CYBERSECURITY TIP

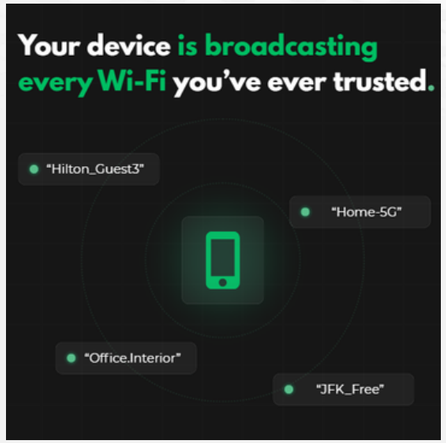
Your phone broadcasts the names of your saved Wi-Fi networks wherever you travel.

Mobile devices and laptops constantly search for previously connected networks.

Attackers deploy portable hardware that mimics common network names, such as generic hotel or coffee shop Wi-Fi.

If your device is configured to automatically connect to known network names, it will join the malicious network without requiring your approval. The attacker then intercepts the data transmitted from your device.

Disable the "Auto-Join" or "Auto-Connect" feature for all networks on your company devices. Require your employees to manually select networks when working remotely.



...continued from page 3

In one business, there's no clear next step. No one knows who handles recovery. Someone suggests, "Maybe Dave knows," but Dave's on vacation. People wait just in case. By lunch, half the day is gone.

In another business, the issue gets reported immediately. The response is clear. Files are restored. The employee is back to work.

Same coffee. Same mistake. Completely different day. The difference isn't luck. It's recovery speed and clarity.

Why Well-Run Businesses Make Problems Boring

Here's the shift most businesses miss: The goal isn't to prevent every possible problem. That's impossible.

The goal is to make mistakes boring. Boring means no scrambling, no guessing, no long pauses, no "who's on this?" moments.

When problems are boring, they don't derail the day. They get handled and everyone moves on.

This Is a Leadership Issue, Not a Tech Issue

When small problems cause big slowdowns, it's rarely because of the tools themselves.

It's because:

- There's no clear plan for what happens next
- Responsibility is fuzzy
- Recovery depends on the right person being available
- The business hasn't defined what back to normal means

What people feel isn't the error or the outage; it's the uncertainty.

Well-run businesses remove that uncertainty.

A Simple Question Worth Asking

You don't need a dramatic audit to start thinking differently about this. Just ask one question: If something small went wrong today, how long would it take for everyone to get back to work?

If the answer is unclear, that's not a failure. It's information that guides the first step toward smoother days, less downtime and work that keeps moving even when a hiccup inevitably happens.

What This Really Comes Down To

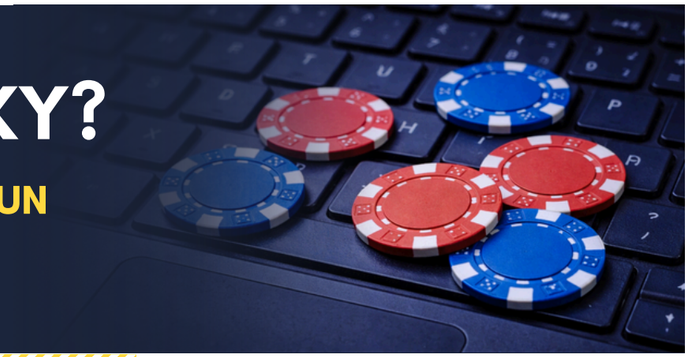
Businesses that stay productive when a normal day quietly goes sideways aren't the ones that avoid mistakes. They're the ones that recover so quickly the mistake barely registers. That doesn't require perfection. It requires clarity.

When recovery is clear and quick, problems become forgettable, momentum remains and a cup of coffee stays just a cup of coffee.

TECHNOLOGY TIMES
Insider Tips to Make Your Business Run Faster, Easier and More Profitably
APRIL 2026

FEELING LUCKY?

THAT'S NOT HOW WELL-RUN BUSINESSES OPERATE



Luck is fun and festive, but well-run businesses don't operate on luck.

No owner would ever say:

- "Our hiring strategy is whoever walks in."
- "Our sales plan is hoping customers find us."
- "Our accounting approach is the numbers working themselves out."

That would be absurd.

The Quiet Double Standard

Somewhere along the way, technology unintentionally gets a pass.

"We've never had an issue."
"It's probably backed up somewhere."
"We'll deal with it if something happens."

That's not a plan. That's superstition dressed up as strategy. Unless you've got a leprechaun assigned to your IT systems, it's a risky bet.

Most owners would never leave payroll, taxes or customer service to chance. Yet when it comes to technology recovery, hope somehow feels acceptable.

Why 'We've Been Fine So Far' Doesn't Hold Up

Here's the trap: When nothing bad has happened, it feels like proof that nothing will.

Every business that's had a long, chaotic, how-did-this-happen day said "we've been fine" the morning before.

Luck isn't a system. It's just risk you haven't met yet.

Think of it like driving without insurance. You might get away with it for years, but the day something goes wrong, you'll wish you had a plan.

Prepared vs. Hoping for the Best

Most businesses don't discover how unprepared they are until they're in trouble.

That's when the questions start:

- Do we have a backup?
- How recent is it?
- Who handles this?
- How long will we be down?

Prepared businesses already know the answers. Luck-reliant businesses find out in real time.

Being prepared doesn't mean expecting disaster. Think about it this way: When your systems are tested and documented, a hiccup is just another Tuesday.

When they're not, that same hiccup can turn into a full-blown crisis.

Customers notice, employees get frustrated and suddenly you're spending more time fixing problems than running your business.

