

KOSI BITS & BYTES

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

Advance Your IT Readiness

March is an excellent time for organizations to reassess the strength and reliability of their technology environment. As cyber threats grow more sophisticated, maintaining a secure and well-managed infrastructure is essential for protecting data, supporting productivity, and ensuring business continuity. A comprehensive Managed IT approach provides consistent monitoring, timely updates, and proactive security measures that reduce risk and minimize disruption. By taking steps now to reinforce your cybersecurity posture, your organization is better prepared for the demanding months ahead. To enhance protection and long-term stability, we invite you to upgrade to our Fully Managed IT Services today.

Ready to Advance and want to know more?

Contact us today. Scan the QR code OR

Call us 419-522-4001



March 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!

Data Security 101:

Protect Your Office and Avoid Costly Breaches



Data security is essential for every office, no matter the size or industry. As an office manager, protecting sensitive information from breaches, leaks, and unauthorized access must remain a top priority. Strengthening everyday practices can dramatically reduce risk and help keep your organization safe and productive.

Understand the Risks

Data breaches often occur due to weak passwords, phishing attempts, malware, or insider threats. Understanding where risks originate allows you to implement the right defenses before issues arise.

Implement Strong Password Policies

Weak passwords are one of the easiest ways attackers gain access. Require employees to use strong, unique passwords that include a mix of characters. A password manager can help store and generate secure passwords. Enforcing periodic password updates adds another layer of protection.

Use Multi-Factor Authentication (MFA)

MFA provides crucial security by requiring two or more verification methods—such as a password, phone code, or biometric check. This significantly reduces the likelihood of unauthorized access.

Regularly Update Systems

Outdated software is a major entry point for cyberattacks. Updates frequently include security patches designed to close vulnerabilities. Enable automatic updates on systems and applications whenever possible to ensure continuous protection.

Encrypt Sensitive Data

Encryption keeps information safe by making it unreadable if intercepted. Encrypt emails, stored files, and data transfers to maintain confidentiality whether the data is in transit or at rest.

Educate Your Team

Human error remains one of the biggest contributors to breaches. Train employees to recognize phishing attempts, avoid suspicious links, and follow device-security best practices. Building a culture of awareness ensures everyone plays a role in protecting sensitive data.

Use Access Controls

Give employees access only to the information necessary for their roles. Following the principle of least privilege minimizes unnecessary exposure. Review access levels regularly and adjust them as responsibilities change.

Back Up Data Regularly

Routine backups protect your organization in the event of a breach, hardware failure, or

accidental loss. Store backups securely—ideally offsite—and test them periodically to ensure they can be restored quickly.

Develop an Incident Response Plan

Even with strong security, breaches can still occur. A clear response plan helps contain damage and restore operations efficiently. Define who to contact, how to contain the issue, and recovery steps. Review and update the plan regularly.

Monitor and Audit Systems

Continuous monitoring helps detect suspicious activity early. Audit logs, network traffic, and access behavior to identify vulnerabilities before they escalate.

Use Secure Communication Channels

Ensure sensitive communication occurs through secure platforms, such as encrypted email, secure messaging tools, or a VPN for remote access. Avoid personal email or unsecured apps for business communication.



DIY IT VS. MANAGED IT:

The Real Impact On Ohio Small Businesses

Ohio businesses that rely on DIY IT often underestimate the true cost of downtime and cybersecurity risks. While handling technology internally may seem budget-friendly, studies show that unplanned IT outages cost small and mid-sized U.S. businesses \$300,000 to \$540,000 per hour due to stalled operations, idle staff, and missed revenue opportunities. In Ohio, the threat landscape continues to intensify, with 88% of ransomware attacks targeting SMBs, many of which lack dedicated IT support or strong security measures.

A real-world example demonstrates the severity: ransomware attacks commonly result in 21 days of downtime, leaving companies unable to access systems or serve customers. Recovery expenses average \$5.08 million per incident, far surpassing the cost of ongoing preventative IT management. Beyond operational losses, Ohio businesses must also comply with state data-breach notification laws, adding legal, communication, and reputational costs.

In contrast, managed IT services offer a proactive and cost-effective alternative. Through continuous monitoring, timely patching, threat detection, and strategic IT planning, managed service providers help Ohio businesses minimize downtime, strengthen security, and keep employees productive. Instead of reacting to emergencies, organizations gain reliable protection at a predictable monthly cost—often far lower than the financial impact of a single major IT event.

AI Tools Are Everywhere.

Here's How to Use Them Without Making a Mess.



You log back into work after a well-deserved break and your inbox is already full. Meetings are stacking up. The to-do list is longer than you remember. You're back to doing too much with too little time. And now, on top of everything else, AI is everywhere.

