TECHNOLOGY TIMES

JUNE 2026

Insider Tips to Make Your Business Run Faster, Easier and More Profitably

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 have been 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.

Contact techsupport@canoncapital.com and ask about our Password Manager option.

HALIFAXTEC

TRUST, SCARCITY AND SECOND CHANCES

Inside Molly Bloom's Poker Empire

Sometimes, rebuilding trust, creating exclusivity and earning a second chance comes down to a few well-timed risks. Molly Bloom, the woman behind one of the world's most exclusive poker games, knows that better than most. She recently shared her lessons with us, offering insights that leaders can apply to their own businesses.

Bloom built and ran one of the most exclusive high-stakes poker games in the world, attracting billionaires and A-list celebrities. At her peak, she was making millions, with powerful players competing for a seat at her table. Then it collapsed. Bloom lost everything. In the years that followed, she rebuilt her life, wrote a memoir and saw her story adapted into an Oscar-nominated film.

"I see a room full of entrepreneurs," she said. "People who want to make their life work, who want to take care of people they love and who want to be proud at the end of the day."

Her story offers a practical lens on how businesses differentiate, build trust and recover when things go wrong.

Trust is the starting point

When Bloom arrived in New York, she didn't begin by promoting a new game. Instead, she spent weeks speaking with players, asking about their experiences.

The answer was consistent: trust was missing. "That's when I knew that was my disruption." Bloom positioned herself as the bank to ensure fairness and transparency. Within months, her game became one of the most sought-after in the city.

For business owners, the takeaway is straightforward. Leading with services isn't enough. Understanding what clients distrust, fear or feel underserved by is what creates meaningful differentiation.

Experience shapes decisions

Bloom began focusing less on outcomes and more on experience, paying attention to how players felt in her games. That shift changed how people responded to her.

In business settings, particularly in sales conversations, this translates directly. Decisions are influenced not just by logic but by whether clients feel understood, respected and at ease.

Details create the difference

Bloom treated details as core to the experience, not as an afterthought. From venue selection to music, food and personal preferences, each element was intentional. "The details matter. They all come together to comprise the emotional imprint you leave."

For other business leaders, those details show up in everyday interactions, from proposals to service delivery. Clients aren't just evaluating outcomes. They're evaluating the experience of working with you.

Exclusivity drives demand

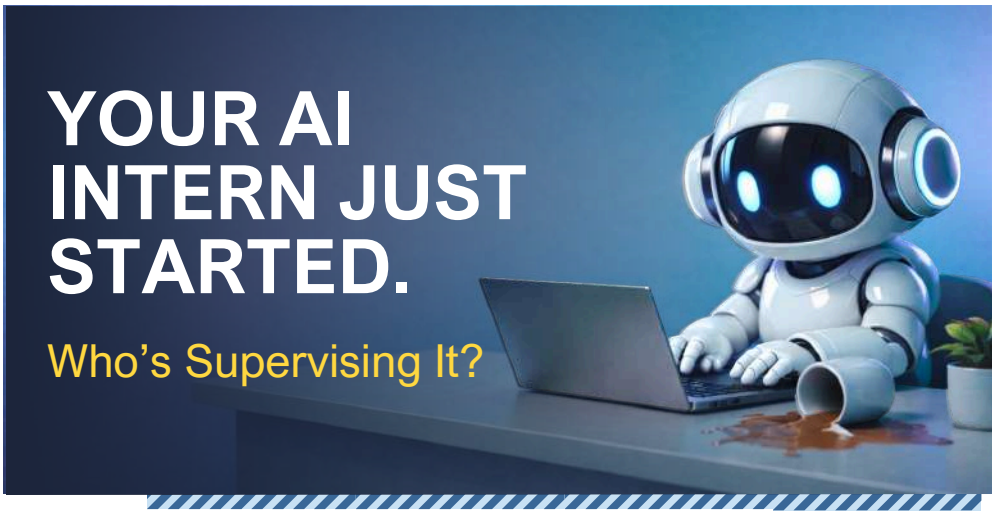
Bloom's games were limited by design. With only a handful of seats available, she created an environment where access felt exclusive. "I don't always have a seat," she'd say. "But hit me up."

That scarcity shifted the dynamic. Instead of persuading people to join, she created demand. When you define who you work best with and where you deliver value, the conversation changes from "why should I hire you" to "how do I get in."

Resilience creates the comeback

After losing everything, Bloom faced a decision: stop or start again. She chose to continue. "I know now, you get as many chances as you're brave enough to take."

This lesson is less about poker and more about resilience. Success doesn't come from a single opportunity. It comes from the willingness to keep moving forward, even after setbacks. Bloom's story reinforces a simple idea. Businesses that solve real problems and create meaningful experiences are the ones that endure.



The proposal looked great. It was polished, professional and exactly the kind of document that signals control.

Then the client called. The market research in section two, the data supporting the entire recommendation, didn't exist. The AI had made it up. Not vaguely, not accidentally, but confidently and in detail.

There's a term for this: hallucination.

It happens when AI produces information that sounds plausible but isn't real. And it's becoming a familiar issue for businesses adopting these tools without clear oversight.

The intern nobody onboarded

Imagine hiring an intern and on day one handing them access to everything. Your client files. Your email drafts. Your financial summaries. Your internal documents.

"Just figure it out. Let me know if you need anything." No orientation. No guardrails. No check-ins. That's how most businesses are adopting AI right now.

Not because they're careless. In fact, it's the opposite.

AI tools are useful, easy to access and already built into the software people use every day. There's an AI button in your email, another in your document editor and one in your project management tool. It feels like help has arrived. And in many ways, it has.

AI is good at drafting, summarizing, organizing information and speeding up work that used to take hours. It reduces friction and helps teams move faster. The issue isn't the tool. It's how it's being used.

Every application seems to have AI built in now. 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 client contracts into free AI tools to get a quick summary. They drop financial data into a chatbot to format a report.

It happens more often than most businesses realize, usually without anyone flagging it. The intent isn't careless. People are just trying to get their work done faster.

...continued on page 4

FREE REPORT

CARTOON OF THE MONTH

"I've changed my work environment."

...continued from page 3

Many consumer AI tools use that input to improve their models. That means your business data may not stay private.

Second, tools nobody approved start appearing. Employees start using whatever works best for them, often without checking if it's been vetted.

IT has no visibility into what's being used, what those tools can access or what their terms say about ownership and privacy.

It's shadow IT, just with AI. Quiet, widespread and building risk in the background.

Third, output gets trusted without being verified. AI is remarkably confident in how it presents information. It doesn't pause or flag uncertainty. It produces clean, convincing content whether it's accurate or not.

The proposal with invented statistics looked just as credible as one based on real data.

A human intern might make that mistake once. AI can do it repeatedly and at scale. That's not a flaw. It's how the tool works. The risk shows up when no one reviews the output.

AI doesn't fix broken processes. It accelerates them. A disorganized business with AI just moves in the wrong direction faster.

How to supervise your intern

The answer isn't to ban AI. That's not realistic and it puts you at a disadvantage compared to businesses that are learning how to use it effectively.

The answer is 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 and which aren't. Keep it simple. A shared list that gets updated as things change is enough. This isn't about adding red tape. It's about knowing what's connected to your business.

Build in a review step.
AI drafts. Humans approve. Nothing should go to a client, vendor or the public without someone reading it first. It sounds obvious, but it's where things tend to slip.

Be clear about what not to share.
Client names, contract details, financial data, employee information. None of that belongs in a consumer AI tool. If people don't know where the line is, they'll cross it without realizing it.

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