The Reality Check

If your accountant managed books the way you manage tech recovery, would you be okay with that? Why give technology a pass?

TechSage Solutions

YOUR ACCOUNTANT IS STRESSED.

HACKERS KNOW IT.

Your accountant is buried. Your bookkeeper is scrambling. Deadlines are looming. Emails are flying faster than anyone can keep up. Everyone is heads down, trying to get through tax season. This isn't news to you, and it's not news to hackers either.

Phishing attempts surge during tax season. Their messages aren't dramatic. They blend in with everyday business requests, right when people are busiest. That's not coincidence. That's strategic timing.

The Stressed Supply Chain

Here's what most people miss: Hackers aren't just targeting accounting firms; they're targeting the chaos around them.

During tax season:

- Clients rush to send sensitive documents
- Staff shortcut normal checks to keep up with volume
- "Just send me the file" replaces usual caution
- Verification gets skipped because everyone is slammed

The whole ecosystem speeds up, making mistakes more common. Hackers don't go after calm, methodical businesses. They go after the busy ones.

What These Attacks Look Like

This isn't a movie plot. It's an email that looks exactly like the others in your inbox:

- A message from "your accountant" asking you to resend documents because something didn't come through
- A note from a vendor saying their bank information has changed and needs updating
- A DocuSign request that "needs your signature today"
- An urgent email from "your CEO" who's traveling and needs help immediately

None of these feel suspicious. They feel like normal business. That's why they work.

Why Busy People Get Caught

Falling for these scams isn't about being careless. It's about being human. When inboxes are full and deadlines are tight, people don't read carefully. They scan. They assume. They react.

Bad actors know this. Their messages are designed for people who are moving too fast to notice the one detail that's off. They don't need you to be reckless. They need you to be busy.

4 Simple Ways to Avoid Being an Easy Target

You don't need fancy tools or a security team to reduce your risk. You just need a few intentional habits during busy months.

1. Verify payment changes by phone

If an email says a vendor's banking details have changed, don't reply to the message. Call a number you trust to verbally confirm.

2. Slow down requests for sensitive information

Urgency should be a signal to pause, not to rush. If someone asks for bank statements, tax documents or other financial files "right now," take a moment to verify.

3. Confirm urgent requests through a second channel

If an email claims something is urgent, verify it another way. A quick call, text or internal message can stop a bad decision before it starts. Real urgency can survive a two-minute check.

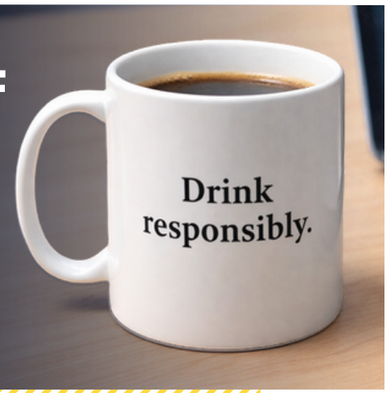
4. Give your team a five-minute heads-up

Remind your team that it's okay to slow down, double-check and ask questions when something feels off. That small permission shift can prevent a lot of unnecessary cleanup later.

The Takeaway

The attacks showing up during tax season aren't clever. The power is in their timing. You don't have to overhaul your systems to avoid becoming the easy target, but you do need to slow down when it matters and verify when things feel urgent.

HOW A CUP OF COFFEE CAN TAKE DOWN YOUR WHOLE BUSINESS



It starts like any normal morning. Coffee in hand. Laptop open. You're settling in, ready to get moving.

Then your elbow clips the mug.

Time slows just enough for you to watch coffee spill across the keyboard and disappear into places coffee should never go.

The screen flickers.

The keyboard stops responding.

The laptop makes a noise laptops shouldn't make.

No hackers. No ransomware. No dramatic warning screens.

This completely normal moment that suddenly changes the day is how many business disruptions start.

The Problem Isn't the Mistake — It's What Happens Next

Most businesses picture downtime as something dramatic. Servers down, systems dead and everything grinding to a halt.

In reality, downtime is often as boring as a spilled drink on a laptop, a file that "definitely got saved" but now doesn't exist, an update that doesn't finish or a computer that won't boot for any obvious reason.

The real damage doesn't come from the mistake itself. It comes from the stall that follows: the waiting, the guessing, the "do we know how long this will take?"

Work doesn't fully stop. It half-stops. And half-working can be as bad as not working at all.

The Hidden Cost of Waiting

Here's what that stall usually looks like.

One person can't work, so they wait. Two others try to help but aren't sure what to do. Someone messages IT. Someone else switches tasks "for now."

Ten minutes turn into 30. Thirty turns into an hour.

Now multiply that by the number of people affected, the interruptions, the mental context switching and the momentum that never quite comes back.

Even small delays add up quickly. Not in dramatic, headline-worthy ways, but in quiet, frustrating ways that drain the day without anyone noticing until it's gone.

Same Problem, Different Outcomes

Let's rewind the coffee spill.

...continued on page 4

SHINY NEW GADGET OF THE MONTH

UGREEN NASync DXP4800 Plus

Imagine a server that not only stores files but also understands them. This AI-ready home and office server organizes your data by content, faces and locations. Instead of digging through folders, you can simply ask for a signed contract from last quarter or a video from a meeting.

It's fast, secure and sits right on your desk. Your data stays private and confidential, accessible only to you.

AI SAFETY

Can an AI outsmart your firewall?

Amazon warns that a single hacker used GenAI to breach 600 firewalls in just 5 weeks. It's a wake-up call for IT teams to evolve their defense strategies against AI-powered threats.