Need Help Filing Business Tax Returns? Startup-Friendly Accountants Are on Page 2.

January 2018

The Monthly Resource Guide For Startup Businesses

NEW BUSINESS MINNESOTA

Special Report

Protecting Your Business

You've Worked Hard to Launch Your Business. Have You Taken Steps to Protect What You've Built? These Experts Offer Their Solutions:
Troy Solis, SOL-IS Technology Solutions;
Bob Bossert and Mike Karch, Floyd Total Security; and
Steve Goldetsky, Inrelex Law Group PLLC.

Your Business Is Under Constant Threat from Hackers, Spammers and Creeps

Working with Managed IT Pros Will Help Keep Your Business Productive and Your Data Safe.

By Troy Solis
SOL-IS Technology Solutions

When it comes to Protecting Your Business, it is essential that you have what the military calls situational awareness of your IT environment. That means knowing where your vulnerabilities are, what solutions are needed and where, and keeping everything current.

If your IT environment is breached or fails, your business could suffer serious damage, diminished productivity and, if it affects your customer service, loss of business.

I know what it's like to start a business. It can be overwhelming. The key, I've found, is to focus on your strengths and delegate the rest. I learned it firsthand and I see my successful clients practice that as well.

You could easily spend four hours chasing a tech problem that we could fix in minutes. That's four hours you could have used for meeting prospects, sending a marketing email blast or engaging your clients.

I started my career in technology as a radar and radio electronics technician in the U.S. Navy. After serving, I joined the medical device industry, where my talent for technology advanced me from electronics technician to roles in IT management and consulting.

I launched SOL-IS Technology Solutions in 2009 to bring that level of service and expertise to small business owners.

Even if you outsource your IT, you will still need a good understanding of the technology you rely on. The issues are the same whether you are a solopreneur on a laptop or a big company with hundreds of users. Here is a quick overview.

Vulnerabilities

The biggest vulnerability is having an internet connection. That's the route hackers take to get in, and they are constantly banging at the door. If your firewall isn't updated regularly, they will get in.

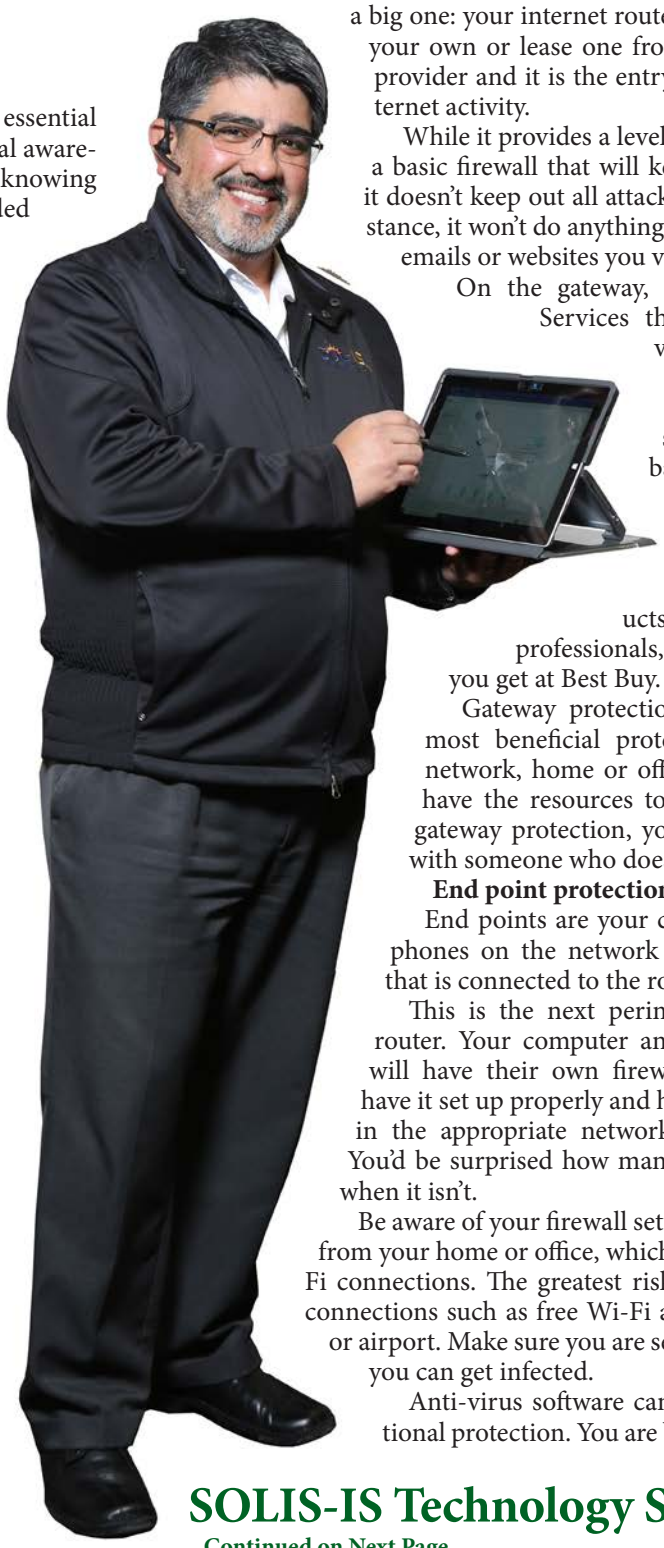
If you want to be totally secure, follow the example of one of my clients. They have NO internet connection on their 15-year old computers and outdated software. Everything works perfectly because they've never touched the internet. They don't need updating or patches.