Every app is pushing the same message: "Add AI." "Automate with AI." "Use AI or fall behind." Meanwhile, you're wondering where this actually helps your business and how to keep it from blowing up in your face.

Right now, AI is the new intern everyone hired without training. While interns can be amazing, they can also make big mistakes if nobody sets rules.

3 Time-Saving Ways to Use AI in Your Business

1. Inbox triage and first-draft replies

AI can scan long email threads, highlight what matters, draft first responses, and flag messages needing attention. What it can't do is interpret nuance or determine the correct final answer. The rule stays simple: AI drafts. Humans approve.

2. Meeting notes that become action lists

The real meeting challenge shows up after the meeting. AI can summarize conversations, highlight decisions, capture action items, and assign owners—reducing confusion and preventing tasks from being forgotten.

3. Simple reporting and forecasting

Business leaders rarely lack data—they lack the time to interpret it. AI can spot trends, flag anomalies, and translate raw numbers into clear summaries. Think of it as a sorting tool, not a crystal ball.

The Guardrails: How to Use AI Without Doing Something Dumb

1: Never paste sensitive data into public AI tools.

Customer info, HR data, passwords, and financials should never be entered into prompts.

Rule 2: Control who can use what.

Shadow AI is growing. Create an approved tools list and establish clear data-use expectations.

Rule 3: AI drafts. Humans decide.

Anything leaving your organization must go through human review.

Rule 4: Assume everything you type is stored.

Treat AI like the internet—assume permanence.

Rule 5: When in doubt, don't paste.

If you're unsure, pause and ask.

Used with intention and guardrails, AI can help you reclaim time without creating new risks.



Do You Safeguard Your Company's Data And Your Customers' Private Information BETTER THAN Equifax, Yahoo And Target Did?

If the answer is **"NO"** – and let's be honest, the answer *is* no – you are leaving yourself and your company open to **massive** liability, **millions** in **fines** and **lost business, lawsuits, theft** and so much more. Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – Social Security numbers, credit card numbers, birthdates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s), it's only a matter of time until they destroy your business, scare away your customers and ruin your professional and personal life.

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Our 100% FREE and 100% CONFIDENTIAL, exclusive CEO Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide your name and company e-mail address. Hopefully, it will be ALL CLEAR and you can breathe easy. But if your company, your profits and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

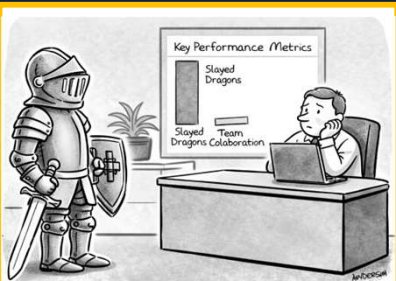
Don't let cybertheft happen to YOU!
Reserve your exclusive CEO Dark Web Scan now!

Claim Your FREE Dark Web Scan Today At
<https://www.kingoffice.com/dark-web-scan>

SCAN ME



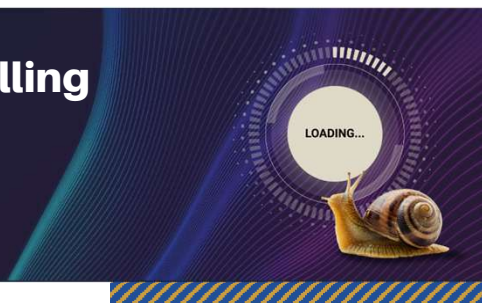
CARTOON OF THE MONTH



"Your results are impressive, but we're concerned you're not working with others enough."

The Hidden Bottleneck Killing Your Productivity

(It's Not Your People)



If you're a business owner, you've likely had this exact thought: "Why does everything take longer than it should?" It's rarely because your team is unmotivated or careless. Most delays come from hidden tech friction—those small, often invisible obstacles that slow your business down a little at a time. Over weeks and months, those delays pile up and become the difference between "we're moving" and "we're stuck." Below are three of the most common bottlenecks slowing organizations down and how to start fixing them.

Bottleneck #1: Your Apps Don't Talk to Each Other

Translation: You're running a copy-paste business.

When systems don't integrate, information gets re-entered repeatedly—into the CRM, into project software, into accounting tools, and then again into spreadsheets. Employees aren't doing this because they want to; they do it because nothing connects cleanly. Humans become the "integration layer," resulting in duplicated work, errors, inconsistencies, and delays. If even ten employees spend just a few minutes per day manually retyping data, your business loses more than 26 hours each month to avoidable busywork. Multiply that by payroll, and the cost becomes obvious.

