

KOSI BITS & BYTES

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

Spring Into a Stronger Cybersecurity Posture

April is the perfect time for organizations to review and strengthen their technology environment. As cyber threats continue to grow, maintaining a secure, reliable, and well-managed infrastructure is essential for protecting data and ensuring smooth operations. A Managed Advantage IT approach delivers consistent monitoring, timely updates, and strong security measures that reduce risk and prevent downtime. Taking steps now to refresh your cybersecurity posture helps your business stay ahead of emerging threats. For long-term protection and peace of mind, consider upgrading to our Managed Advantage IT Services today.

Ready to refresh your security this April?
Contact us today. Scan the QR code OR
Call us at 419-522-4001



SCAN HERE

April 2026

This monthly publication is provided courtesy of Jen Evans, CEO & Owner of King Office Service, Inc.



OUR MISSION:

We leverage technology to provide simple and secure solutions to enhance profitability and productivity in our clients' organizations.

KOSI - Your Trusted Local Partner for Over 45 Years!

Putting All Your Eggs in One Basket?

THAT'S NOT HOW WELL-RUN BUSINESSES OPERATE



The saying makes for a great metaphor, but it's not how strong, well-run businesses operate. No one wants everything riding in one fragile basket.

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.”

We'd never accept that in any part of the business.

The Quiet Double Standard

But for some reason, technology often gets treated differently.

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

These aren't real plans, they're assumptions. And assumptions leave you with all your eggs in one unsupported basket.

Most owners would never leave payroll, taxes, or customer service up to

chance. Yet when it comes to technology recovery, uncertainty somehow slips through the cracks.

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

The problem is simple: when nothing bad has happened, it's easy to believe nothing ever will. But every business that's faced a chaotic “how did this happen?” kind of day also said, “*we've been fine*,” just hours earlier. Relying on a single approach—or worse, no documented approach at all—is exactly how things end up in one vulnerable basket.

It's a lot like driving without insurance. Everything seems fine... right up until the moment it's not. And when something goes wrong, the lack of preparation becomes a very big deal, very quickly.

Prepared vs. Hoping for the Best

Most businesses don't realize how unprepared they are until they're already in the middle of a problem. That's when questions start flying:

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

Prepared businesses already know the answers. Everyone else is scrambling to find them. Being prepared doesn't mean expecting the worst. It just means making sure small issues stay small. When systems are tested and documented, hiccups are manageable. When they're not, those same hiccups can quickly turn into bigger problems—disrupting customers, frustrating employees, and pulling attention away from running the business.

The Reality Check

If your accountant managed your financial records with the same uncertainty that surrounds your tech recovery plan, would you be comfortable with that? If not, then your technology—one of the foundation pieces of your business—deserves the same structure and attention as everything else.

AI Fools Week: Why Modern Businesses Must Stay Sharp

AI Fools Week is more than a clever name; it is a reminder that even the smartest technologies can be fooled, manipulated, or misused in ways that directly affect businesses. Created by the National Cybersecurity Alliance, AI Fools Week is a one week awareness campaign designed to educate organizations about AI security, privacy, and the growing risks of AI enabled scams.

Recent years have shown a sharp rise in AI related incidents, from deepfake scams to data leaks and AI generated misinformation. In one well known 2024 example, Samsung employees accidentally exposed confidential source code by pasting it into ChatGPT, leading the company to temporarily ban generative AI tools. In 2025, a Hong Kong finance worker was deceived into sending twenty five million dollars after joining a video call with deepfake versions of his executives.

For everyday businesses, the risk is not only advanced cybercrime but simple mistakes made during busy workdays. A notable case in early 2024 involved an Air Canada customer who used the airline's AI chatbot to secure a refund larger than company policy allowed. The issue was not hacking, but an unmonitored tool making confident, incorrect decisions.

AI Fools Week encourages organizations to be proactive: train employees to verify unusual requests, understand where AI tools are used, and follow one essential rule—AI assists, but humans approve. While the campaign lasts only a week, its message is a year round reminder to stay vigilant as AI threats evolve.

YOUR ACCOUNTANT IS STRESSED. HACKERS KNOW IT



Your accountant is buried. Your bookkeeper is scrambling. Deadlines are looming, emails are flying, and everyone is heads-down trying to survive tax season. This isn't news to you — and it isn't news to hackers either. Phishing attempts spike during this time because the messages blend in with everyday business requests. It's not coincidence — it's strategic timing.

The Stressed Supply Chain

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
- "Just send me the file" replaces usual caution
- Verification gets skipped because everyone is slammed

When the entire ecosystem speeds up, mistakes multiply. Hackers don't go after calm organizations — *they go after busy ones.*

What These Attacks Look Like

These scams aren't dramatic. They look like routine emails:

- "Your accountant" asking you to resend documents
- A vendor claiming their banking info changed

- A DocuSign request demanding same-day signature
- A message from your "traveling CEO" needing urgent help

Nothing feels suspicious and that's why they work.

Why Busy People Get Caught

Falling for these attacks isn't carelessness; it's human nature. When deadlines are tight, people skim instead of reading carefully. Attackers design messages for someone moving too fast to notice one wrong detail. They don't need you to be reckless — they just need you to be busy.

4 Simple Ways to Avoid Becoming an Easy Target

1. Verify payment changes by phone. Use a trusted number.
2. Slow down urgent information requests. Urgency means pause.
3. Confirm unusual or urgent emails through a second channel.
4. Remind your team to double-check. A quick reset prevents costly mistakes.

The Takeaway

Tax-season attacks aren't clever — *their power is timing.* You don't need new tools to stay safe. You need to slow down, verify, and think before acting when things feel urgent.

