TECHNOLOGY TIMES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY SINCE 2003

June 2025

From Defense to Risk:

How MFA Became a New Vulnerability

In today's digital landscape, multi-factor authentication (MFA) is widely recognized as one of the most effective ways to secure business accounts. But cybercriminals are catching on. A growing threat known as "MFA fatigue attacks" is turning this powerful security measure into a new point of vulnerability. If your business relies on push notifications to verify logins, you could be more exposed than you think.

What is an MFA Fatigue Attack?

MFA fatigue attacks, also known as MFA bombing, occur when a cybercriminal repeatedly sends login verification requests to an employee's phone, hoping the person will eventually approve one out of annoyance, confusion, or habit. These attacks are particularly effective against organizations that use push-based MFA apps like Microsoft Authenticator or Duo.

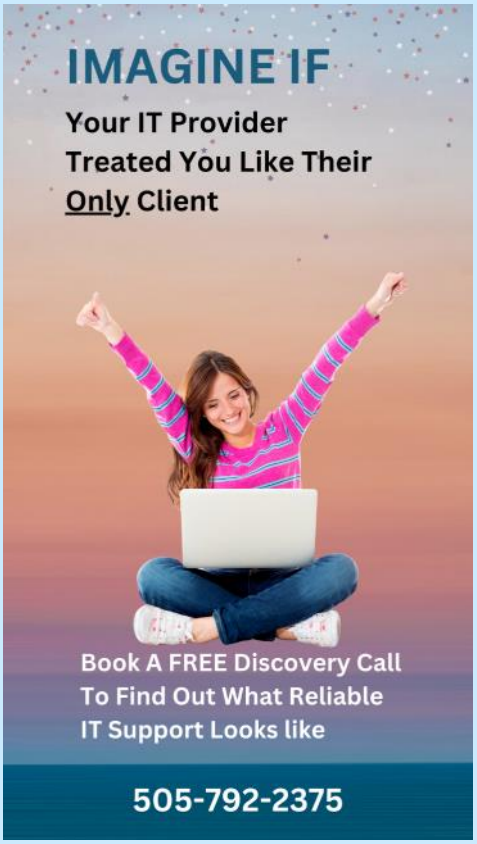
Attackers often gain the user's login credentials through phishing or the dark web. Once they have the correct username and password, they trigger a flood of MFA prompts in quick succession, sometimes even in the middle of the night. The goal? Wear down the victim until they hit "approve" just to make it stop.

Why Small Businesses Are Especially Vulnerable

Small businesses often lack the layered security infrastructure of larger enterprises. MFA is a great first step, but if it's implemented without additional safeguards or employee training, it can backfire. Employees at small companies may not have had cybersecurity training and are more likely to approve a prompt out of habit, especially when they're juggling multiple roles and responsibilities.

Additionally, many small businesses rely on default MFA configurations that prioritize ease of use over security. Push-based authentication is fast and convenient, but without controls like number matching or time restrictions, it's easier for attackers to exploit.

Continued on pg.2



CELEBRATING 22 YEARS ANNIVERSARY

This monthly publication provided courtesy of David Luft, CEO of LDD Consulting, Inc.

Our Mission:

We promise to provide knowledgeable, courteous and prompt service. We care as much about your business as you do. If you are not completely satisfied, be sure to let us know. If we cannot resolve the issue, we will refund your money.

... continued from cover

Real-World Consequences

MFA fatigue attacks have already led to breaches at major companies, including Uber and Cisco. In both cases, attackers were able to gain internal access after tricking employees into approving login requests. For a small business, even a minor breach can be catastrophic—leading to data loss, financial theft, reputational damage, or regulatory fines.

Imagine a scenario where an employee unknowingly approves a malicious MFA request. The attacker gains access to your cloud storage, email system, or financial software. From there, they could exfiltrate sensitive customer data, impersonate executives to request wire transfers, or lock you out of your own systems until a ransom is paid.

> **"Security tools are only as strong as the strategies behind them."**

How to Strengthen Your MFA Strategy

The good news? There are several simple, effective ways to reduce the risk of MFA fatigue attacks:

1. **Enable Number Matching or Verified Push Prompts:** With number matching, users must enter a code displayed on their login screen into their MFA app. This ensures they are intentionally approving the request.
2. **Limit MFA Prompts Per User:** Configure your system to allow only a certain number of MFA attempts in a given period. This prevents attackers from spamming requests.
3. **Disable Push Notifications for High-Value Accounts:** Use more secure MFA methods for sensitive accounts, such as hardware tokens or biometrics.
4. **Educate Your Team:** Regularly remind employees that they should never approve an MFA request unless they initiated the login. Include MFA fatigue scenarios in your security training.
5. **Monitor for Unusual Login Activity:** Set up alerts for multiple failed logins or MFA attempts from unfamiliar locations or devices.

When to Reassess Your MFA Tools

If you're currently using a basic MFA solution that doesn't support number matching or contextual awareness, it might be time to upgrade. Many modern MFA platforms now offer adaptive authentication, which adjusts security requirements based on risk factors like location, device, or time of day.

For example, if a login attempt comes from an unfamiliar device or location, the system might require a second factor beyond the standard push notification. These types of intelligent systems make MFA harder for attackers to exploit.

Final Thoughts

MFA remains a critical layer of defense against cyber threats—but like any security tool, it needs to be used wisely and kept current. As attacker tactics evolve, small businesses must stay informed and proactive.

If you haven't reviewed your MFA setup recently, now is the time. Talk to your IT provider about number matching, monitoring unusual activity, and refreshing employee training.

