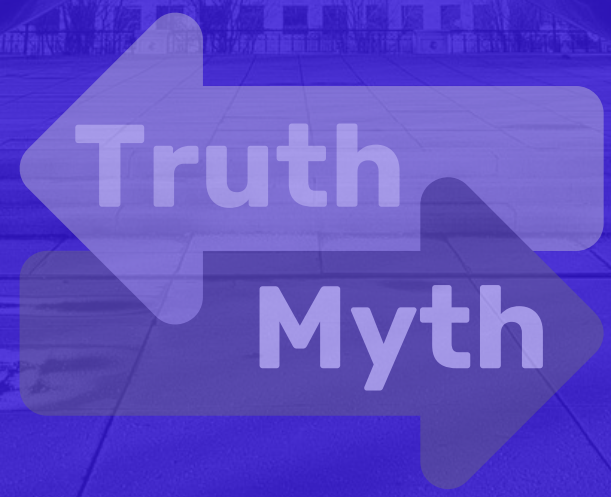
9 cybersecurity myths Chicago SMBs still believe

and what's really true



Myth 1

“Hackers only chase big brands.”

Truth:

Smaller orgs are easier to break into.

And often have more to lose when work stops.

REINTIVITY

Myth 2

“We bought security software, so we’re covered.”

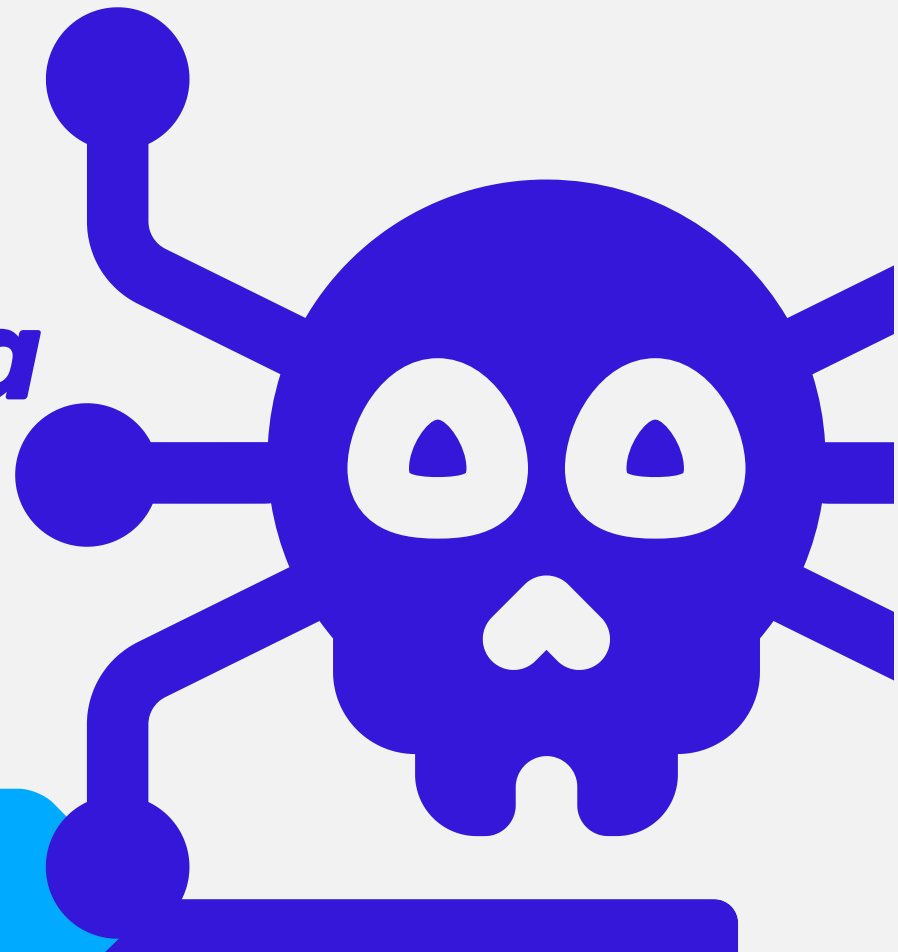
Truth:

Tools are just one layer.

