CyberFOX™

eBook

# THE SIMPLE 7™

## Essential Cybersecurity Rules Every Client Should Understand

**The MSP guide to converting "tech mumbo jumbo" into language your clients understand (and listen to!)**

# BRIDGING THE CYBERSECURITY COMMUNICATION GAP

You don’t just solve clients' tech problems — you protect their entire business. But explaining the importance of cybersecurity to people who think "phishing" is something you do on weekends?

**That's where things get tricky.**

This guide gives you straightforward language to explain seven simple (but critical) cybersecurity concepts to clients who don't "speak tech."

For each of our "simple seven" rules, you'll find:

- **A technical refresher (and commiseration about the struggle to make clients care)**
- **Client-friendly explanations that highlight YOUR value**

Use these explanations in newsletters, client meetings, or if you spot concerning behavior. These simple, relatable explanations help clients understand why your cybersecurity recommendations matter — and why they should appreciate the protection you provide.

Because at the end of the day, clients can't value what they don't understand.

**Let’s change that.**

# 1 Software updates

***The digital equivalent of locking your doors***

**The Struggle Is Real**

You know software updates are a device's first line of defense. But between clients ignoring prompts to restart their machine or disabling automatic updates altogether (*shudder*), keeping users' software up to date can feel like an uphill battle.

The hardest part isn't the technical implementation — it's getting clients to understand why that restart notification can't wait until next week.

**What to Tell Your Clients**

**Skipping updates is like leaving your front door unlocked overnight.**

Those update notifications might seem annoying, but they're actually your cybersecurity system at work. When your computer asks to restart, it's not being difficult — it's keeping you safe.

**Fast fact:**
In 2019, 60% of data breaches could have been prevented by software updates.

**Think about it like this:**

Just like you lock your front door at night, software updates secure your network against known threats.

Without updates, you're essentially leaving your company's front door wide open and rolling out the welcome mat for hackers.

When you see that update notification, just click "Update Now" and grab a coffee. And never turn off automatic updates.

Your business will thank you.

**True story:**
In 2017, Equifax suffered a massive data breach that exposed the personal information of 143 million people — all because they missed a routine software update. The patch had been available for months, but it wasn't installed in time.

**The result?**
A $1.4 billion cleanup bill and a permanent stain on the company's reputation.

# 2 Password Protection

***Because Password123 won't cut it***

**The Password Nightmare**

Let's be honest — getting clients to follow best practices for their login credentials can feel like herding cats. You've seen the sticky notes on monitors and the dreaded "CompanyName123!" password used everywhere.

(At least they used a special character?)

With a password manager like CyberFOX's Password Boss, you can offer clients a simple way to create and store strong passwords without the headache. We want to help make your life easier while significantly improving your clients' security posture.

**True story:**
A 150-year-old logistics company in the UK had to shut down — for good — because of one weak employee password. Hackers guessed the password, broke into their systems, leaked sensitive data, and caused so much financial damage that the company couldn't recover. Over 700 people lost their jobs.

**All because of one bad password.**

**That's why we take password protection so seriously.**

## What to Tell Your Clients

**Using weak passwords is like locking your front door but leaving the windows wide open.**

We implement several layers of password protection for your business:

Multi-factor authentication (or MFA) adds a second step to logging in. (Which is a good thing!) It's like how your bank card requires both the physical card AND your PIN code.

When we set up MFA for your accounts, your team members will need both their password and a second verification method (usually a code sent to their phone) to log in.

This ensures that even if someone steals a user's password, they can't get into the account without that second verification.

We also use a password manager to create and remember strong, unique passwords for all your accounts.

Think of it as a digital vault that only you can access. You'll only need to remember one master password instead of hundreds of different ones. You can also easily share passwords with other team members — without sending them via chat, email, or other channels that hackers may be able to infiltrate.

# 3 Admin Rights

***Not everyone needs a master key***

**The Admin Access Battle**

Oh, the admin rights dance. The CEO insists they need admin access to install their fantasy football tracker. The accounting department needs it for tax software updates. Everyone has a special reason why they should be the exception.

But you know that if a hacker gets access to these high-level privileges, it's game over for the business — and the fantasy football league.

CyberFOX AutoElevate keeps you and your clients in the game. Our privileged access management (PAM) solution allows end users to get their jobs done without permanent admin privileges. When someone needs elevated access, AutoElevate grants it temporarily either through pre-set rules you define for end users or via your direct approval. Either way, you maintain complete control.

**True story:**
In 2021, hackers got hold of an admin password for a company called Verkada — and it gave them access to over 150,000 security cameras. We're talking live footage from schools, hospitals, and even inside Tesla factories.

**It's a perfect example of why we lock down admin access — and why not everyone needs a master key to your business.**

## What to Tell Your Clients

**Admin accounts are the master keys to your digital kingdom.**

Imagine your computer network is an office building. Regular user accounts are like keys that open specific doors. Admin accounts are master keys that open EVERYTHING.

Admin accounts (also called administrator or privileged accounts) have special powers. They can install software, change any setting, and access everything on your network. That's why hackers target them first — with admin access, they can take over your entire system.

