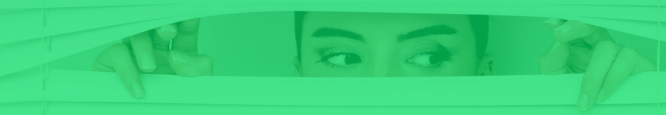
OCTOBER 2025

Your monthly newsletter, written for humans not geeks

TECHNOLOGY INSIDER



The hidden cybersecurity risk in your business

It happens far too often. An SMB believes its cybersecurity is under control…

…until a routine check uncovers something unexpected, like an old piece of malware quietly running in the background. Or a phishing attack that slipped through weeks ago.

These incidents don't usually involve cutting-edge hackers or advanced tools. They succeed because simple, everyday safeguards have been missed.

One of the biggest reasons those basics get missed?

Employee burnout.

Yep. When staff are tired, stressed, or stretched too thin, important cybersecurity habits start to slide.

And in businesses without a dedicated IT team, people are already wearing multiple hats.

- A manager might put off installing an important software update because they're trying to get quotes out before a deadline
- An accounts assistant might click a suspicious link because they're working late to balance the books and rushing through emails
- A senior staff member might skip checking security settings on a new device because they're busy keeping operations running

This isn't about carelessness. It's about capacity.

Cybersecurity depends on routine discipline. Applying updates, checking access controls, and staying vigilant for unusual activity. When teams are overwhelmed, those routines break down.

Attackers are aware of this, and many of today's most common threats rely on it.
Even basic scams, like fake login pages or convincing emails that trick staff into running malicious code, only need a single moment of inattention to succeed.

Technology alone can't prevent that.

The most effective protection often starts with looking after the people responsible for keeping systems safe. Realistic workloads, clear priorities, and regular training can all help employees stay alert and confident.

Creating a culture where it's acceptable to pause and double-check can make all the difference.

When staff feel supported and have the bandwidth to focus on the fundamentals, those simple, routine defenses work exactly as they should. And that's often enough to stop an attack before it begins.

If you need help staying on top of your cybersecurity, we can help. Get in touch.

DID YOU KNOW…

even Elmo needs cybersecurity training?

Elmo, the lovable Sesame Street star, recently had his official X (formerly Twitter) account hacked. And some very un-family-friendly posts were made.

Experts quickly pointed out that a simple security step called Two-Factor Authentication (2FA) could have stopped the hackers. That's the extra step where, after your password, you also need a code from your phone or an app to log in.

It's a basic safeguard every business should use on social media, email, and banking accounts. And if it's important enough for Elmo to learn, it's definitely important for your team too.

TechFacts

1. Amazon now has almost as many robots in its warehouses as it does human workers. Over a million robots are busy zipping around, picking, packing, and moving goods alongside people in sites all over the world. It's a glimpse into how automation is reshaping the way businesses operate behind the scenes.

2. Korean scientists have been testing a new kind of PC filter inspired by the human nose. It uses a light coating of oil (just like the mucus on our nasal hairs) to trap dust more effectively and keep the inside of a computer clean. It might sound a bit gross, but it could mean far less dust clogging up your devices in the future.

3. Scientists in Japan have smashed the world record for internet speed, hitting 1.02 petabits per second. That's about 127,500 gigabytes every single second, over 1,800 km of fiber optic cable. To put that in perspective, it's roughly 350,000 times faster than the average home broadband. At that speed, you could download the entire Netflix library in under a second.

Technology update

Hotpatching is GO

Hotpatching is now part of Windows Autopatch, which you manage using Microsoft Intune (a tool to look after your company's devices). This makes it easier to keep devices secure without stopping people from working.

What's Hotpatching, you ask?

Hotpatching installs Windows quality updates in the background, without forcing a restart. Your team stays protected while staying productive.

Any new update policies created in Intune have this switched on by default. And existing policies can be updated by enabling the "apply without restarting the device (hotpatch)" option in the Intune admin center.

It's a simple change that helps reduce downtime and keeps your devices compliant with the latest security updates.

INSPIRATIONAL QUOTE OF THE MONTH

"The quality of a leader is reflected in the standards they set for themselves."

