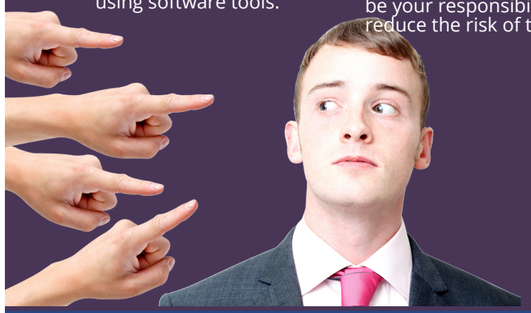
Who's to blame for a cyber security breach?

We all know what a huge danger a cyber security breach can be for a business. And just how many businesses are being breached right now.

In truth, we hate having to write this. We don't want to feel like we're scaring you, or being all doom and gloom! But it's really important that you're fully aware of the risk to your business if you suffer a breach.

Last year, the number of reported data breaches rose 68% compared to 2020.

And while it's a good idea to implement the right cyber security tools to help reduce the risk of an attack, it's practically impossible (or definitely unworkable) to give your business 100% protection from attack, just using software tools.



Because according to research, 85% of data breaches are caused by human error.

If that happens, who's to blame for your cyber security breach? Your employee? Or you, the business owner /manager?

It's a difficult question. Sure, your employee is likely the one to have clicked the link or downloaded a bad file that turned out to be malware. They may even have disabled security features to try to speed up their work.

However, as the business owner or manager, it should be your responsibility to reduce the risk of that happening in the first place.

It all starts with training your people regularly to make sure they understand the risks and how to avoid them. But you should also have the right policies in place to remind your employees of best practice, and what happens if they fail to comply.

Employees are your first line of defense against security breaches. They can only ever be as good as your cyber security strategy. Get that in place and everyone knows:

- What's expected of them
- How to avoid risk
- What to do if things go wrong.

We say, don't worry about who's to blame – just get your ducks in a row, starting with your cyber security strategy. If we can help, get in touch.

RIVERCITY TECHNOLOGY SERVICES LTD

This is how you can get in touch with us:

CALL: 306-933-3355 | EMAIL: hello@rivercitytech.ca

WEBSITE: www.rivercitytech.ca

SEPTEMBER 2022

RIVERCITY TECHNOLOGY SERVICES LTD

THE MONTHLY DOWNLOAD

Your monthly newsletter, written for humans not geeks

Here's why you need to automate more, now

Most staff love automation.

Because it's about creating a set of rules that software can follow automatically, so humans don't need to do boring and repetitive tasks.

Who in your business would be against that?!

As well as saving you and your employees valuable time, automation has loads of other benefits for a business.

You should see a productivity boost as people can get more done in the same amount of time. It can also produce a leap in motivation and job satisfaction.

That's because your people are spending longer enjoying the work they do.

They'll feel more listened to as you've made their jobs better, and will reward that with increased loyalty. Recruitment might be easier as your reputation gets a boost.

Another benefit of automating tasks is for your customers. Perhaps they can get a response to a question a lot faster. Or maybe have a smoother experience when they deal directly with you.

So which tasks in your business could be automated? Even the simplest automations can have a really big impact on the way your business works.

DID YOU KNOW... your executives might be your weakest link?

When it comes to cyber security, your executive-level managers might be the least vigilant members of your team.

A recent report showed that a huge 49% of execs had requested to bypass security measures on at least one occasion over the past 12 months.

If you're already in the practice of regularly training your people in cyber security, are you including everyone in the business, from the top down? It's one of the best ways to make sure all your people are aware of the risks of skipping vital security steps.

