July 2019

TechTidbit.com

brought to you by Tech Experts

Small Businesses Are Under Cyber Attack

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

Ransomware, crypto jacking and phishing are now the biggest threat to the survival of small- and medium-sized companies (not to mention large companies, local governments, and even the federal government). Here are some sobering statistics:

1. Ransomware or hackers attack a business every 14 seconds in the United States.
2. Sonicwall (a major firewall vendor) reported a 300% increase in the frequency of attacks in 2018.
3. Ransomware attacks on healthcare organizations will quadruple by next year.
4. The financial impact of ransomware attacks against small companies is predicted to reach $11.5 billion dollars in 2019.
5. MOST ALARMING: 91% of cyberattacks begin with a spear phishing email, the most common way to infect a company with ransomware.

The threat landscape has changed significantly in the last 12 months. It used to be the reliability of our client's backups and disaster recovery options that would worry me at night.

Now, it is that Susie in accounting will get an email from what looks like a friend, click on a link, and in 60 seconds, accidentally encrypt and infect the client's entire network. This is happening hundreds of times a week across the US to companies of every size.

Local Time	ID	Category	Priority	Message
14:06:12 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:103.16.205.186 Country Name:Thailand
14:05:42 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
14:04:40 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
14:04:37 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:180.126.2.30 Country Name:China
14:04:18 Jul 03	1199	Security Services	Alert	Responder from country blocked: Responder IP:93.190.144.28 Country Name:Romania
14:03:38 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
14:03:30 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:92.126.123.130 Country Name:Russian Federation
14:02:36 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
14:02:30 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:103.16.205.186 Country Name:Thailand
14:02:29 Jul 03	608	Security Services	Alert	IPS Detection Alert: INFO SIP Session Progress, SID: 1188, Priority: low
14:01:34 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
14:01:26 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:203.226.138.12 Country Name:Korea, Republic of
14:00:32 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
14:00:20 Jul 03	608	Security Services	Alert	IPS Detection Alert: INFO Irregular SIP Traffic 2, SID: 5567, Priority: low
14:00:19 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:103.16.205.185 Country Name:Thailand
13:59:52 Jul 03	1199	Security Services	Alert	Responder from country blocked: Responder IP:195.209.111.17 Country Name:Russian Federation
13:59:31 Jul 03	82	Security Services	Alert	Possible port scan detected
13:59:30 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
13:59:18 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:202.188.1.176 Country Name:Malaysia
13:58:28 Jul 03	608	Security Services	Alert	IPS Detection Alert: ICMP PING, SID: 293, Priority: low
13:58:18 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:103.16.205.186 Country Name:Thailand
13:57:17 Jul 03	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:103.16.205.185 Country Name:Thailand

Here is a log snapshot from Tech Experts' firewall – our own firewall! In the 10 minutes I captured the log, our firewall stopped 11 attacks from countries like China, Romania, Russia and Korea. That is more than one per minute.

As I said, the threat landscape facing small- and medium-sized companies has changed entirely and has never been more dangerous.

With nearly a billion dollars a month of potential ransomware payouts, all of the bad guys – including nation-states like Russia and China – are putting a ton of resources into attacking anyone and everything in the hopes of hitting pay dirt.

The truly scary part: We have to get your systems and network protection 100% right, 100% of the time. Your employees have to be smart about their email and what they click on 100% of the time. However, the cybercriminals only have to get things right once and we've all lost.

So, what are we going to do about it?

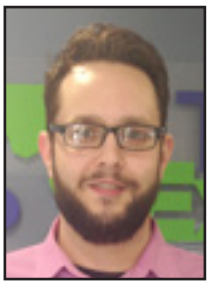
Simply, we have to help our clients implement good cyber and security hygiene, deploy security best practices such as complex passwords and password rotation, lock down application installations and other local admin rights, and expand the protection layers with more comprehensive security applications.

We do a lot to protect your network and your business – but we have to do more. Please call our office to discuss IT security for your company.

The threat landscape has changed significantly in the last 12 months. It used to be the reliability of our client's backups and disaster recovery options that would worry me at night. Now, it is that Susie in accounting will get an email from what looks like a friend, click on a link, and in 60 seconds, accidentally encrypt and infect the client's entire network. This is happening hundreds of times a week across the US to companies of every size.

