November 2017

TechTidbit.com

brought to you by Tech Experts

Five Keys For Small Business Preventive Security Measures

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

We continually mention the importance of network and password security for small businesses for good reason. The increasing security threats and cases of security breaches in both large and small enterprises show that we are more at risk than ever before of suffering a security violation.

Regulated entities such as medical offices (HIPAA) and financial institutions (FINRA) are especially susceptible to breachs and security incidents.

Prevention is always better than cure. To this end, here are five security measures you should start putting in place today.

Limit lateral data transfers

One of the biggest contributors to internal data breaches is a lack of employee knowledge of security issues. It's important to protect strategically important information and data by limiting who has access to it.

Furthermore, you can employ network segmentation to reduce any unnecessary communication between internal and external networks.

Ensure machines and devices are updated

Internal breaches can result from the use of unprotected machines. Without being aware, employees may download malware or ransomware.

However, this may not be a problem if the software and operating systems on the machines are up to date.

Keeping all devices and the accompanying software and security structures up to date will make a significant contribution to protecting your systems.

Monitor activity to identify suspicious activity

Sometimes, a security breach may not involve any employees. Network administrators should ensure the latest monitoring software is in use to monitor behaviors and immediately detect anything that looks amiss.

Cyber criminals are aware of these types of activities and often conceal themselves deep in the network to exploit the system over a prolonged period of time.

Even if you miss the threat the first time, the monitoring system will provide meaningful insights that will help you recognize foul play.

Ensure robust passwords are in place

When it comes to system passwords and login procedures, you can always improve. In addition to the more traditional text-based password access, you should also ensure you have more up-to-date security mechanisms in place such as fingerprint access and smartcards. These are much more challenging for cyber criminals to replicate.

Embrace cyber insurance policies

No system can be completely safe from a cyber attack. Criminals are getting smarter and smarter, and what appears to be an impenetrable system one day can be infiltrated the next.

For this reason, you may wish to take out cyber insurance to cover any costs you incur if things do go seriously wrong.

No system can be completely safe from a cyber attack. Criminals are getting smarter and smarter, and what appears to be an impenetrable system one day can be infiltrated the next.

Digital Display Boards: For You Or Your Clients

"Your display board could show anything from a movie to informational slides, videos, or promotional pricing. You could even have customer reviews streaming on the board to let new customers know that you are a well-respected addition to the community."

Ron Cochran is a Field Service Engineer at Tech Experts.

With the advancement of technology, magazine racks and fish tanks have been replaced with phones and tablets. But what if I told you that, instead of your clients or customers paying attention to their phones, they could watch content that you would benefit from them watching while waiting for service?

Wireless connectivity has sprouted a new way to connect devices of all types.

Take, for instance, an HDMI dongle that can connect wirelessly to any PC or Mac that is also connected to the same network. After a few short minutes, it is set up and ready to start displaying what you want it to.

Your display board could show anything from a movie to informational slides, videos, or promotional pricing. You could even have customer reviews streaming on the board to let new customers know that you are a well-respected addition to the community.

You can also set them up for internal business use by utilizing the display board and wireless connection for conference room meetings, employee training sessions, or displaying productivity/metric reports.

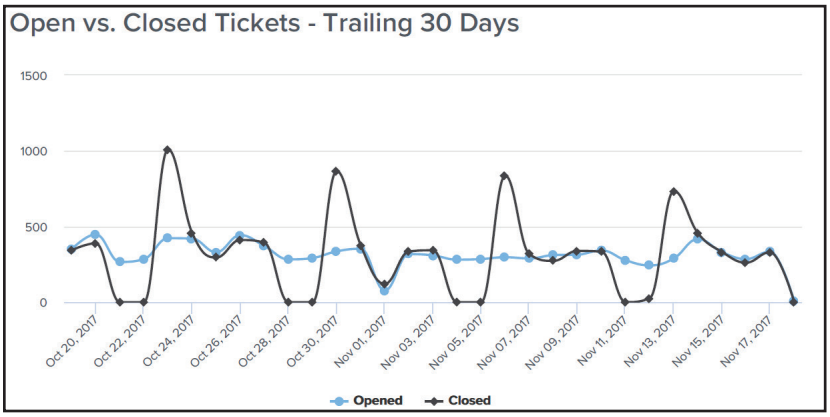
The days of pulling the TV cart out of the closet with that cumbersome CRT TV and dealing with all of the wires and connections are a thing of the past.

There are a few different ways you can set up a display board. You can have as many display boards as you want and each one would have their own assigned ID.

You could then start the streaming process by launching an application from your computer, company server, or even have a small form factor computer dedicated to each display board.

Let's say you want to have your server control the display boards because you want to have four display boards throughout your place of business.

You can have the server send, in example, a slideshow of reviews.



You would launch the application, select which display boards you want to stream to, and now you're connected.

In order to start streaming the slideshow, you would open up the program that you use for the slideshow or picture viewer and press play. Once you press play, the slideshow will play on the display boards you previously selected.

Now, let's say you wanted to use the display boards for company productivity and metrics reports. You would first set up your KPI dashboard software the way you want it displayed.

Once you have that set up, you would open up the connection to the HDMI dongle or display board connection and connect to the desired display boards' IDs. Just like magic, everyone in the building that is in view of the display boards can see why everyone is getting that quarterly bonus and why.

So, if the thought has crossed your mind that you might want to have a couple TV's replace your magazine rack or that fish tank that requires expensive monthly maintenance, then give us a call today and we will discuss your options after hearing your concerns and business needs.

Is It Time You Had A Failover ISP?

Jason Cooley is a Network Technician at Tech Experts.

