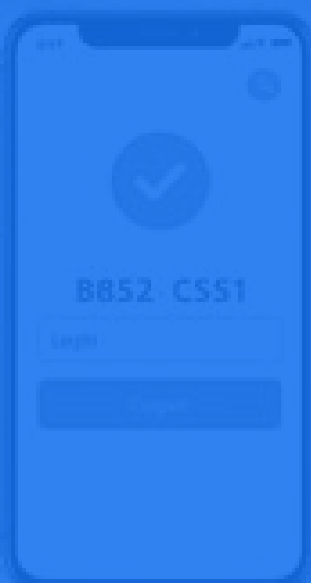


# **“MFA is a hassle.”**

**True.**

**So is incident response at 2:00 a.m.**

**Which inconvenience do you want?**



# MFA

is one of the *fastest, lowest-cost* ways to shut down most break-ins.

**And a surprising number of businesses still skip it.**



# PASSWORDS

get copied, bought,  
and traded daily.

**MFA makes a stolen  
password incomplete  
without the second  
step.**



Most attacks begin with a password grab.

## MFA blocks:

**x** Lookalike sign-in pages

**x** Phishing messages

**x** Reuse passwords

Automated login  
attempts

**x** Stolen credential lists



**YES,**

**MFA adds a few  
seconds at login**



**AND...**



... it can save you from:

- ✓ **Inbox takeovers**
- ✓ **Payment and banking fraud**
- ✓ **Data leaks**
- ✓ **Ransomware**

**That “extra step”  
suddenly feels cheap.**



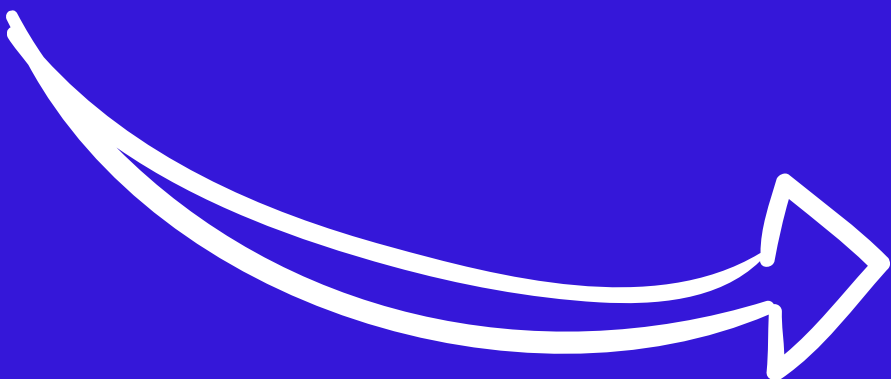


Think of MFA as a second lock on the door.

**A time-based code**

**An approve/deny prompt**

**A hardware security key**



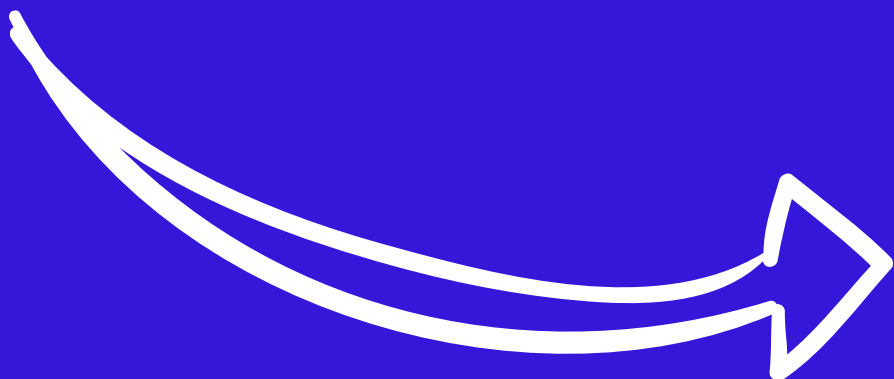
Roll it out where risk is highest first:

**1 Email accounts**

**2 Remote access**

**3 Accounting and payroll tools**

**4 Admin and privileged users**



**Adoption is all about friction.**

**Reduce it with:**

- ✓ **Authenticator apps (preferable to SMS)**
- ✓ **Trusted/remembered devices**
- ✓ **Simple, step-by-step instructions**



# **MOST RESISTANCE**

**is really  
confusion.**

**Message it plainly: "MFA  
protects your account  
and your work."**

**You'll see better buy-in  
fast.**



# SECURITY

isn't just  
protection.

**Customers feel safer  
when you can show you  
take access seriously.**



If convenience is the only goal, skip MFA.

If reliability and safety matter, turn it on.

**Need help  
implementing it  
cleanly? Reach out.**