Most employees only need keys to their own office, not the master key to the whole building. The same principle applies to your network. By limiting who has admin access, you dramatically reduce your risk.

We can set up your systems so employees can still do their jobs without permanent admin privileges. When they need to install approved software, we have tools to grant temporary access without creating permanent security risks.

**Fast fact:**
Proper access management can even lower your cyber insurance premiums by showing you take security seriously.

# 4 Approved Apps

***Not all software is created equal***

**The Shadow IT Nightmare**

Shadow IT is the bane of your existence, isn't it? You set up a secure environment, then discover the marketing team is using some sketchy free design tool and uploading company assets to who-knows-where.

The challenge isn't just technical — it's psychological. Employees want to be productive and will find workarounds if they feel restricted. The key is balancing security with usability while explaining the very real dangers of using unapproved software.

**True story:** A Disney employee downloaded a free AI tool from a code-sharing site — only to find out it was infected with malware. Hackers used it to steal the employee's login credentials and break into Disney's internal systems, exposing millions of sensitive messages, including financial, and employee data.

**The worst part?**

**It all started with one unapproved app. That's why we always recommend sticking to the software we've vetted — it's not about control, it's about keeping your business safe.**

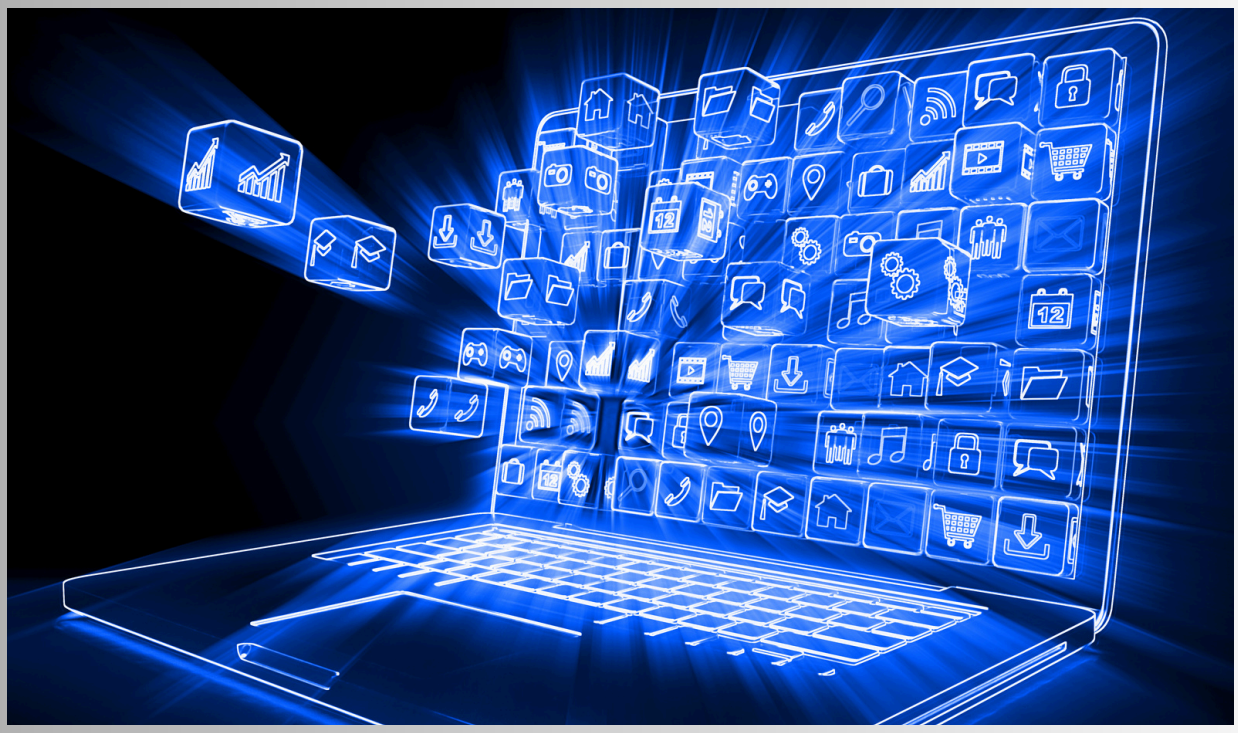
## What to Tell Your Clients

### Not all apps are safe — even if they're free and popular

Some software is safe and helpful, but others can steal your information or lock up your files (and charge a hefty ransom to release them.)

When you download apps from anywhere other than your IT-approved list, you're taking a big risk. That "free" version of some fancy new expensive software? It may contain hidden malware (malicious software) designed to steal your information.

Assume unapproved apps are unsafe until we say otherwise. And if you want to use a specific tool that’s not on the list, talk to us. We can help find safe options that won't put your business at risk



# 5 Network Security

***Your digital fortress***

**Helping Clients Understand What They Can't See**

Network security is the foundation of everything you do. But all that hard work is often invisible to clients until something goes wrong.

You've probably had clients question why they need to pay for "all that fancy network stuff" when "things seem to be working fine."