Mozilla And Google Boosts Anti-Tracking And Security

"On top of regular infections, there are many data gathering processes that can run in the background of your system. These can be gathering data to send to someone attempting to steal your information. There are also websites that gather data when you visit, login, or create an account."



Jason Cooley is Support Services Manager at Tech Experts.

Internet security changes all the time and so does the variety of issues. We have to be sure to run anti-virus, watch out for infections and phishing, and regularly change our passwords just to start the process of being safe on the Internet.

There are people that spend time to create these viruses and other hidden or unwanted system modifications.

While their motivation may not be known (usually money), one of the hazards of using the Internet is dealing with the headaches these things can cause.

On top of regular infections, there are many data gathering processes that can run in the background of your system.

These can be gathering data to send to someone attempting to steal your information. There are also websites that gather data when you visit, login, or create an account.

While there are instances where gathering data is used maliciously as I mentioned, it is also something legitimate sites can be guilty of. In 2019, you may have heard of sites like Google and Facebook gathering information, but what and how much are they gathering? What can you do about it?

Earlier this year, the International Computer Science Institute investigated Google and the Applications linked with its Playstore.

Applications downloaded from Google and the Playstore can gather data, and that can be used to create your Advertising ID. This ID is unique, but is and can be reset.

Many applications were also linking that Advertising ID with the hardware IDs of a device, such as the MAC address. This is forbidden as it allows the data to be permanently stored, even when you erase your history and erase the application data. Google is addressing the issue and already forcing some applications to change its data gathering process.

Google is also stepping up security for mobile devices in another way. Users that are familiar with Chrome and its password storing may know the browser version of Google can suggest a strong password.

This is now coming to mobile devices as well, which will sync security across all devices, prompting you to use a strong and unique password when it is determined your password is weak or frequently used.

Facebook may be the king of data harvesting. I am sure many of you have searched for something on the Internet, then noticed ads on Facebook showing that item. This is part of targeted advertising done by Facebook.

Facebook has the ability to follow you around the web, checking your browser habits and collecting user data anytime you are on a site with a Like or comment section from Facebook attached.

Mozilla Firefox introduced the Facebook Container extension for its browser last year, which keeps Facebook isolated.

While it has been out for awhile, 2.0 was just released, which blocks those sites with the Facebook links from gathering information.

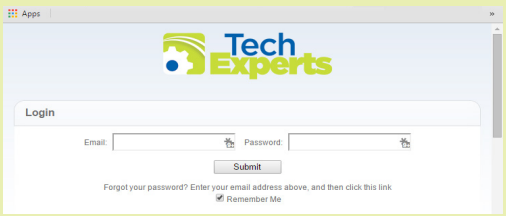
Firefox is stepping up the anti-tracking to another level as well. The browser debuted its new "Enhanced Tracking Protection." Mozilla teamed up with Disconnect, an open source anti-tracking program to create this new protection that blocks over 1,000 third party websites from gathering data while you browse the Internet.

This feature is enabled by default once the browser is updated to its newest version.

Some may not worry about their privacy online, but for those who do, it's time to update.

Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com



How To Save Your Business From Phishing Scams

Alexander Stahl is a help desk intern at Tech Experts.

Workplaces today are filled with computers and machines, but just as these workstations optimize efficiency and profit, they also increase the possibility of attacks designed to steal, destroy, or corrupt your data through the use of malicious programs.

The most probable avenue for these malicious programs is through phishing scams. To understand how to stop these attacks, you must first understand what a phishing scam entails.

A phishing scam is an attempt for someone to steal sensitive information or install malware onto your PC by tricking you into clicking a link, opening an attachment, or providing personal information.

Although these attacks use tactics that trick people every day, you can stay safe by staying smart. Through time and practice, it can become easy to spot a phishing attack and keep your PC and personal information safe.

If you receive an email containing a threatening message, usually one demanding immediate action, it is probably a phishing scam. Most of these messages try to trick users into clicking a link or opening an attachment with threatening messages like, "Your account has been compromised! You are no longer protected! Click here to protect your account!"

Once you click the link, though, you are redirected to a phishing site.

Another example may be what seems to be an email from your boss' boss demanding sensitive information to complete company documentation.

Always beware when you see a threatening or demanding message.

Another indicator of a phishing scam is an unfamiliar email address or domain name. Some scammers may use domain names or email addresses similar to your normal contacts, but they will never be the same. If you notice an inconsistency, report the email.