Today’s attacks demand a multi-layered approach.

Myth 3

"We'd notice a breach right away."



Truth:

Many intrusions sit quietly for weeks.

Attackers rarely wave a flag.

REINTIVITY

Myth 4

“Our team can spot every phish.”

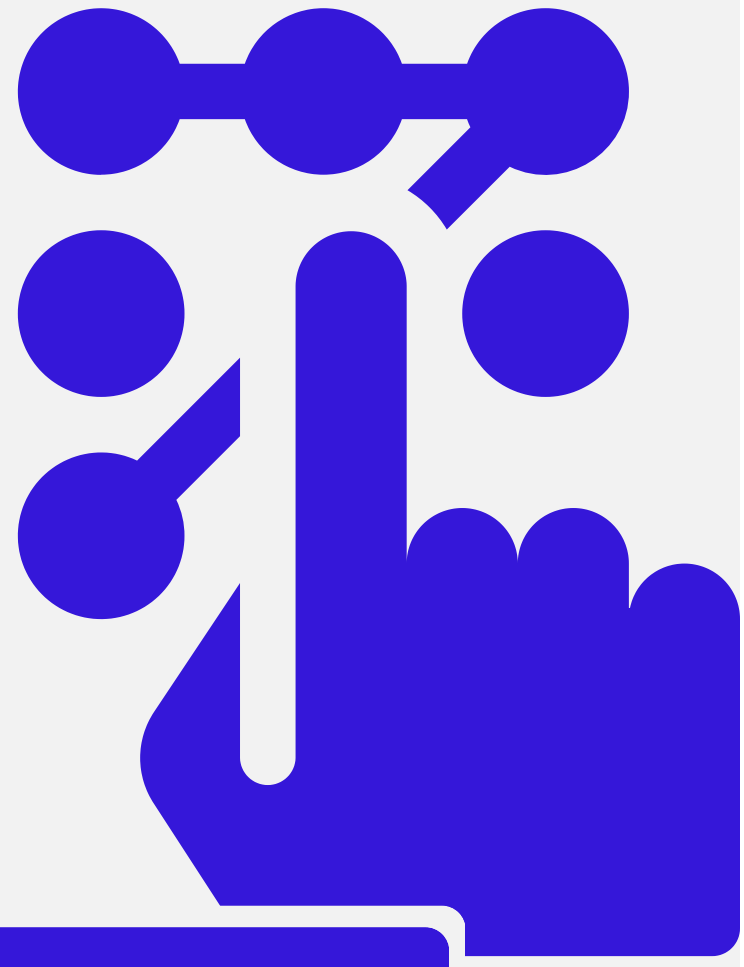
Truth:

Phishing is polished.

Even savvy users get fooled.

Myth 5

“Strong passwords are enough.”



Truth:

Without multi-factor authentication (MFA), one stolen password ***is a master key.***

REINTIVITY

Myth 6

“We back up, so we’re safe.”

Truth:

Backups fail—or get encrypted too.

Test them and store them safely.

Myth 7

“Security is IT’s problem.”

Truth:

People are the front line..

Everyone needs the basics.

REINTIVITY

Myth 8

“We don’t have anything worth stealing.”

Truth:

Customer records, bank details, emails, logins

-

hackers call that treasure.

Myth 9

"Security slows us down."

Truth:

Modern controls are fast.

A few seconds now beats weeks of downtime later.

REINTIVITY

Cybersecurity isn't a horror story

unless you ignore it.

If you're a Chicago-area healthcare practice, school, insurer, government office, or nonprofit, **we can help cut through the noise and protect your business..**

Let's talk.

REINTIVITY