To get started and claim your free assessment now  
call our office at 732-792-2021.**



## Client Spotlight

Stephill takes care of several established CPA firms. The largest is Steven Sewald & Company CPAs & Consultants. Steve founded his practice in 1989. He and his staff of four CPAs provide a full range of Accounting, Tax, Payroll, and Business Consulting services in the following Practice Areas;

Financial Statements  
Engagements  
Individual and Corporate  
Income Taxation  
QuickBooks Pro Advisor  
Estate and Trust Income  
Taxation  
Managerial Advisory  
Quasi Chief Financial Officer  
Closely-Held and Family  
Businesses  
Real Estate  
Litigation Support  
Non-for-Profit Organizations

Steven Sewald & Company, CPAs and Consultants, is located in Morganville, NJ and can be reached at (732) 332-1700.

Their website is;  
<http://www.sewaldcpa.com>



## Are You in a State of Stuck? Here's How to Win the Battle Against Inertia

By Andy Bailey

Momentum is key to business growth. When you're moving forward and good things are happening, it can feel almost effortless. One action leads to the next, and you're achieving results at a rapid pace.

But what if you had a good run, and you're now feeling a little stuck? It could be that you're suffering from inertia. It's very real and can be very destructive. I work with businesses every day, and even the most seasoned leaders experience inertia from time to time.

The good news is that there's always a way out — it depends on you. The key is to get moving. Shake things up and make choices that force you out of your state of stuck.

Take these five steps to break through inertia and get your wheels rolling again:

**1** Get specific about what you want to accomplish. What do you want to do, and what does success mean? In creating your goal, ask yourself, "What does that look like?" And be specific about your answer! Avoid using words like "less" or "more" — those terms mean nothing.

**2** Plan it out. What steps are necessary to reach your goal? How will you ensure your success? Write it all out and indicate when you plan to complete each step. Set dates for completion and stick to them.

**3** Ask what might get in your way. If you set a goal, but you don't think about potential obstacles, you're setting yourself up for failure. For example, if you want to go to the gym three times a week at 5 a.m., but haven't considered that you may be needed at home to help with child care, you're probably not going to the gym. Get real about any hurdles that might get in the way of

achieving your goal, so you can work around those circumstances and find your best path to success.

**4** Make yourself accountable. It can be easy to tell yourself that you're going to do something, but if you make your intentions public, it's much tougher to make excuses and abandon your commitments.

**5** Do it now! There's no time to waste and there's a lot of power in the present moment. No matter how small the first step is, make every effort to take it immediately. Demonstrate to yourself and others that you're committed to the process and you're ready to move forward. In the words of Lao Tzu, "The journey of a thousand miles begins with one step." Take that step as soon as you can.

I'm a big Yoda fan, and I quote him a lot. Here's my favorite line of his: "There is no try ... only do." Trying won't get you anywhere. Set your goal, figure out how to meet it, and really do it. Anything else will stop your momentum in its tracks and lead to inertia (or the Dark Side, as Yoda might put it).

*As the founder of Petra Coach, Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success and coaching them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business,*



*which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.*



### ■ Is Your Coffee Maker or Thermostat a Security Threat?

Internet-connected devices, including coffee makers and thermostats, are slated to hit 20 billion in number by 2020. That makes them ripe for hacking, as we saw last November with DDOS attacks that targeted smart devices in addition to regular laptops and computers. Standard security measures apply, including strong passwords and from home use policies. Get your IT people trained on smart device security, and only use those devices if totally necessary. *SmallBusinessComputing.com* – November 30, 2016

### ■ Phone Power Companies Are Here To Prevent You From Ever Letting Your Battery Die.

Phone charging on the fly is a growing market in China, and

one company, Anker, is trying out its platform in Seattle. Power-bank sharing is the way of the future, or so Anker believes, anyway. People use bike-sharing services because it provides for some convenience. People used to buy products, now they want a service. Today, people think that they need to bring a portable charger out with them. That might change with power bank-sharing. Whether people will pay \$1.99/day so they don't have to bring a charger with them remains to be seen. *Mashable.com* – May 9, 2017

### ■ A Vicious Microsoft Bug Left A Billion PCs Exposed.

Speaking of which, thank goodness security researchers in May found the exec bug in Windows that could have been used by hackers to gain entry

without physical access or user action. The bug would have exploited Windows Defender, Microsoft's in-house antivirus software, and left anybody running Microsoft Windows vulnerable. As Google engineers note in a report on the bug, to pull off the attack a hacker would have only had to send a specialized email or trick a user into visiting a malicious website, or otherwise sneak an illicit file onto a device. This also isn't just a case of clicking the wrong link; because Microsoft's antivirus protection automatically inspects every incoming file, including unopened email attachments, all it takes to fall victim is an inbox. Microsoft has since patched the bug. *Wired.com* – May 9, 2017

### ■ Amazon Makes Landline Phones Trendy Again.

They say that everything old is new again, and landlines are making an Amazon comeback thanks to the tech company's new Echo Show system. Similar to the existing home assistant Echo system, the Echo Show includes robust speakers, a camera, and a video touch screen to facilitate video calls with family and friends. Retailing for just north of \$200, the Echo Show might be the future of at-home phone calls, in addition to its other home-assistant functions.

*TechCrunch.com* – May 13, 2017