They do, however, have a separate computer for email and online things, which is the computer we fix and maintain.

For most of us, the internet is not an optional thing. Therefore effective protections and management systems must be in place.

Perimeter Gateway Protection

This is the outer edge of your security perimeter. This is a big one: your internet router. You may own your own or lease one from your internet provider and it is the entry point of all internet activity.



While it provides a level of security with a basic firewall that will keep hackers out, it doesn't keep out all attack threats. For instance, it won't do anything about incoming emails or websites you visit.

On the gateway, there are other Services that enable anti-virus and anti-ransomware tools or other subscription-based software to protect you. These are business-class products that are used by professionals, not something you get at Best Buy.

Gateway protection is by far the most beneficial protection for your network, home or office. If you don't have the resources to get the quality gateway protection, you need to work with someone who does.

End point protection

End points are your computer, tablet, phones on the network and any device that is connected to the router.

This is the next perimeter after your router. Your computer and other devices will have their own firewall. You should have it set up properly and have it turned on in the appropriate network environments. You'd be surprised how many assume it's on when it isn't.

Be aware of your firewall settings when away from your home or office, which are private Wi-Fi connections. The greatest risk is from public connections such as free Wi-Fi at a coffee shops or airport. Make sure you are set up properly or you can get infected.

Anti-virus software can give you additional protection. You are better off using a

SOLIS-IS Technology Solutions

Continued on Next Page

paid anti-virus subscription service, which provides regular updates and anti-virus definitions automatically.

There are free versions you can use, but they aren't as robust. And you have to remember to get the updates and make sure they are installed.

End Point / Patch Management

Once you have your protection in place, you have to manage it. That means knowing how to properly use your anti-virus and malware software and patch updates for Windows or Mac.

Recently, hackers developed a Malware product and then set their sights on Windows operating systems that were missing a certain patch. My business clients didn't have issues because we keep them up to date and manage it for them. Those who were on their own were left scrambling to find a fix for it.

Email protection

Email is one of the most common entry points for bad guys. It's an opportunity for things to get into your computer from anywhere in the world.

Deception is the favored tool. If they don't know you, they will pretend they do. They might send a Dropbox notice saying you have a document you need to sign. DON'T. It's coded software that will give them remote access to your computer or track your key strokes to get passwords to your bank accounts.

We recommend using an email service that includes anti-malware, anti-virus and anti-spam software as part of their service. Some of the popular free services leave the scanning to you, costing you an additional layer of protection.

Training

The biggest component in any protection scheme is training. You and your users need to know what to look out for. Hackers are tricky. They will send you emails about wanting to pay one of your invoices or ask you to reset you bank password. Beware of their offer to "Just click here."

They are masters of replicating logos and email formats used by any business. One of my customer had just agreed, in an email with his real lawyer, to mail a $6,500 check to a certain address.

Within minutes, another email arrived that looked just like his lawyer's format with instructions to send the money by wire transfer instead. Fortunately, the accounting person didn't fall for it.

No "anti" anything software can protect you against that. You have to keep your eyes open, your wits about you and question everything.

If in doubt, you can put your cursor over the link and see if you can identify who it's coming from. Or you can call the apparent source to verify if they sent it.

Get training for you and your staff, because ultimately, you are the weakest link. A good managed service provider can help with that.

Backups

When all goes wrong, whether it's a virus, bug, ransomware or hard drive crash, you have no hope of recovery if you don't have a solid backup.

If you get a ransomware alert and they lock your data, backups that include version histories can be a lifesaver. You can go back to a point before you were attacked and your data was encrypted and do a restore from there. It could be from hours or days to a year earlier.

If you get a ransomware message on your computer screen — STOP. Disconnect power from your computer and seek professional help. If you have a good backup version history that predates the attack, you have a decent chance to recover.

Back when ransomware first appeared, we obtained a new client because they were hit with a demand for payment to unencrypt his files.

His best course of action was to do a restore. Unfortunately, he had been using a free backup service that was just mirroring what was on his computer – the virus was backed up as well. Beware of free stuff. He lost everything.

Don't overlook, as many do, the need to back up your email data, contacts and accounts. Don't forget your calendar. You don't want to lose your future, too.

Password change policies

If you want the easy route to a miserable life, convince yourself that you only need one password. Be serious about protecting your business and create real password policy. Write it down on a piece of paper.

- How frequently to change it.
- Required level of password strength.
- Number of characters, special characters, numbers, upper and lower case.
- Enforce the policy with special tools to monitor and ensure it matches password strength policies.

You should strike a balance between memorable and overly complex. Sixteen characters is extremely strong and is a good goal for length. To keep it memorable, try combining three or four easy to remember password. Mix them together.

As you consider solutions for protecting your business, remember that there is no such thing as one size fits all. Your computer environment, how you work, where you work and the software you use all present challenges that are different from other businesses.

Because of the range of services and pricing packages available, any business can afford to work with a managed IT services professional who can make sure they are protected, productive and getting only what they need.

Managed IT is all about monitoring your systems to ensure your technology systems are operating properly, and are secure. An IT professional will continually ensure that your systems are prepared to face emerging threats before you are attacked.

One of the things you learn about running your own business is that you don't know what you don't know. Take the IT responsibility off your plate so you can focus on what you do best – grow your business.

NBM

Troy Solis is President and owner of SOL-IS Technology Solutions, an IT company serving the Twin Cities and surrounding areas with managed IT services, data network security, technology consulting and cloud solutions. He can be reached at (952) 279-2424 or

support@sol-is.com

www.sol-is.com