*(Eye roll.)*

**True story:**
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 chik-fil-a.com, a malicious clone of the real site, chick-fil-a.com. (Notice the extra "C"?)**

**The fake site was designed to steal users' login credentials. That means all of the company's data could have been accessed in exchange for the promise of a free chicken sandwich.**

**Fortunately, our clients don't have to worry about this. Our DNS filters block your users from accessing malicious sites so your data stays safe.**

**What to tell your clients**

**Hackers love weak networks — don't make it easy for them.**

Here are the tools and tricks we use to keep hackers out of your system:

1. **Firewalls** - Think of these as security guards for your network. They monitor all internet traffic, blocking threats before they reach your systems. Without a firewall, cybercriminals can easily sneak in and wreak havoc.
2. **DNS filtering** - This acts like a bouncer that blocks dangerous websites. If you accidentally click on a malicious link, DNS filtering stops the website from loading, protecting your business from malware, phishing, and scams.
3. **Network separation** - We keep your work and personal devices on different networks. This means if a hacker compromises someone's personal device, they can't use it to access your sensitive company data.
4. **Secure remote connections** - When your team works from public Wi-Fi spots (like coffee shops or airports), we provide secure connections (called VPNs) that encrypt their data. This prevents hackers from stealing information even on unsecured networks.

# 6 Security Training

***Because technology can't fix human error***

**The Human Element**

"Why do we need security trainings? Can't you just block the bad stuff?" If you had a dollar for every time you heard that, you could probably retire, right?

You know human error is the leading cause of security breaches. All the technical controls in the world can't stop an employee from clicking a convincing phishing email or giving their credentials to a scammer on the phone.

Running regular security trainings is relatively straightforward — the hard part is getting clients to see them as an investment rather than an interruption.

**True story:**
A business in the UK had its PayPal account drained after the owner clicked on a phishing email.

**We protect our clients from these attacks by offering regular cybersecurity trainings. We know phishing emails can be very, very convincing. We also know everyone at a company, from the CEO to the most recent hire, is very, very busy. It's easy to fall for a scam when you already have a lot on your plate.**

**Our goal is to make it easy for your team to identify malicious emails. Because even one wrong click can have serious consequences.**

## What to Tell Your Clients

**Even the best technology can't protect you from bad actors.**

Here's a surprising fact: hackers don't usually "break into" systems — they trick someone into letting them in.

Today's scammers are sophisticated. They create fake emails that look exactly like they're from your bank, boss, or business partners. They make phone calls pretending to be tech support. They design fake websites that look just like the real thing.

# 7 Backups

***Your safety net when everything else fails***

**The "We Have a Backup, Right?" Moment**

The challenge isn't creating backups. It's getting clients to understand their value before disaster strikes, and to budget appropriately for comprehensive backup solutions rather than the cheapest option.

**True story:**
A few years ago, the city of Lafayette, Colorado got hit with a ransomware attack that shut down their phones, email, and online payment systems. It brought operations to a standstill.

**The worst part? They didn't have recent backups. So instead of restoring their data, they had to pay the hackers $45,000 just to get back up and running.**

**It's a perfect example of why backups aren't optional — they're your safety net when everything else goes wrong.**


**What to tell your clients**

**Without backups, one mistake or attack could wipe out everything.**

Backups are your business insurance policy for digital disasters. They ensure you can recover when (not if) something goes wrong.

Imagine coming to work and finding all your business records, customer information, and financial data gone. For 60% of small businesses, this is a fatal blow. Most go out of business within six months of losing their data.

We create automatic backups of your important information and store copies in multiple locations. This protects you from all kinds of disasters: ransomware attacks, accidental deletions, hardware failures, even physical disasters like fires or floods.

The question isn't whether you need backups — it's how quickly you need to be back in business after a breach or other data-loss event. Without proper backups, recovery might be impossible, no matter how much you're willing to pay.

# YOU'RE MORE THAN JUST IT SUPPORT

The simple seven rules outlined in this guide aren't just best practices — they're business survival essentials.

Your clients might not always understand the technical details of what you do, but we hope these simple explanations help bridge that gap.

Of course, we know these seven rules don't cover every tool or tactic needed to stay secure. Cybersecurity is complex, and staying protected takes more than just checking a few boxes. But this framework gives your clients a solid foundation — and helps you start the right conversations.

**Use them to**

- Create educational newsletters
- Develop lunch-and-learn presentations
- Send quick reminders when you spot concerning behavior
- Justify security investments during budget discussions
- Explain why certain security measures can't be skipped

**Explore our full Marketing Toolkit HERE to access all the brandable Simple 7 materials designed to help you communicate your value.**

Whether you're battling sticky-note passwords, convincing CEOs they don't need admin rights, or helping clients understand why they can't just skip software updates, keeping clients safe can be a struggle.

That's why we created AutoElevate and Password Boss. They're easy to use, affordable, and effective — making it easier for you to keep clients secure without adding complexity to your workflows.

Because when it comes to cybersecurity, simplicity isn't just nice to have — it's essential.

Have questions about the simple seven or how CyberFOX works? We're here to help!

Visit CyberFOX.com and contact our team today to see how our solutions can strengthen your security offerings and help your clients understand the value you provide.