Technology update

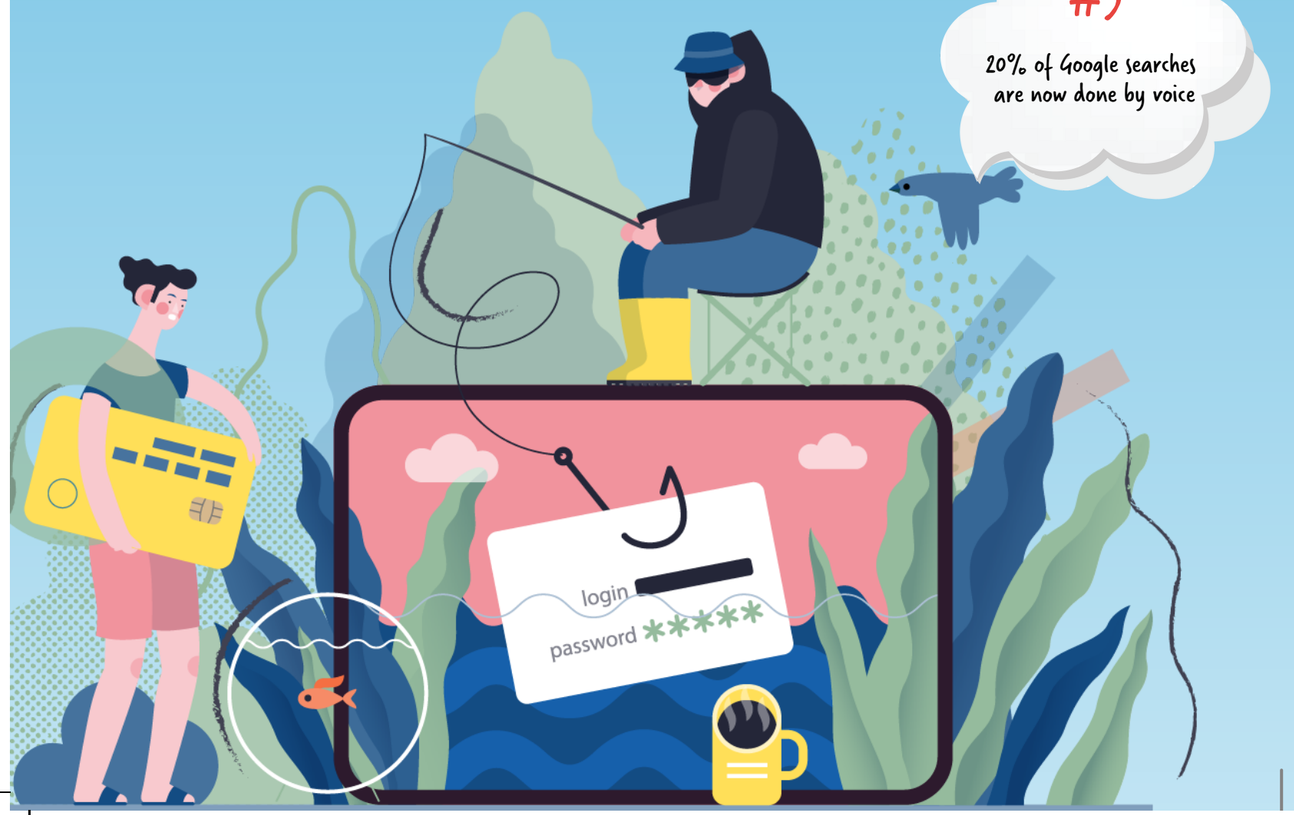
Home and small office routers are being targeted by cyber criminals in an attempt to steal sensitive data.

This is a smart move by the bad guys, as these routers exist outside of your business's usual security protection. It means they may have additional weaknesses to exploit.

How to protect your data?

If you have remote or hybrid workers, you need to make sure they have the right firewalls installed so that incoming and outgoing traffic can be monitored.

Insisting they use company devices for business work is a good idea. You can also give them encrypted connections when they're working away from the office.



TECH FACTS

#1

Nearly three quarters of execs believe AI will be a business advantage in the future

#2

A typical person spends an average of 6 hours and 55 minutes online, daily

#3

20% of Google searches are now done by voice

INSPIRATIONAL QUOTE OF THE MONTH

"Just because something doesn't do what you planned it to do doesn't mean it's useless."

Thomas Edison, Inventor, and business legend

Q&A

Q: I just closed an Office file without saving it. Please tell me I can get it back?

A: You should be able to recover your file, with a bit of luck. If you saved the document once, AutoSave may have done its job. Otherwise, try using AutoRecover or check your temporary files.

Q: I've had an email telling me an account needs updating. Is it genuine?

A: Don't click any links in the email. If you're even slightly unsure, the safest thing is to visit the website by typing the URL into your web browser.

Q: I can't open an email attachment

A: First make sure this is a genuine file – phone the sender to check. Then, it's possible you don't have the software the file was created with. Right click the document and select 'Open With' to see if there's another option.

IT'S TIME FOR ANOTHER MONTHLY QUIZ!

Winner gets bragging rights for 30 days.

1. How many generations of computer have been invented (so far)?
2. What does CPU stand for?
3. Which company designed the first CPU?
4. What's the name of the information storage used to store short-term running programs and data in a computer?
5. Which company invented the USB port?

The answer are below.

1) Five. The first generation started in 1940 with the vacuum tube. Our current generation is starting to use AI
2) Central Processing Unit
3) Intel
4) RAM (Random Access Memory)
5) It's Intel, again. The first USB-compatible product was a Mac in 1998, followed by USB support for Windows 98 a year later. The rest is history

NEW TO MICROSOFT 365

Managing your Outlook signature in one place

You know when you set an email signature in Outlook on one device, but when you use Outlook on the web, the signature isn't there?

It's a frustration that's been around for years. Traditionally the solution has been to use independent software to manage your signatures.

But Microsoft is hard at work changing the way it stores signature settings. It is moving them to the cloud, so you get a consistent experience wherever you use Outlook.

It's due to go into testing this month and be available next month... although it's been delayed for a couple of years up to this point, so... watch this space.