Subject: **“Restart Required” – Why That Update Could Save You Thousands**

It’s a non-stop day at work and then it hits—**“Restart Required.”**

We’ve all been tempted to click “Remind me later.” But here’s why those updates matter: **outdated software is one of the easiest ways for hackers to break into your network.**

Take one small business that delayed a security patch for just two weeks. That “later” turned into a **$55,000 ransomware attack.**

Software updates aren’t just about features—they’re about protecting your data, your clients, and your bottom line.

At **[MSP Name]**, we help businesses like yours manage updates seamlessly while following **The Simple 7 Rules of Cybersecurity** to stay secure and productive.

Let’s connect to review how we can reduce downtime while we keep your systems safe.

Talk soon,

 **[Your Name]** **[MSP Name]
 [Website] | [Phone Number]**

Subject: **“Password123” Won’t Protect Your Business**

We know managing passwords isn’t fun—but ignoring them will cost you.

 **77% of hacking-related breaches start with stolen or compromised credentials.**

When you reuse the same weak password across accounts, you’re giving cybercriminals an easy way in. Once a hacker gets access to one system, they can access even more.

That’s why at **[MSP Name],** we provide two simple tools for our clients:

* A **password manager** to generate and store strong, unique passwords
* **Multi-factor authentication (MFA)** to add a second layer of protection

These tools help us follow **The Simple 7 Rules of Cybersecurity**—protecting your business from preventable breaches while keeping your team productive and moving forward.

Want to make password management simple and secure for your business?
We can help.

Let’s connect soon,

 **[Your Name]
 [MSP Name]
 [Website] | [Phone Number]**

**Subject: Don’t hand out your master keys**

“Ugh, I need admin access to update QuickBooks, and now I have to wait on IT just to do my job?”

We get it. Waiting on permissions is frustrating. But giving every employee admin access is like handing out the master key to your entire network—and that opens the door to serious security risks.

At **[MSP Name]**, we strike the balance.
 You shouldn’t have admin rights, but you also shouldn’t be stuck waiting on us. That’s why we use tools that grant trusted users the access they need to update approved applications. No tickets, no delays.

It’s all part of how we follow **The Simple 7 Rules of Cybersecurity**—keeping your business protected from preventable threats without slowing your team down.

Fewer risks. Less downtime. Zero hassle.

**Ready to secure your systems and keep your workflow moving? Let’s talk.**

Looking forward to connecting,

 **[Your Name]
 [MSP Name]
 [Website] | [Phone Number]**

**Subject: That download just opened the door to a data breach**

That video editing tool your teammate just downloaded?

It just cost your business thousands.

We get it—restrictions around software installs can be frustrating. You find a tool that looks helpful and think, Why not just download it? But even well-meaning installs can open the door to malware, data theft, or serious downtime.

At **[MSP Name**], we make sure your team has secure access to the tools they need—without putting your systems at risk.

Need to download a new tool? Talk to us first so we can make sure you’re protected.

It’s all part of how we follow **The Simple 7 Rules of Cybersecurity**—practical steps we take to keep your business secure and your team moving forward.

Let’s talk about keeping productivity up and risks down.

Talk soon,

 **[Your Name]
 [MSP Name]
 [Website] | [Phone Number]**

**Subject: Is a chicken sandwich worth a data breach?**

Hi [First Name],

A school district in Georgia tested staff with a fake phishing email offering a free Chick-fil-A sandwich.

The catch? The link led to **chik-fil-a.com**—a fake site, just one letter off. Had it been real, hackers could’ve accessed sensitive data… all for the promise of lunch.

At [MSP Name], we help prevent attacks like this by following **The Simple 7 Rules of Cybersecurity: Shield Your Network.**

We use DNS filtering and other layered defenses to block access to malicious websites before they can load—stopping phishing attempts in their tracks.

Hackers count on human error. We make sure one wrong click doesn’t turn into a crisis.

**Let’s talk about locking down your network.**

Talk soon,

 **[Your Name]
 [MSP Name]
 [Website] | [Phone Number]**

**Subject: “I can spot a scam email.” …Can you really?**

Hi [First Name],

“Why do we need security training? I can spot a scam email.”

We hear that a lot. But here’s the truth; **human error is still one of the top causes of data breaches.** Even the most tech-savvy team member can be tricked by a convincing phishing email, fake login page, or spoofed phone call.

That is why at [MSP Name], we abide by **The Simple 7 Rules of Cybersecurity,** which means that we keep you cyber-smart with ongoing Cybersecurity training.

We provide the tools to protect your business, but **technology alone isn’t enough.** Security training helps your team spot the signs before it’s too late.

Think of cybersecurity training like a fire drill. You hope you never need it, but if something happens, you’ll be glad your team knows exactly what to do.

Let’s make sure your people are just as strong as your tools.

**Let’s connect soon,**

 **[Your Name]
 [MSP Name]
 [Website] | [Phone Number]**

Subject:

Imagine walking into work and finding all your customer records, financial data, and business files wiped out.

It happens more than you think—from ransomware attacks to accidental deletions. **60% of small businesses that suffer major data loss shut down within six months.**

That’s why at **[MSP Name]**, we follow **The Simple 7 Rules of Cybersecurity**, ensuring your business data is backed up and protected.

Backups are your safety net. Whether it’s a cyberattack or a simple mistake, we make sure your data is restorable—and never gone for good.

**The real question isn’t if something will go wrong—it’s how prepared your business will be when it does.**

Let’s connect and see how we can keep your business protected,

 **[Your Name]
 [MSP Name]
 [Website] | [Phone Number]**