

**Think of your password
like the deadbolt on
your office door ...**

***Now ask yourself:
would you trust just
one lock?***



One password = a single lock

**If a cybercriminal picks it...
it...**

**they walk
right in.**





Attackers adore single-lock setups:

- X They can guess weak passwords**
- X Trick staff with phishing emails**
- X Or buy leaked logins on the dark web**



Multi-factor authentication

(MFA) =

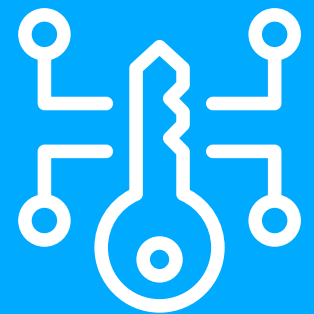
add an alarm to that door

Even with a stolen key, the alarm stops them.



Passkeys are like ditching keys entirely

They use your phone or laptop



+ quick biometric

(face/fingerprint) to sign in.

No password to steal, and far harder to phish.



MFA asks for:

Something you know
(your password)



Something you have
(e.g. a one-time code on your phone)



That could be:



A code texted or sent to your app



An approval pop-up



A fingerprint or face scan



**Here's the
kicker:**



about

80%

**of breaches trace
back to weak or
stolen passwords.**





**MFA (and passkeys)
block most of those
attempts—*full stop.***





**It's the quickest
security win for
your business:**

***seconds to use,
dramatically
cheaper than
cleaning up a
breach.***





Turn on MFA for email, cloud apps, banking.



Make it standard for your team.



Use an authenticator app, not just SMS.



**Want MFA and
passkeys rolled out—
without the
headaches?**

**We'll handle the
setup, training, and
support.**

**Let's lock things
down.**



Serving Chicagoland