## **Entra Backup Campaign-in-a-Box Social Media Posts**

## **📣 Social Media Strategy: Build Awareness. Spark Conversations. Drive Action.**

These posts are written for your clients—not tech experts. They don’t need to understand what "Entra ID" is. What they *do* need to know is that **their login systems, email access, and day-to-day operations depend on something Microsoft doesn’t fully protect.**

That’s where you come in.

Each post below is designed to help you start simple, impactful conversations about **what could go wrong if that system breaks**—and how you’re already thinking ahead to protect them.

Just copy, paste, and share on LinkedIn, Facebook, or Twitter. Every post ends with a call to action that invites clients to schedule a quick chat about their security setup.

Let’s help them see the risk—**before** it becomes a reality.

### **✅ Post 1: Accidental Lockouts**

**🔷 LinkedIn Version:**  
 One small mistake can cause a major business disruption.

If the wrong setting or user is deleted, your team could lose access to email, calendars, and files—instantly. Microsoft doesn’t fully protect the system behind those logins.

We do.

Let’s set up a quick call to make sure your business isn’t one click away from downtime.

[Link]

**🐦 Twitter Version:**  
 One wrong click could lock your team out of email and files.  
 Microsoft can’t fix that.  
 We can.  
 **Book a quick call—let’s protect your business.**  
 [Link]

### **✅ Post 2: Ransomware & Hackers**

**🔷 LinkedIn Version:**  
 Hackers aren’t just after your data—they’re going after your logins.

If someone gets in and changes your access settings, it could shut down your entire business. And unfortunately, Microsoft doesn’t offer an easy way to undo that.

That’s why we back up what others don’t. Let’s review your protection plan—schedule a call today.

[Link]

**🐦 Twitter Version:**  
 Hackers can lock you out of your own business.  
 Microsoft doesn’t cover that.  
 We do.  
 **Let’s talk about your protection.**  
 [Link]

### **✅ Post 3: Business Stops Without Access**

**🔷 LinkedIn Version:**  
 Your business depends on your team having access—email, documents, logins.

If something goes wrong behind the scenes, everything can come to a halt. No email. No files. No way in.

We protect that layer most businesses forget. Let’s chat and make sure your business stays online, no matter what.

[Link]

**🐦 Twitter Version:**  
 No logins = no work.  
 We protect the behind-the-scenes systems your business depends on.  
 **Let’s make sure you’re covered.**  
 [Link]

### **✅ Post 4: Microsoft Doesn’t Back This Up**

**🔷 LinkedIn Version:**  
 Here’s something most businesses don’t realize: Microsoft doesn’t fully back up the system that manages your logins and access.

If something is deleted or changed, it’s often gone for good after 30 days.

That’s why we step in. We protect what Microsoft doesn’t—so you’re never stuck. Book a quick call today to talk security.

[Link]

**🐦 Twitter Version:**  
 Microsoft doesn’t fully back up your access settings.  
 After 30 days, they’re gone.  
 We make sure you’re protected.  
 **Let’s talk.**  
 [Link]

### **✅ Post 5: Stay Compliant**

**🔷 LinkedIn Version:**  
 If your business needs to follow strict compliance rules, here’s a blind spot you may not know about:  
 The system that controls your employee access? Microsoft doesn’t back it up.

That can be a problem for audits and recovery. We help fill the gap—schedule a call and we’ll walk you through it.

[Link]

**🐦 Twitter Version:**  
 Following compliance rules?  
 Microsoft doesn’t protect the system behind your logins.  
 We do.  
 **Let’s talk recovery and peace of mind.**  
 [Link]

### **✅ Post 6: Trusted Partner Message**

**🔷 LinkedIn Version:**  
 You don’t have to understand every part of your IT system. That’s our job.

We stay on top of the hidden risks—like the system behind your logins that Microsoft doesn’t fully protect—and we make sure your business stays running, no matter what.

Let’s set up a short call to review your security coverage.

[Link]

**🐦 Twitter Version:**  
 You don’t have to think about every IT risk.  
 That’s our job.  
 We protect what others miss.  
 **Book a quick call today.**  
 [Link]

## **💡 Using AI to Create More Social Posts**

Want to post more often or tailor your tone? AI tools like **ChatGPT** or **Microsoft Copilot** can help you quickly draft additional posts based on your **audience, brand voice, or industry focus**.

Here are a few ways to use AI to scale your social strategy:

* **Remix existing posts**: Ask AI to reword a post to match a more professional, casual, or humorous tone.
* **Tailor by industry**: Generate new posts for specific sectors (e.g., legal, healthcare, nonprofits) by prompting AI with:  
   *“Write a LinkedIn post about the risks of not backing up Microsoft logins and user access for a healthcare provider.”*
* **Create variations for different platforms**: Shorten for Twitter, expand for LinkedIn, or repurpose as a blog intro or newsletter snippet.
* **Highlight your unique services**: Include your MSP’s value props in the prompt, like white-glove onboarding, local support, or 24/7 monitoring.
* **Incorporate customer stories or testimonials**: Prompt AI to weave in success stories, e.g.:  
   *“Write a LinkedIn post about how we helped a client recover from an access lockout using backup protection.”*

🛠️ **Pro Tip**: Start with this prompt in ChatGPT or Copilot:

*“Generate a LinkedIn post for an MSP targeting SMB clients, focused on why protecting login and access settings is critical to preventing downtime. Include a CTA to schedule a call.”*

Let AI do the heavy lifting—just **review and personalize** to reflect what makes *your* MSP stand out.