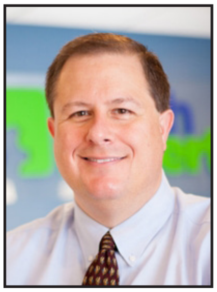
April 2021

TechTidbit.com

brought to you by Tech Experts

Over $1 Trillion Lost To Cyber-crime Every Year



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

$1 trillion! That's a lot of money. And it's a figure that's increased by more than 50% since 2018.

In 2019, two-thirds of all organizations reported some type of incident relating to cyber-crime.

You could make a sure bet this figure rose significantly last year, thanks to criminals taking advantage of the pandemic.

It's easy to look at big figures like these and not relate them back to your own business. But here's the thing. The average cost of a data breach to a business is estimated to be around $500,000.

The most common types of crime are 1) ransomware, where your data is locked away until you pay a ransom fee.

And 2) phishing, where criminals pretend to be someone else to get you to click on a bad link. This is how they get access to critical systems.

That huge average breach figure includes:

- Any ransom demanded by criminals who lock your data and remove your access to it
- The cost of recovering your data and undoing the extensive damage done
- Putting in place additional ongoing security measures after the breach.

On top of the financial impact, there's the reputational one.

Could you imagine picking up the phone to every single client to tell them your data about them had been accessed and stolen? And was probably for sale on the dark web?

What would happen if the local media or news blogs got hold of this and ran a story about it?

There are other consequences. 92% of businesses that are hacked say there's an enormous impact on company performance.

Plus, they lose on average 9 hours of work time, per member of staff.

You must ask yourself very carefully: Could your business afford to be hit by a ransomware or phishing attack? The truth is that many small businesses really couldn't.

So why do so few businesses have a plan in place to a) prevent and b) respond to cyber-crime?

It's estimated that more than half of businesses don't have a plan. Does yours?

If not, it's time to do something about it. There's been an explosion in the number of ransomware and phishing attacks over the past couple of years.

If you don't have an effective plan in place to keep your business protected – and to minimize damage should the worst happen – you're leaving yourself vulnerable.

Cyber-criminals are targeting all businesses all the time, using clever automated tools that sniff out vulnerabilities. So, it's only a matter of time till your business's defenses are tested.

Here's our recommended five step plan to prepare for an attack, and protect your business.

Training, training, training

Believe it or not, your devices and software aren't the weakest link in your defense. Your people are.

Your team's awareness of the risks, and their mindset towards spotting risks and acting on them, can make a dramatic difference towards your chances of being affected.

Although they'd never knowingly do a thing to damage your business, all it takes is one click for them to bring you down.

One click. On one bad link. In one email.

Continued on page 4

Phishing scams are getting more sophisticated every day, and they're easy to fall for. You don't have to be an 80-year-old email newbie to fall for a phishing scam these days. With some of the smartest social engineering, even the wariest person can be caught out.

Phishers Lure Targets In With COVID-19 Schemes

> *"Attackers know this. In fact, they count on it. Phishers rely on human nature, and that is what makes it hard for the end user: you have to go against your basic human emotions."*

Mark Funchion is a network technician at Tech Experts.

You may have noticed that we talk about phishing a lot. Unfortunately, phishing is an issue that will never go away and the tactics change constantly. That constant change makes it difficult, if not impossible, to eliminate as a threat.

Fortunately, there are red flags that end users can keep an eye out for.

If you get an email that answers a common demand, treat it with a high level of skepticism.

For example, a few years ago when the Nintendo Wii was hard to find and a lot of people wanted them, a lot of "Click here to buy a Wii now!" emails went out. I think you can guess how many people actually got a Wii through those schemes.

Well, it's not Christmas, but the ongoing hot topic in the world is COVID-19 and its vaccine.

As we strive to return to normalcy, there are people who want the vaccine who do not qualify yet, are on a waiting list, or want to get it in a quick and easy way.

Attackers know this. In fact, they count on it. Phishers rely on human nature, and that is what makes it hard for the end user: you have to go against your basic human emotions.

All emails should be evaluated as if they are a phishing email. Look for the standard warning signs such as an offer that's too good to be true, misspelled words, or if the wording of the message is a little off. Some are very obvious. Some are more subtle.

The attackers may also appear as though they are from a reputable company like a national pharmacy chain, a local doctor, or a large hospital system.

However, the typical format legitimate providers follow is that they'll send you information on the vaccine and remind you to contact your health care professional to schedule an appointment.

Another example of the phishers' methods is that they'll send a link asking you to verify your information to determine eligibility (or even a link to buy the vaccine from a supplier).

Again, red flags. Take a moment to ask yourself why – when the vaccine distribution is so controlled – would a random person have a surplus of product?

These are all pretty basic ideas, but it is easy to get lax in proceeding with caution. It's even more of a challenge to stay alert when the attacks are using current events to their advantage.

The days of free money from a "Nigerian Prince" are mostly over, but almost everything we do right now is influenced by COVID.

If and when you get the message asking you to "click here to verify your vaccine eligibility," don't do it. Next month, when you are hit with messages for updates on your taxes or missing money, don't click on those either. Later this year at Christmas, don't click on the link for the discounted, hot item everyone wants. And in 2022… rinse and repeat.

Phishing will always find a way to be relevant, and you can never let your guard down.

Please Don't Give Everyone Access To Everything

With so many potential vulnerabilities in every business IT system, there is no "silver bullet" - no single safety measure that will let you sit back and relax, knowing your IT is safe and data is secure.

Most of the risks are ongoing and constantly changing. They need an active approach to stop your business falling victim to a data breach or malicious cyber-attack.

