**SLIDE ONE**: Welcome to our lunch and learn on the simple 7; Essential cybersecurity rules [MSP Name] applies, and you should understand.

**SLIDE TWO**: Cybersecurity isn’t just about protection — it’s about helping your business thrive with minimal disruptions to your time and bottom line.

At [MSP name], we’re more than just IT support. We’re your partner in building a smarter, more secure, and more profitable future for your team.

To keep you protected, we follow a set of core principles we call the Simple 7 — clear, actionable rules that strengthen your defenses and support long-term success.

Let’s walk through what they are, why they matter, and how we put them to work for you.

### **SLIDE THREE: Rule Number One, Maintain Regular Updates**

**SLIDE FOUR:** Skipping software updates is like leaving your front door unlocked overnight.

**SLIDE FIVE: What are software updates exactly?**These are changes to your computer or apps that fix bugs, give access to newer features, and most importantly - cover up security holes. They can sometimes require a quick restart and may look like a harmless pop-up — but they’re your first line of defense.

**Why are these important?**Cybercriminals specifically target known vulnerabilities in outdated software. When you delay updates, you’re inviting them in

Take the case of a small marketing agency. They delayed a critical Windows security update for over two weeks. Hackers used this vulnerability to access their network, hide important files, and demand ransom to return them. The firm ended up paying $37,000 to recover their data and lost another $18,000 in productivity due to downtime. They lost $55,000 all because of a missed update.

**So how can we help and prevent a situation like this for your business?**

We automate updates so you don’t have to worry about them. If we prompt you to restart — just do it! That quick reboot is locking up your digital doors and potentially preventing a major loss in time and money.

**SLIDE SIX: Rule number 2, Protect Logins**

**SLIDE SEVEN:** When your logins aren’t secure, it’s like locking your front door but leaving a window wide open!

**SLIDE EIGHT:** Protecting your logins means making sure only the right people, you and your team, can access your accounts. It means keeping out cybercriminals who try to sneak in using weak or stolen passwords.

**Why does this matter?**

One vulnerable account can be all it takes to bring down an entire business.

Take the case of a150-year-old logistics company in the UK that had to shut down permanently after hackers guessed an employee’s weak password. Over 700 people lost their jobs — because of one bad password.

So yes, creating complex, unique passwords is essential. But let’s be honest — no one has time to remember 50 different, 30-character passwords.

The good news is that there are tools your team can utilize that make login protection easier and stronger.

Multi-Factor Authentication (MFA) requires a second device to confirm your identity — like entering a code sent to your phone or approving a login through an app.

Password managers create, store, and manage strong passwords for you — and let you securely share them with coworkers (no sticky notes or “just text me the login”).

So how can we help protect your logins?

We set up MFA and a secure, business-wide password manager for your team, so you don’t have to rely on memory or risky habits. We also educate to make sure everyone on your team understands best practices — because password123 isn’t going to cut it.

### **SLIDE NINE: Rule Number Three, Manage Access**

**SLIDE TEN:** Giving too many people admin access is like handing out the master key to your entire building. If just one of those keys gets stolen, attackers can go anywhere they want.

**SLIDE ELEVEN:**

**What are Admin Accounts?**

Admin accounts have the power to change settings, install software, and access everything on a system. Have you ever tried changing the time on your work device and been denied? That’s because you don’t have admin access- and no one on your team should either.

Removing admin privileges from employees is one of the smartest ways to prevent cyberattacks- it adds an extra layer of protection and significantly reduces your risk of a breach.

**Why is this important?**

Take for example a small accounting firm with just 20 employees- they suffered a ransomware attack after a staff member with an admin account clicked on a link sent from a hacker to a malicious site. The hacker gained access to that employee’s admin account and installed malware that allowed them to steal the firm’s client records.The business lost over $62,000 between ransom negotiations, downtime, and emergency IT services- plus two weeks of disrupted client work during tax season.

All of it started with one admin account.

**So how can we help and prevent an admin account breach?**

We remove local admin access from your users and keep it secured within our team. When elevated access is needed, we implement tools that allow us to grant it temporarily — with strict controls and tracking.

For example, if QuickBooks needs an update, you won’t have to call us every time. Just send a request, and we can securely approve it in seconds. This keeps your exposure low, your team moving without unnecessary delays, and most importantly- keeps your business secure.

### **SLIDE TWELVE: Rule Number Four, Approve Software**

**SLIDE THIRTEEN:** Downloading unapproved or unknown apps is like opening your front door and inviting a hacker in.

**SLIDE FOURTEEN:** We verify certain software tools for a reason — not to be picky, but to protect your business. Every app your team installs should be vetted, because it only takes one bad download to create a serious security risk.

