

KOSI BITS & BYTES

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

June Is the Time to Get Your IT Summer-Ready

June marks the start of summer and the worst time for a technology failure. With staff vacations, lighter oversight, and heavier reliance on remote access, the gaps in your IT environment become more exposed than ever.

Our Managed Advantage IT Services keep everything running while your team enjoys the season. Proactive monitoring, automated patching, and layered cybersecurity protection mean small issues get caught before they spiral into costly downtime.

Get ahead of summer disruptions now. A quick assessment this June can lock in performance, close security gaps, and keep your business running smoothly all season long.

Get your IT summer-ready before the season heats up. Let's lock things down this June.

Scan the QR code or call us at 419-522-4001 to schedule your June checkup



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!

Your Password Is the Key Under the Doormat



Picture walking up to a house and lifting the welcome mat to find a key underneath. It's convenient, predictable and exactly where someone with bad intentions would look first. Most businesses treat their passwords the same way.

No one starts a business thinking they'll need to manage passwords for the entire organization. But at some point, it becomes part of the job, quietly growing as you add more tools, more logins and more people.

The reuse problem

A typical breach doesn't usually start within your business. It starts somewhere else entirely: a shopping site, a food delivery app, a subscription you forgot you had. That company gets breached, and suddenly your email and password are part of a database being sold on the dark web.

From there, attackers get efficient. They take that same login and try it everywhere: your email, your banking portal, your business applications, your cloud storage. One breach, one reused password and it's not just one door that's open — it's the whole building.

The most common attacks aren't sophisticated; they're automated. Software runs your stolen credentials against hundreds of sites while you're asleep. By the time you find out, the damage is already done. It's called

credential stuffing and it works because most people reuse passwords across multiple accounts.

The illusion of 'strong enough'

A lot of business owners feel covered because their password has a capital letter, a number and a symbol. That might've felt secure in 2006, but the landscape has changed since then. Modern attacks use tools that can test billions of combinations per second.

A strong password is still a single point of failure. One phishing email or one vendor breach can undo it entirely. No matter how clever the password is, it's still just one layer standing between an attacker and everything you've built.

The fix is simpler than you think

A password manager creates and stores a unique password for every account, so your team doesn't have to remember them or fall back on reusing the same easy-to-guess password.

Multi-factor authentication adds another layer, so even if a password gets exposed, access is still blocked. Neither needs an IT degree and both can be set up in an afternoon.

Good security isn't about perfect habits; it's about systems that still work when people make honest mistakes.

Don't make it easier for hackers and leave the key under the mat.

PARTNER SPOTLIGHT



Leverage Strong IT Security To Secure Better Cyber Insurance

Cyber insurers are rewarding businesses with strong IT security—often with broader coverage and lower premiums. At the same time, AI-driven scams and social engineering attacks are becoming more frequent and harder to detect, making strong insurance coverage more important than ever.

Security controls that matter to insurance companies:

- Multi-factor authentication (MFA)
- Endpoint detection & response (EDR)
- Tested backup & recovery

Pro Insurance Partners specializes in cyber insurance and works across multiple carriers to help clients turn strong IT environments into better cyber insurance outcomes.

Interested in learning more or a second look at your existing coverage?

Email: Info@ProInsPartners.com or call: 614-653-6392 to get started.

Mention KOSI for a prioritized review.

Trust, Scarcity and Second Chances

Inside Molly Bloom’s Poker Empire



Molly Bloom ran one of the world’s most exclusive high-stakes poker games, attracting billionaires and celebrities. Then she lost it all. At a recent TMT Producers Club event, Bloom shared the lessons she learned about trust, exclusivity and resilience—insights any business leader can use.

Trust is the starting point

Before launching her New York game, Bloom spent weeks listening to players. The consistent answer: trust was missing. She positioned herself as the bank, guaranteeing fairness, and her game quickly became the most sought-after in the city. For business owners, the lesson is clear—understanding what clients distrust is what creates real differentiation.

Details create the difference

Every element of Bloom’s games was intentional—venue, music, food,

personal preferences. “The details matter. They all come together to comprise the emotional imprint you leave.” Clients aren’t just evaluating outcomes; they’re evaluating the experience of working with you.

Exclusivity drives demand

With only a handful of seats, Bloom turned scarcity into demand. Instead of persuading people to join, she had them competing to get in. When you clearly define who you serve best, the conversation shifts from “why should I hire you” to “how do I get in.”

Resilience creates the comeback

After losing everything, Bloom chose to start again. “You get as many chances as you’re brave enough to take.” Success comes from the willingness to keep moving forward. Businesses that solve real problems and create meaningful experiences are the ones that endure.

The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report!

Download your free copy of this Executive Report today online at: www.kingoffice.com/cybercrime Or Scan the code



CARTOON OF THE MONTH



“I’ve changed my work environment.”



The proposal looked polished and professional. Then the client called—the market research supporting the entire recommendation didn’t exist. The AI had made it up, confidently and in detail.