It would take a lot more space than is available in this newsletter to talk about all the risks you face.

So instead, we can talk about two of the most important things you can do to stay safe.

Make sure your team only has access to the data it needs

Keep an eye on who has access to what and whether they need it.

The more people have access to sensitive data, the more potential routes there are for the wrong people to get access to it.

If you give everybody access to everything, all it will take is for one account to become compromised.

And before you know it, criminals armed with malware will have access to your systems.

Just as important as this is how you manage the IT accounts of people who leave the business or change jobs internally.

For example, if an employee switches from accounting to a management job in a completely different part of the business, they probably won't need to keep access to all the data they needed for their last role. Failing to adjust permissions only adds to your level of risk. When people leave your business, you must immediately restrict their access to your systems and data. Implement appropriate policies and processes to reduce the risk of something slipping through.

Keep your devices secure

Another important thing to watch out for is how frequently you're installing updates on devices. This includes tablets and phones as well as computers. They must all be kept updated with the latest security patches. All it takes is one weak link for your whole business to potentially be compromised.

Make sure that you replace old devices that are no longer getting updates, or can't support the latest versions of software. And of course, it's also important to make sure that all devices are backed up in real time.

Consider computer and mobile device encryption. It turns the data into unreadable garbage if the wrong person gets hold of your device.

"Consider computer and mobile device encryption. It turns the data into unreadable garbage if the wrong person gets hold of your device."

Three Trillion Minutes On Zoom (Is That Just This Week?)

Zoom calls… Teams meetings… Google Meets… whichever tech platform your business uses*, do you ever get to a Friday evening and feel a bit "over Zoomed?" Especially if you then have ANOTHER Zoom arranged with friends or family?

According to estimates, over three trillion minutes will be spent on Zoom this year. That's about 5.5 million years!

As much as they're a pain when you have them all day, video calls really do help us be productive and get things done while we're working remotely.

76% of all employees use video calling for remote work, according to some stats we've been reading. Three quarters of those say it makes them more productive. 41% of employers believe video calls lead to better engaged teams.

How to feel less "over Zoomed" then… here are three suggested rules that have worked well for us.

1. Do a tech test before every meeting: Check your video and sound are working. Zoom has a test call facility at www.zoom.us/test

2. Never meet unless you have a written agenda: And put the agenda on screen using screen share. This stops meetings from dragging on.

3. Stand up, especially if you're the organizer: This is good for real life meetings, too. When you stand for a meeting, your body will give you feedback when the meeting's dragging. Standing desks are a great idea for productivity and keeping energy levels high.

* Side note: Do you remember in the old days (2018) when people used GoToMeeting for video calls? Or the really, really old days (2017) when we used Skype?

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

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

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.

Over $1 Trillion Lost To Cyber-crime Every Year, continued

Phishing scams are getting more sophisticated every day, and they're easy to fall for. You don't have to be an 80-year-old email newbie to fall for a phishing scam these days. With some of the smartest social engineering, even the wariest person can be caught out.

Fortunately, with the right training, your team can be taught the tell-tale signs of a scam email, looking at:

- The email address it was sent from
- The language used
- The font and design of the email
- How to check if a link is safe before clicking on it

Back-up all data, all the time

We can't stress this enough: if you don't already have an automated daily back-up of your data every day that's kept somewhere other than your business's premises, arrange this today.

Keeping a copy of all your data in this way is your fall-back option. If anything ever goes wrong and your data is lost, corrupted, or held to ransom, you retain a copy of everything you need to keep your business functioning.

If you already have off-site back-up in place, well done. Now check that it's working as it should be. This is a process known as verification, and it needs to be done every day.

You'd be surprised to learn how many people leave their back-up unchecked until they need it… only to find the back-up stopped working a few days earlier or the data was corrupted.

Use the tools available to you

There are a lot of tools out there to help keep your business safe and protected from cyber-criminals. Make use of them.

Some of the most used tools are:

- Password managers: These generate long random character passwords for new applications, then remember them so you don't have to
- Multi-factor authentication: This is where you enter a code from another device to prove it's really you logging in
- VPNs: A Virtual Private Network gives you a secure connection to your business when working remotely
- Encryption: This makes the content of your devices look like thousands of random characters to anyone without the encryption key. So, it's only a minor inconvenience if you lose a device, not a major catastrophe.

PPP

Create a policy, protocol, and procedure in the event of a data breach. Sounds obvious, but this needs to be done before your business has a problem.

Your policy will set out how your business will deal with any form of data breach or cyber-attack.

Make your policy as detailed as possible, as it's a guide for your company to reach the most desired outcome (in this case, minimal impact from an attack).

Include the things your people must do as a minimum to help keep the business safe, such as using a password manager and multi-factor authentication.

Every member of staff in your business should have a copy of this policy, ideally in your company handbook. Maybe you'd even get them to sign that they've read it and are committed to it.

That way, no one can plead ignorance if they've directly put your company at risk.

Your protocol is a written plan that contains the procedures your people must follow in the event of a cyber-attack.

Bring in the experts

If you're not an IT expert, a lot of this can seem very time consuming and complicated.

We completely get that. However, you should understand that it's very much a worthwhile investment of your time and energy.

If you feel it's not something that you can do justice, it's a smart idea to bring in the experts.

A great IT support provider – or IT support partner, in this case – should be more than willing to help you.

In fact, a great IT support partner will get it all done for you, without you having to prompt them. Honestly, the things we've talked about here are just the basics that you should be doing to cover yourself.

If you find you could do with some honest, expert help and advice, we'd love to be of service. Let's talk - (734) 457-5000.