Phishing scams can also normally be identified by the sender's grammar skills. Here is an example from a phishing email: "Click here to cancel this request, else your öffice 365 accöunt…" Terrible grammar and unfamiliar characters as shown here are indicators of a scam.

Lastly, be wary of any request for any type of personal or sensitive information whatsoever, even if it initially seems to be from a trustworthy source.

Even if it does not show any other signs of being a phishing scam, always double and triple-check the authenticity of the request.

If you do stumble across a phishing scam, your best course of action would be to delete the email in question without opening any attachments or clicking any links.

In addition, you should report the incident to your superior or your IT service provider. If a phishing attack happened to you, it can happen to your coworkers as well.

Giving sensitive company information away to a scammer is the last way you want to start your week.

Their tactics are always changing, so the best way to fight attacks like these is through education and awareness rather than programs or filters. Remember the red flags of a phishing scam, and you will have no problem keeping your business safe and secure.

"A phishing scam is an attempt for someone to steal sensitive information or install malware onto your PC by tricking you into clicking a link, opening an attachment, or providing personal information."

Three Reasons To Regularly Test Business Systems

Protecting your business requires more time, effort and energy from your technology team than ever before.

Business systems are increasingly complex, requiring staff members to continually learn and adapt to changing conditions and new threats as they emerge.

It's not unusual for a single ransomware incident to wreak havoc on carefully balanced systems, and this type of attack can be particularly damaging if you do not have the backup and disaster recovery procedures in place to regain critical operations quickly.

From checking for system vulnerabilities to identifying weak points in your processes, here are some reasons why it is so important to regularly test your business systems.

Business System Testing Helps Find Vulnerabilities

The seismic shift in the way business systems work is still settling, making it especially challenging to find the ever-changing vulnerabilities in your systems. Cloud-based applications connect in a variety of different ways, causing additional steps for infrastructure teams as they review the data connectors and storage locations.

Each of these connections is a potential point of failure and could represent a weakness where a cybercriminal could take advantage of to infiltrate your sensitive business and financial data. Regular business system testing allows your technology teams to determine where your defenses may need to be shored up.

As the business continues to evolve through digital transformation, this regular testing and documentation of the results allow your teams to grow their comfort level with the interconnected nature of today's systems — which is extremely valuable knowledge to share within the organization in the event of a system outage or failure.

Experts note that system testing is being "shifted left", or pushed earlier in the development cycle. This helps ensure that vulnerabilities are addressed before systems are fully launched, helping to protect business systems and data.

Business System Testing Provides Valuable Insight Into Process Improvement Needs

Business process improvement and automation are never-ending goals, as there are always new tools available that can help optimize the digital and physical operations of your business.

Reviewing business systems in depth allows you to gain a higher-level understanding of the various processes that surround your business systems, allowing you to identify inefficiencies as well as processes that could leave holes in your cybersecurity net.

Prioritizing these process improvements helps identify any crucial needs that can bring significant business value, too. This process of continuous improvement solidifies your business systems and hardens security over time by tightening security and allowing you to review user permissions and individual levels of authority within your business infrastructure and systems.

Business System Testing Allows You to Affirm Your Disaster Recovery Strategy

Your backup and disaster recovery strategy is an integral part of your business.

Although you hope you never have to use it, no business is fully protected without a detailed disaster recovery plan of attack — complete with assigned accountabilities and deliverables. It's no longer a matter of "if" your business is attacked but "when", and your technology team must be prepared for that eventuality.

Business testing allows you to review your backup and disaster recovery strategy with the parties that will be engaged to execute it, providing an opportunity for any necessary revisions or adjustments to the plans.

Whether a business system outage comes from a user who is careless with a device or password, a cybercriminal manages to infiltrate your systems or your business systems are damaged in fire or flood, your IT team will be ready to bring your business back online quickly.

Regularly testing your business policies and procedures and validating your disaster recovery plan puts your organization in a safer space when it comes to overcoming an incident that impacts your ability to conduct business.

The complexity of dealing with multi-cloud environments can stymie even the most hardened technology teams, and the added comfort level that is gained by regular testing helps promote ongoing learning and system familiarity for your teams. No one wants to have to rebuild your infrastructure or business systems from the ground up, but running testing procedures over time can help promote a higher level of comfort within teams and vendor partners if the unthinkable does occur.

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