It’s called hallucination: when AI produces plausible-sounding information that isn’t real. And it’s becoming a familiar issue for businesses adopting these tools without oversight.

The intern nobody onboarded

Imagine giving a new intern access to your client files, email drafts, financial summaries and internal documents on day one—no orientation, no guardrails, no check-ins. That’s how most businesses are adopting AI right now.

AI is good at drafting, summarizing and speeding up work. The issue isn’t the tool—it’s how it’s being used. Every application has AI built in now, but not every business has stopped to ask what happens when someone clicks that button.

What your unsupervised intern is really doing

When AI tools show up without a plan, three things tend to happen.

First, data gets shared in ways no one intended. Employees paste contracts and financial data into free AI tools just to work faster—and

many of those tools use that input to train their models.

Second, unapproved tools start appearing. It’s shadow IT with AI—quiet, widespread and building risk in the background.

Third, output gets trusted without being verified. AI produces clean, convincing content whether it’s accurate or not. A human intern might make a mistake once; AI can do it at scale. The risk shows up when no one reviews the output.

How to supervise your intern

The answer isn’t to ban AI. It’s to treat it like a new hire with a lot of potential and no context.

Set boundaries before people start. Decide which tools are approved. A shared list that gets updated as things change is enough—it’s about knowing what’s connected to your business.

Build in a review step. AI drafts. Humans approve. Nothing goes to a client or the public without someone reading it first.

Be clear about what not to share. Client names, contracts, financial data and employee information don’t belong in consumer AI tools. If people don’t know the line, they’ll cross it.

The goal isn’t perfect AI use. It’s a team that knows how to use it without creating unnecessary risk.

SHINY NEW GADGET OF THE MONTH

Oura Ring 4

Turn Daily Health Data Into Better Workdays

When your calendar is packed and your tasks keep growing, knowing when to push or pause becomes a competitive edge. The Oura Ring 4 tracks sleep, activity, stress and readiness, then translates that data into a daily score designed for professionals like you.

No screen clutter or wrist fatigue, just a lightweight titanium ring that works in the background, flagging recovery gaps before they become productivity problems..

QUICK TECH TIP

Your Mid-Year Access Cleanup Starts Now

June is the perfect time to audit who has access to what. Former employees, old vendors and forgotten shared accounts quietly pile up—and every one of them is a potential entry point for attackers.

Block an hour this month to review your user lists, disable inactive accounts, and confirm that multi-factor authentication is turned on everywhere it can be. Check shared mailboxes and admin roles too—these are often overlooked and over-permissioned.

One hour now can prevent months of damage later.



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

Your Password Is the Key
Under the Doormat

PG 2

Trust, Scarcity and Second Chances:
Inside Molly Bloom's Poker Empire

PG 3

Your AI Intern Just Started.
Who's Supervising It?

Who Wants To Win A \$25 Gift Card?

TRIVIA

The first iPhone launched on June 29,
2007, changing the tech world forever.
What was the starting price of the
entry-level 4GB model?

- A. \$299

B. \$399
- C. \$499

D. \$599

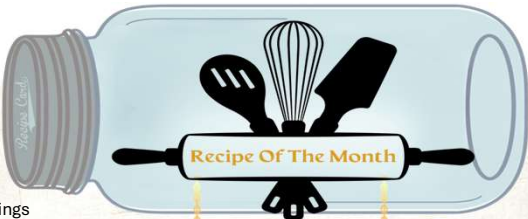
Q & A : Last Month's Trivia:

In May 1991, Tim Berners-Lee, a British computer scientist
working at CERN, set up the first web server and made the
World Wide Web publicly accessible for the first time.

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: 12 servings
Total Time: 26 min
www.allrecipes.com

Crispy Chicken
Schnitzel

INGREDIENTS

- ❖ 2 large eggs

❖ 3 Tbsp honey

❖ 3 Tbsp Dijon mustard

❖ 2 ½ Tbsp soy sauce

❖ 1 Tbsp crushed garlic

❖ 3c bread crumbs (or as needed)
- ❖ 1 tsp salt

❖ 1 tsp ground black pepper

❖ vegetable oil for frying

❖ 12 boneless chicken breast
halves, pounded very thin

❖ 1 lemon, cut into wedges

INSTRUCTIONS

- Step 1:** Whisk eggs, honey, Dijon mustard, soy sauce, and garlic
together in a bowl. Mix bread crumbs, salt, and pepper together in a
shallow bowl.
- Step 2:** Heat 1/2 to 1 inch of vegetable oil in a heavy skillet to 350
degrees F (175 degrees C). You can also use a deep fryer.
- Step 3:** Put chicken slices in the egg mixture and knead until fully
coated. Press chicken in the bread crumbs until evenly coated.
- Step 4:** Working in batches, carefully place chicken in the hot oil using
tongs and cook until no longer pink in the center and browned on the
outside, 3 to 4 minutes per side. Drain on paper towels and serve with
lemon wedges.