**Why is this important?**

Even tools that may seem trustworthy can carry hidden malware if they’re downloaded from the wrong place.

For example, in 2023, a Disney employee downloaded a free AI tool, assuming it was safe. But the tool was secretly laced with malware. Once installed, it gave hackers access to the employee’s personal device and login credentials — eventually leading to a breach of Disney’s internal systems. The hackers stole over 1 terabyte of data, including 44 million internal messages and sensitive financial information. The breach caused serious damage to the company — and cost the employee their job.

So, how do we help prevent a situation like this?

We maintain a list of approved, secure tools for your team to use. Need something new? Just reach out. We’ll help you find a safe option that gets the job done — without putting your business at risk.

###

###

###

###

###

###

###

###

###

###

###

### **SLIDE FIFTEEN: Rule Number Five, Shield Your Network**

### **SLIDE SIXTEEN:** Hackers love sneaking into unsecured networks — it’s like a bouncer letting them slip past the door and into your business.

**SLIDE SEVENTEEN:**

What does it mean to shield your network?

It means using a combination of tools to help guard your internal systems from cyber threats — blocking dangerous websites and securing your internet connection from outside attacks.

**Why are these important?**Weak networks are one of the easiest ways in, and once inside, attackers can steal data, install malware, or shut your systems down.

Strong network security is your digital fortress, it keeps bad actors out and sensitive data in.

For example, a school district in Georgia wanted to test how prepared their staff were for phishing attacks, so they sent out a fake email that said, “Click here for a free Chick-fil-A sandwich.” Sounds harmless, right? Well, the email purposefully sent people to a malicious clone of the real website- Chik-fil-a.com (missing the C in chick!).

If this had been a real attack, it could’ve given hackers access to sensitive school data — all for the promise of a chicken sandwich.

**How do we help mitigate real attacks that are designed to sneak into your network and steal data?**

We take care of the tools and protections that make up a secure network:

* **Firewalls** that monitor and block threats before they reach your system
* **DNS filtering** to block access to malicious sites (like that fake Chick-fil-A page)
* **Network separation** that keeps personal and work devices isolated
* **Secure remote connections** (VPNs) to protect your team when working from public Wi-Fi

Together, these tools lower the chances of a breach and keep your network resilient.

###

###

### **SLIDE EIGHTEEN: Rule Number Six, Encourage Cyber-Smarts**

**SLIDE NINETEEN:** Hackers don’t always just break in—they often trick you into letting them in!

**SLIDE TWENTY:**

**What are “Cyber-Smarts”?**

Cyber-smarts are like street smarts — but for the digital world. Ongoing education helps you and your team recognize phishing emails, fake websites, and social engineering tricks before they cause harm.

**Why is this important?**

Even the best security tools can’t stop someone from being fooled into handing over a password. Breaches don’t always come from a hacker breaking in — they can start with someone accidentally opening the door. All it takes is one click.

Take the case of a UK business owner who clicked a phishing email disguised as a PayPal notice. Within hours, their account was drained and the attacker vanished — all from a single scam.

**How can we help avoid situations like this?**

We provide regular, interactive cybersecurity training so you and your team know how to spot red flags — and report them before they turn into real threats.

From the CEO to the newest hire, we help everyone stay cyber smart — because awareness is your first and strongest line of defense.

**SLIDE TWENTY-ONE : Rule Number Seven, Back Up Data**

**SLIDE TWENTY-TWO :** Backups are your business insurance policy for digital disasters!

**SLIDE TWENTY-THREE:** Backups are secure copies of your important data — saved in case the originals are lost, damaged, or stolen. They allow you to recover quickly when something goes wrong.

**Why are backups important?**

Without them,a single accident or cyberattack could wipe out everything — from customer records to financial data.

Take the case of the City of Lafayette, Colorado. A ransomware attack froze their phones, email, and online payment systems. With no recent backups in place, they had no choice but to pay the hackers $45,000 just to regain access.

One backup could have saved them thousands — and prevented days of downtime.

Backups ensure you can bounce back fast after a crisis. When all else fails, they’re there to help.

**What do we do to keep your data safe?**

We configure automatic backups of your critical data and store them in multiple secure locations. Whether it’s a cyberattack, accidental deletion, or even a natural disaster, you’ll have a reliable copy ready when you need it most.

**SLIDE TWENTY-FOUR:** Cybersecurity isn’t about paranoia — it’s about being prepared.

At [Your MSP], we apply these Simple 7 rules to help safeguard your systems, protect your people, and support your business’s growth — even as threats evolve.

You don’t have to face cybersecurity challenges alone. We’re here to guide, protect, and partner with you every step of the way.

Let’s stay secure and maintain growth — together.

[Insert Call to Action for end user in last slide]