Convenience should never come at the cost of security. One quick tap might seem harmless—until it opens the door to your entire network.

WHAT WE LEARNED FROM BARBARA CORCORAN

At a recent business event, we had the chance to meet and hear from Barbara Corcoran. She spoke candidly about being underestimated, being told she'd never make it, and using that doubt as fuel. Her advice to entrepreneurs was clear: *"Bet on yourself—especially when others won't."* It's a message that hit home for us.

Before she was a star investor on *Shark Tank*, Corcoran was a diner waitress with a dream and a $1,000 loan. That modest investment—and a lot of grit—launched The Corcoran Group, one of NYC's most successful real estate firms. But the path wasn't easy. Early on, her boyfriend and business partner ended their relationship and told her she'd never succeed without him. Instead of folding, she used his doubt as motivation.

Corcoran once said, "The difference between successful people and others is how long they spend feeling sorry for themselves." For small business owners facing rejection, her story is a strong reminder: your response matters more than the setback.

Failure Is Just the First Draft

Corcoran failed at over 20 jobs before she found her lane. She struggled with dyslexia and barely passed high school. But she used her background as a strength, becoming a personal branding expert—turning listings into headlines and herself into a go-to name in real estate.

"You don't have to get it right," she says. "You just have to get it going." That mindset helped her outpace better-funded competitors. It's a valuable approach for any entrepreneur: move fast, stay flexible, and make the most of limited resources.

Rejection Can Be Fuel

Corcoran's defining moment didn't come from success, but from betrayal. After her ex said she'd fail, she lit a fire that never went out. She didn't let his words become her reality.

Her advice? Don't take rejection personally—use it. Whether it's a lost client or a silent pitch, keep moving.

Stand Out by Being Real

Before social media influencers, Corcoran knew how to stand out. She used storytelling and humor to make her listings—and herself—memorable. Her printed newsletter became must-read material in NYC real estate.

That's a valuable insight: your story is your unfair advantage. People want to do business with someone real—not just a logo.

Lessons for Today's Entrepreneurs

Barbara Corcoran's story is more than a bootstrapper's fairytale. It's a blueprint for resilience and resourcefulness. Here are three takeaways for small business owners:

- ✓ **Bet on yourself—especially when others won't.** Self-belief is the first domino in any success story.
- ✓ **Use your story to stand out.** Don't try to sound like everyone else. Show people who you are and what you value.
- ✓ **Take imperfect action.** You can always tweak and improve—but you have to start.

As Corcoran says, "Don't you dare underestimate the power of your own instinct." That advice, especially in uncertain times, may be exactly what small business owners need to hear.

Client Spotlight

LDD's Support is Reliable & Personal

The biggest benefit of working with LDD is their truly personal approach. They respond quickly—day, night, even holidays—and resolve issues fast. If there's ever a concern, it's addressed without delay. If you're considering LDD as your IT provider, I recommend giving David Luft a call. He'll take the time to understand your needs and provide an honest, straightforward recommendation. It's rare to find an IT team this responsive, knowledgeable, and committed to their clients.

Teresa Montano
Practice Manager
Albuquerque Nephrology Associates

Albuquerque Nephrology Associates

Quick Little Bytes

Microsoft Copilot Now Recaps Meetings for You

Wish you could skip a meeting and still get the gist? Microsoft's AI tool, Copilot, is rolling out in Teams with a new feature that summarizes meetings—whether you attended or not. It pulls key points, decisions, and action items into one tidy recap. Less time in meetings, more time getting things done.

Getting Tracked at Airports? Here's One Setting to Check

Even with Bluetooth "off," your phone may still scan for nearby devices—especially in places like airports and shopping centers. That opens the door to unwanted tracking. Want to lock it down? Head to your phone's settings > Location > Location Services > System Services and turn off "Bluetooth Scanning." One tweak, more privacy.

Making Technology Work for You
2420 Midtown PL NE, Suite K
Albuquerque, NM 87107

PRST STD
US POSTAGE
PAID
ABQ, NM
PERMIT 1187

Return Service Requested

Inside This Issue

«Name»
«Company Name»
«Street Address 1», «Street Address 2»
«City», «State» «Postal Code»

SUN, SAND, & SCAMS: AVOID SUMMER CYBER TRAPS

Vacation season is prime time for cybercriminals. With just a few precautions, you can enjoy your time off without falling into a tech trap.

Don't Get Burned Booking

Watch out for fake websites offering too-good-to-be-true deals on flights, hotels, or vacation rentals. Stick to well-known platforms and double-check URLs—scammers often spoof popular sites with subtle spelling changes. Look for "https" and browse verified reviews before you book. When in doubt, book directly with the airline or hotel instead of clicking email links or pop-up ads.

Be Smart About Free Wi-Fi

It's tempting to hop on free Wi-Fi at the airport, hotel, or beach café, but unsecured networks can leave your data wide open. Avoid checking bank accounts, email, or any sensitive apps unless you're using a VPN. If possible, use your phone's hotspot instead—it's a safer option that's often faster, too.

Oversharing Can Invite Trouble

Posting your travel plans in real time can signal to would-be thieves that your home is empty. Save the vacation selfies and location tags for when you're back—your photos will still shine, and so will your security. If you have smart home cameras or alarms, make sure they're armed and set to send alerts.

Bonus Tip: Check Your Settings

Before leaving, disable auto-connect on your devices to prevent them from joining unfamiliar networks without your knowledge. And make sure all software updates are installed—patches often include critical security fixes.

With just a few simple steps, you can keep your summer focused on fun, not fraud.