

TECH CHRONICLE



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.

Don't make it easier for hackers by leaving the key under the mat.

Is Your Business AI Ready?
See back of newsletter to take the
AI Readiness Self-Assessment



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.

Your Kid's Gaming Rig Could Survive a Cyberattack.

CAN YOUR OFFICE?



Remember blowing into Nintendo cartridges to make them work? Once upon a time, that was our version of IT support.

Cartridge wouldn't load? Blow on it.
Still wouldn't load? Blow harder.

If that failed, you smacked the console and hoped for the best.

We thought we were pretty good at technology.

But your kid has never had to fix anything by hitting it. Their setup is a finely tuned machine: solid-state drive, 32 gigs of RAM, a processor powerful enough to render a short film, mesh Wi-Fi with no dead zones, real-time performance monitoring and multi-factor authentication on every account.

It's optimized, tuned and maintained.

Now think about your office. There's a workstation from 2019 that takes four minutes to boot, a printer that jams every Tuesday, shared folders named "New New Final FINAL" and software that doesn't talk to each other. Then there's the Wi-Fi that mysteriously dies in the conference room and the laptop with a "Restart to update" notification that's been dismissed every morning for three weeks.

Gamers optimize. Businesses tolerate.
That gap is more expensive than most people realize.

Why Gamers Win This Comparison

It's not about budget. A solid gaming PC costs about the same as a business workstation. Business internet is often faster than residential. The tools to monitor and secure a network aren't out of reach.

The difference is attention.

Gamers update everything immediately: operating systems, drivers, firmware, patches. Outdated software means lag, and lag means losing. Meanwhile, every postponed update on your office laptops represents a known vulnerability with a fix that hasn't been installed.

Gamers back up their progress religiously. Lose a 200-hour save once and you never forget. Many businesses, however, don't regularly verify that backups are running properly. When a gamer loses data, it's frustration. When a business loses data, it's client records, financial history and possibly the ability to operate.

Gamers also monitor performance in real time. CPU temperature. Network speed. System load. They notice a small dip and investigate before it turns into a crash. Most businesses discover issues when someone says, "The internet's slow today." That's not monitoring. That's reacting.

Your kid would never run their setup that way. And their setup isn't responsible for payroll.

How this happens

No one designs a messy office network on purpose.

Business technology grows gradually. A tool gets added to solve a problem. Another platform comes in for accounting. Then CRM. Then file sharing. Then payroll. Then security layered on top.

Each decision makes sense in the moment. Over time, though, technology stops being designed and starts being accumulated. Accumulation creates friction.

Gaming rigs are built intentionally for performance. Business systems often evolve for convenience. One is strategic. The other is incremental. And incremental systems eventually become expensive systems.

Back when we were blowing on cartridges, we didn't know better. Today, the tools and knowledge exist. The question isn't whether improvement is possible. It's whether anyone is actively paying attention.

...continued on page 4

CARTOON OF THE MONTH



"I've changed my work environment."

The Cost Nobody Calculates

The biggest cost rarely shows up as a dramatic outage. It appears in small, daily inefficiencies everyone has learned to accept.

It's the five minutes waiting for a slow login. Searching for a misplaced file. Re-entering data into systems that don't sync. Restarting the same machine twice a week. Creating workarounds because "that's just how it works here."

Individually, those interruptions feel minor, but that five-minute glitch often costs far more than five minutes. It can take over 20 minutes to fully regain focus after being disrupted. Multiply that across your team, week after week. What feels normal becomes expensive.

In gaming, lag is unacceptable. In business, lag becomes routine. And routine inefficiency quietly drains productivity.

The Better Question

When asked about their technology, most business owners say, "It works fine." But working and working efficiently aren't the same thing.

Ask yourself the following: Are your tools integrated or simply coexisting? Are your systems streamlined or stacked on top of one another? Are your processes supported by technology or constantly working around it? Is anyone watching your network proactively, before something fails?

Hardware will always evolve. What drives real productivity today is integration, automation, security and thoughtful system design.

None of that improves by accident.

SHINY NEW GADGET OF THE MONTH

Dell UltraSharp 52" 6K USB-C Display

Named a standout in Windows Central's Best of CES 2026, this 52" 6K display is built for users who live in multiple windows.

Run dashboards, remote sessions, ticket queues and documentation side by side without constant tab switching.



A single USB C Cable delivers power, video and data, keeping your desk clean. If you're building a true command center, this is the screen that anchors it.

2 Free Hours A \$550 VALUE

2 Free Hours of IT Support To
Diagnose Any IT Problem You
Have.

Wondering What You Can Do With 2 Free Hours of IT Support?

- Speed Up Computers to Run Efficiently
- Set Up Security & Monitoring on Remote Computers
- Configure Multiple Emails on Outlook
- Dark Web Scan & Monitoring to Protect Your Data
- Dual Monitor Setup to Maximize Productivity
- Share Printers on Multiple Computers
- **DIDN'T SEE WHAT YOU'RE AFTER? JUST ASK!**



**SCAN HERE
For 2 Free Hrs
of IT Support**