Bottleneck #2: Slow or Unstable Networks

Translation: Death by a thousand loading screens.

A sluggish network doesn't always feel like an emergency, which is why many businesses tolerate it for far too long. Files take forever to open. Cloud apps freeze. Video calls stutter. People restart tools without thinking twice.

Each delay seems harmless on its own, but the cumulative effect destroys momentum. Nothing breaks focus faster than a spinning wheel—especially when a customer is waiting. Over time, these delays chip away at morale, making even motivated employees feel drained and frustrated.

Bottleneck #3: Approval and Access Chaos

Translation: Everyone is waiting on the one person with the password.

Work comes to a halt when employees need access, authorization, or a login they don't have. Maybe only one person can approve purchases or grant access to a shared folder—and that person is out for the day. This creates an accidental permission system that slows projects, creates single points of failure, and encourages risky workarounds that expose your business to security issues.

The 10-Minute Bottleneck Diagnostic

Ask your team three key questions:

- What is one thing you do every day that feels like a waste of time?
- Where do you get stuck waiting?
- What tool or system makes your job harder than it needs to be?

Their answers will reveal patterns—and those patterns reveal the friction.

Fixing the Bottlenecks

Integrate systems so data flows automatically. Audit and optimize networks to restore speed. Clean up access rules and use a password manager to eliminate single-person dependency. These improvements aren't flashy—they're foundational. Fix even one of these bottlenecks, and your entire team moves faster.



Solos AirGo A5 AI Smart Glasses

The Solos AirGo A5 AI Smart Glasses bring hands-free AI into your line of sight. With these smart glasses you can translate text on the fly and access contextual information while staying focused on the task in front of you.

For busy business leaders, this means fewer interruptions and faster decisions. Instead of stopping to search, information comes to you in real time. It's a small shift that adds up to time savings over a busy week.



QUICK TECH TIP

The Byte-Sized Spring Refresh!

DO an app Check:
Give your apps a quick "Do I actually use you?" check.

*If the answer is no, show them the uninstall button.

Clear out that Downloads folder you pretend doesn't exist.

*Yes, the one with 47 copies of the same PDF.

Sweep away sneaky browser extensions.

*If you don't recognize it, it doesn't get to stay.

Freshen passwords.

*Let your password manager do the heavy lifting—no more "Spring2026!"

Turn on multi-factor authentication.

*Future-you will thank you when your accounts stay locked down.

Run updates.

*Your devices deserve a little spring refresh too.





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

Data Security 101:
Protect Your Office and
Avoid Costly Breaches

PG 2

AI Tools Are Everywhere.
Here's How to Use Them Without
Making a Mess.

PG 3

The Hidden Bottleneck Killing
Your Productivity
(It's Not Your People)

Who Wants To Win A \$25 Gift Card?

TRIVIA



Which cybersecurity concept ensures
that data cannot be altered without
detection?

- A. Authenticity C. Availability
B. Confidentiality D. Integrity

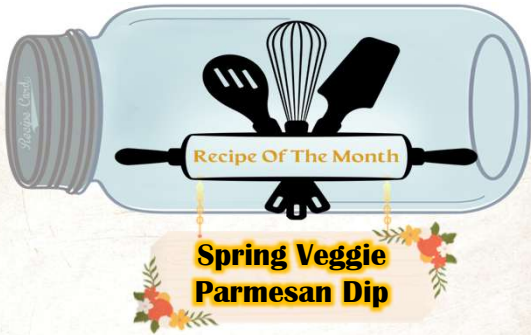
Last month's Trivia: Q : Which historic technology
milestone first occurred on February 14, 1946?

C : ENIAC, one of the earliest electronic general-purpose
computers, was unveiled

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.



Prep: 10 min
Cook: 15 mins
Yield: 2 cups)

Spring Veggie
Parmesan Dip

INGREDIENTS

- ❖ 1 cup frozen peas
- ❖ 1 cup chopped asparagus (fresh or frozen)
- ❖ 1 clove garlic, minced
- ❖ Salt & pepper to taste
- ❖ 1/2 cup grated Parmesan cheese
- ❖ 1/3 cup sour cream or Greek yogurt
- ❖ 1 tbsp lemon juice
- ❖ Olive oil (optional drizzle)

INSTRUCTIONS

- Step 1. Steam peas and asparagus until tender (about 5–7 minutes).
- Step 2. Add vegetables, garlic, Parmesan, sour cream, and lemon juice to a blender.
- Step 3. Blend until smooth and creamy.
- Step 4. Season with salt and pepper; add a drizzle of olive oil if desired.
- Step 5. Serve warm with crackers, pita chips, or sliced veggies.