So, you may want to ask – what is a failover ISP? Let's not over complicate it: it is exactly what it sounds like. A failover ISP is a backup Internet connection through a secondary Internet service provider.

This means paying two monthly bills, for two Internet connections. Strong selling point? Probably not for most people. So what is the appeal? Is it something that will be that useful? First, we would need to know a few things.

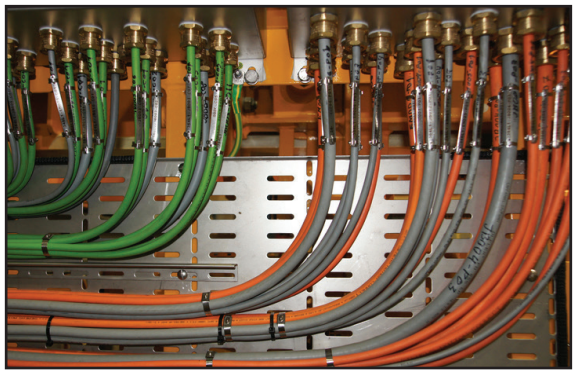
How much of your business relies on the Internet? Sure, a quick 10 minute outage is an inconvenience, but most businesses will survive, albeit with different levels of comfort and success.

What happens if there is an extended outage? Can you operate an entire day without an Internet connection? How much money would you lose from being offline for an entire business day?

While the answers to these questions will vary, the fact is there are a growing number of daily business operations that utilize an Internet connection.

VoIP phones? No Internet, no phones. Credit card processing? Unless you use an analog telephone line, that's out too. Rely on email?

Your phone may be capable, but is that something you want to be stuck doing for an extended period? The fact is, more and more, we really on a stable Internet connection.



What impact does lost time have on your daily operation? While I touched on some of the basics here, think about how you could function without a connection. For some people, it just isn't possible.

If you are a financial institution that utilizes an offsite financial database, you rely on a connection to service your customers. If you are an insurance company that sends and receives quote information over the Internet and take payments through online processing, you can't operate.

If you have an office with all VoIP phones and every employee utilizes online tools and services, you can't operate. Or maybe you are a healthcare provider that needs a connection for patient insurance?

You will have to make some choices about losing a day if any of these apply to you. This is a reality and, in some cases, a gamble.

This just isn't something we need right now.

Understandable for a lot of businesses out there. There are different needs for different business types.

Restaurants, for instance, probably couldn't accept credit or debit cards if they lost connection. During a temporary outage, you can relay to your customers that you can only accept cash.

If you have a few users and work from a laptop, you can tether your mobile connection. Whatever the case, it isn't something everyone needs.

Isn't it just wasted money if my connection never drops out? Not necessarily. With some good IT work, you can route different Internet traffic through your two ISPs.

Consider it like load-balancing. You can also have it set up that if one of your two networks drop, the other one connects automatically. Again, lots of options are available to you.

Think you need a failover ISP?

There are places where you may not have the option of multiple providers, but in most business areas, there are different options available.

So what happens if you do have a second connection? How do you connect to your backup? Is it automatic?

Your IT department or managed service provider, like Tech Experts, can set that up for you. There are many options depending on your specific setup, but being covered against Internet service outages is universal.

"What happens if there is an extended outage? Can you operate an entire day without an Internet connection? How much money would you lose from being offline for an entire business day?"

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Yahoo! And The Hack Heard 'Round The World

Evan Schendel is a help desk specialist at Tech Experts.

In the age of Russian super-hackers and nation-wide credit reporting agencies with pitiful security, what could be safe? One thing is for sure – not Yahoo!.

In September of 2016, Yahoo! released the news that 500 million accounts were hacked in the latter half of 2014. That news severely impacted Verizon's business deal to buy them out, but they only lowered the price by $350 million USD to a total of $4.48 billion USD.

Three months after this business deal was done and the prior hack had been announced, Yahoo! let the nation know that approximately 1 billion accounts had been hacked in 2013. Verizon was not pleased, to say the least.

Just recently, Yahoo! released even more grave information.

In the earlier part of October, Yahoo! bumped the number of affected accounts up to 3 billion. This estimate encompasses every single Yahoo! account, including its subsidiaries like Tumblr and Flickr. That is a lot of data – and if you had any accounts (even unused) linked to these websites dating back to 2014, you could have even had the information sold.

The cybersecurity firm InfoArmor has reported some of this information has been sold on the dark web, a small part of the web not indexed by search engines.

The group selling this information has sold the data to three sources, two of which are known spammers. All paid upwards of $300,000 USD.

With this information, reused passwords from past accounts can be the largest risk, as many people recycle the same password(s) for all of their various online accounts. While no financial information was stolen, security questions, dates of birth, and backup emails were taken.

All of this can be used for not only breaking into the Yahoo! account in question, but also any other accounts with similar information.

A good course of action from here on would be to, as you should, never reuse passwords, and change any existing passwords you feel might be in danger. Ensure that no shady happenings have occurred with any accounts, up to and including bank accounts.

The information sold was reportedly utilized to spy on a range of US White House and military officials, alongside Russian business executives and government officials.

With this information kept in mind, a document was released stating that four men were indicted, two of whom were Russian intelligence officers working for the Russian Federal Security Service. Which is, ironically enough, an agency dedicated to aiding foreign intelligence agencies track cybercriminals.

To finalize, remember to keep safety measures on all your accounts and protect yourself from email fraud or spam to the best of your ability. Only sign up for accounts on legitimate websites and, when you do create an account, use a unique password for that site. For sites with sensitive information, elect to use two-factor authentication when possible.

That way, when a company's security is pushed back in lieu of other things, you can serve as a second defense for yourself.