Ray Kroc, businessman behind McDonald's global expansion.

Tech or treat? It's October's fun tech quiz...

1. What is the function of a CPU in a computer?
2. What's the difference between a file and a folder in a computer's file system?
3. What makes "Save" and "Save As" different in most applications?
4. What's the purpose of a web browser's "private browsing" or "incognito mode"?
5. Which file extension typically indicates a video file?

The answers are below.

1. The Central Processing Unit processes data and executes instructions. It's the main control center of your computer
2. A file is a container for storing data, while a folder is a collection of files
3. "Save" overwrites the existing file, while "Save As" lets you save a copy with a new name or location
4. It stops your browsing history and cookies being stored on your computer
5. MP4

NEW TO

MICROSOFT

More control over your software

Microsoft's testing a new policy that could make it much easier to remove Windows built-in apps you don't want. In a recent preview build, there's an option called "Remove Default Microsoft Store packages from the system" tucked under Administrative Templates.

Turn it on, and it lets you tick apps like Teams, Weather, Xbox services, or even Snipping Tool and Paint (if you really want to). Then remove them in one go, instead of uninstalling each individually.

Core apps like Edge are still untouchable, and the feature is still in testing. But it's a step toward giving businesses more control over the software on their devices.

5 cyber scams your business should watch out for

Cyber scams don't need to be sophisticated to cause serious damage to a business.

In fact, many of today's most effective scams rely on busy people making quick decisions and not having time to double-check what they're doing.

Staying informed is one of the best ways to stay protected. **So here are five scams we're seeing right now:**

1 Robocall scams

With artificial intelligence, scammers can clone someone's voice using only a short audio clip. You get a call that sounds exactly like a supplier or even a colleague, asking you to urgently confirm bank details. It feels genuine, but it isn't.

Some scams even use this information to carry out a "SIM swap", tricking a phone provider into moving your number to a criminal's SIM card so they can intercept security codes.

2 Crypto investment scams

A convincing email or social media post might offer an incredible return on a business investment. Some of these projects, known as "rug pulls", are designed to collect funds and then disappear, leaving investors with nothing.

3 Romance scams (sometimes called pig-butchering scams)

These might sound unrelated to business, but they're not. Scammers build trust over weeks or months, often through social media or messaging apps, and then persuade someone to share sensitive information or even send money.

In some cases, they use AI-generated images or videos to make the scam more believable and later threaten to leak personal material unless they're paid.

4 Malvertising

Criminals hide malicious links inside paid ads on legitimate sites. An employee looking for a new supplier or tool could click an ad and unknowingly install malware onto a company laptop.

5 Formjacking

This is where criminals inject code into an online checkout form to steal payment or login details. If staff buy supplies or services from websites that aren't secure, those details can be intercepted.

The common thread is simple: **These scams exploit human attention and trust.**

Regular reminders and training help staff stay alert, question unexpected requests, and think twice before clicking. A little extra caution can stop a scam before it starts.

We can help you make sure your team is vigilant about these scams and more? Get in touch.

Q: Is it ok to let staff install their own apps on work devices?

A: Not without approval. Unchecked apps can introduce malware or data leaks.

Q: How often should we test our data backups?

A: A few times a year at a minimum and check your backup is working weekly. A backup isn't useful if it doesn't restore when you need it.

Q: Can we save money by turning off automatic software updates?

A: No. It might save a little time now but leaves you wide open to attacks fixed by those updates.

Business gadget of the month

Plugable 4 HDMI Multi Monitor Adapter

Sometimes one monitor isn't enough, right? You're busy working across multiple apps, trying to get lots done. You need to see more.

But what happens when two monitors aren't enough?

That's where the Plugable Multi-Monitor Adapter comes in. It lets you connect up to 4 monitors to your device. So now you'll need another excuse for "missing" that email about that last-minute meeting you wanted to avoid.

$124.95 from Amazon.

This is how you can get in touch with us:

CALL: 509-956-4916 | EMAIL info@nexgenwa.com
WEBSITE: nexgenwa.com

nexGen TECHNOLOGY SERVICES