The 10 Disaster Planning Essentials For Any Small Business



Don't lose everything you've worked so hard to achieve in an instant! This report will reveal important planning strategies you should have in place now to protect yourself from common data-erasing disasters including natural hazards, human error, cyber criminals, hardware failure, software corruption and other IT failures.

Everything You've Worked For...GONE...In An Instant?

This report will be a real eye-opener for you with information that can literally "save your bacon" in the event of a digital disaster.

Claim Your **FREE 10 Disaster Planning Essentials Now**,
CALL US: at 567-323-5679
SCAN THE QR CODE: SCAN ME
GO TO: www.kingoffice.com/10essentials



SCAN ME

CARTOON OF THE MONTH



HOW A CUP OF COFFEE CAN TAKE DOWN YOUR WHOLE BUSINESS



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

Then your elbow taps 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 are not designed to make.

No hackers. No ransomware. No dramatic warning screen. Just a completely ordinary moment that instantly changes the day.

The Problem Isn't the Mistake — It's What Follows

Most people imagine downtime as something dramatic—servers crashing, systems failing, operations grinding to a halt. But real-world downtime is usually much more mundane: a spilled drink, a file that “definitely got saved” but isn't there, an update that refuses to finish, a device that won't boot for reasons unknown.

The mistake rarely causes the real damage. It's the stall afterward—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 just as disruptive as not working at all.

The Hidden Cost of Waiting

A typical stall looks like this: 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 stretch into 30. Thirty become an hour. Multiply that across people, interruptions, and lost momentum, and even tiny delays compound quickly. These aren't

headline-worthy failures. They're silent drains—the kind that erode a day without anyone realizing until it's already gone.

Same Problem, Very Different Outcomes

Rewind the coffee spill. In one business, no one knows the next step. Responsibility is vague. Someone says, “Maybe Dave knows,” but Dave's on vacation. So people wait—just in case. By lunch, half the day is gone.

In another business, the issue is 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 organizations miss: the goal isn't preventing every possible problem. That's impossible. The goal is to make problems boring. Boring means no scrambling, no guessing, no extended pauses, no “who's on this?” moments. Issues get handled, and the day keeps moving.

This Is Leadership, Not Technology

Small problems become big slowdowns not because tools fail, but because plans, roles, and expectations are unclear. Uncertainty—not the outage—is what people feel.

A Question Worth Asking

If something small went wrong today, how long would it take for everyone to get back to work? If you don't have a clear answer, that's not a failure. It's a starting point—the first step toward smoother days, less downtime, and work that keeps moving even when the inevitable hiccup happens.



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.



QUICK TECH TIP

Run a Quick “Access Audit” to Prevent Data Leaks!

Permission Clutter is one of the most common—and most overlooked—business risks. As roles shift and projects end, employees often keep permissions they no longer need. This not only increases the chance of accidental data exposure but also inflates software costs and slows down internal processes.

A quick access audit helps you regain control. Review all user accounts, disable logins tied to former employees, and ensure each team member has only the access required for their current responsibilities. This strengthens security and supports accountability across departments.

While you're reviewing permissions, look for unused Microsoft 365 or software licenses. Reassigning or removing these prevents waste and keeps your tech budget aligned with actual business needs.

A well-executed access audit protects data, reduces costs, and keeps your operations running cleanly and efficiently—small effort, big business impact.





110 West 3rd Street
Mansfield, Ohio 44902

Keeping Technology Secure & Simple

PRST STD
US POSTAGE
PAID
BOISE, ID
PERMIT 411

INSIDE
THIS ISSUE

PG 1

PUTTING ALL YOUR EGGS IN ONE BASKET?
That's Not How Well-run Businesses Operate

PG 2

YOUR ACCOUNTANT IS STRESSED.
Hackers Know It

PG 3

HOW A CUP OF COFFEE CAN TAKE
DOWN YOUR WHOLE BUSINESS

Who Wants To Win A \$25 Gift Card?

TRIVIA



What is the BEST way to
identify a phishing email?

- A. The sender asks for personal info or urgent action

B. The email uses bright colors
- C. The message includes a lot of emojis

D. The email contains an attachment

Last month's Trivia:

Q : Which cybersecurity concept ensures that data cannot be altered without detection? A : Integrity

You can be a Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question (no cheating!) and receive a \$25 gift card.

Ready? Call us right now at 419-522-4001 or send an email to katies@kingoffice.com with your answer!

If you would like to share our Newsletters and want extra copies in your office, we would be happy to provide them.
Email katies@kingoffice.com and we will take care of your request.



Makes: 20 truffles
Prep Time: 30 minutes
Total Time: 1 hour
Recipe Created By: Jodie Shield
Featured In: Illinois Farm Bureau Partners

No - Bake Sugar
Cookie Truffles

INGREDIENTS

- ❖ 12 medium-sized prepared sugar cookies

❖ ¼ cup pecans

❖ 3 cups white chocolate chips
- ❖ 8 ounces (1 package) reduced-fat cream cheese, room temperature

❖ Sprinkles, for frosting

INSTRUCTIONS

- Step 1.** In a food processor, combine the cookies and pecans. Pulse mixture into fine crumbs. Add the cream cheese and blend until thoroughly combined. The mixture should hold together when pressed.
- Step 2.** Scoop mixture into tablespoon-size portions and roll into balls. Place each ball on a parchment paper-lined platter.
- Step 3.** In a med, microwave-safe bowl, microwave white chocolate chips on high in 15-second increments, stirring between each, until completely melted and smooth.
- Step 4.** Dip each cookie ball into the white chocolate to coat completely. Return to the platter and decorate with sprinkles.
- Step 5.** Transfer platter to the refrigerator and chill until the chocolate hardens, about 30 minutes. Keep truffles refrigerated until ready to serve.
(Not in the mood for sugar cookies? Use your favorite cookie variety instead.)