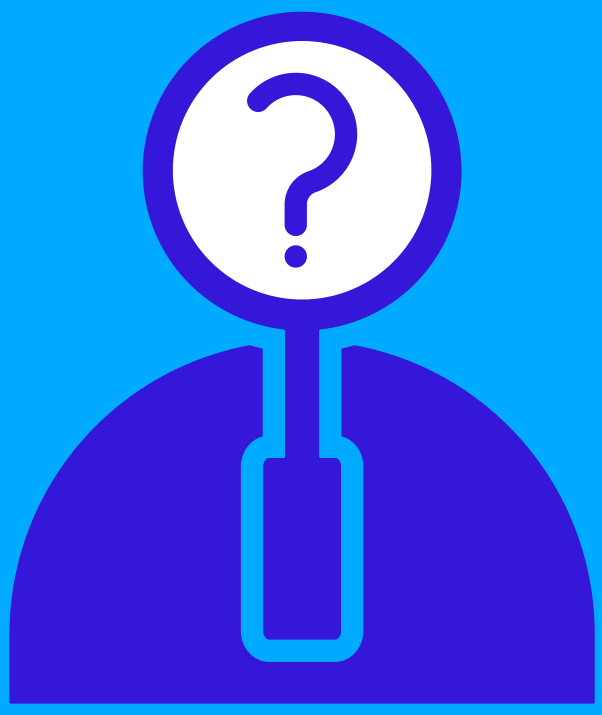
Your Website Talks

More than you realize

And yes—criminals are listening

Two Minutes, Tops

They land on your site... and in under 120 seconds begin collecting clues for an attack.



About Us = About You

Names, roles, and hierarchy?

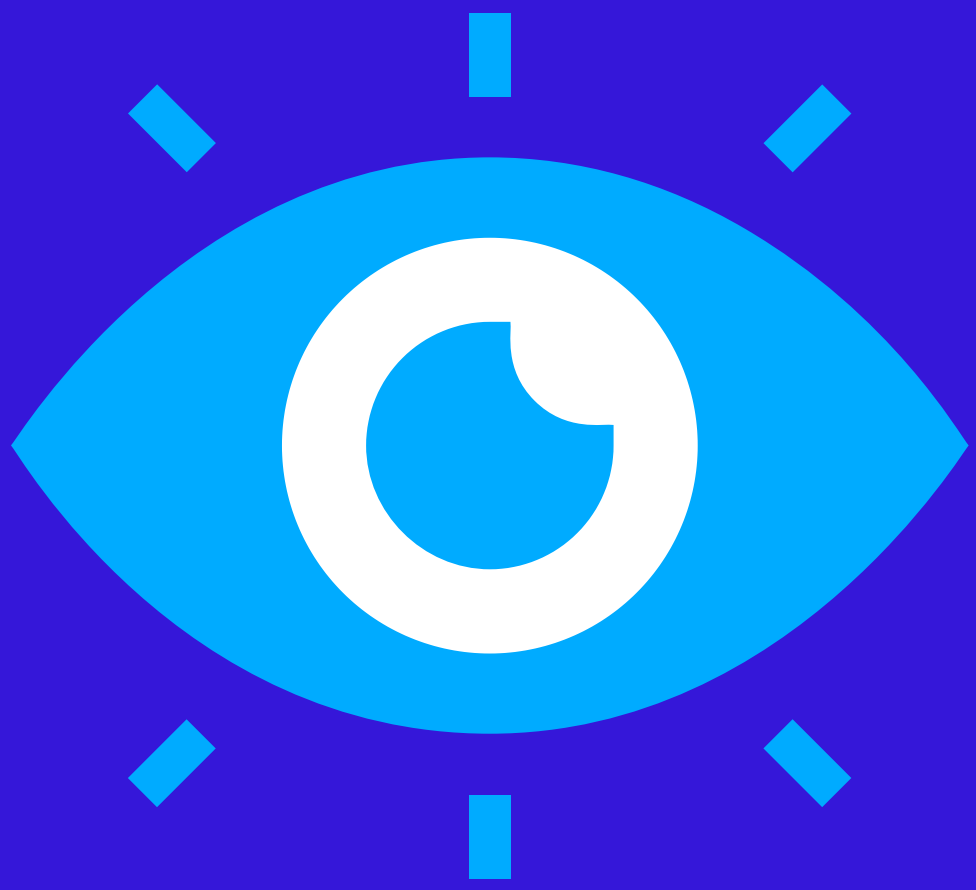
Goldmine for spear-phishing and CEO-impersonation scams.

Who To Target First:

Jane Doe – CFO

Tom Sample – Office Manager

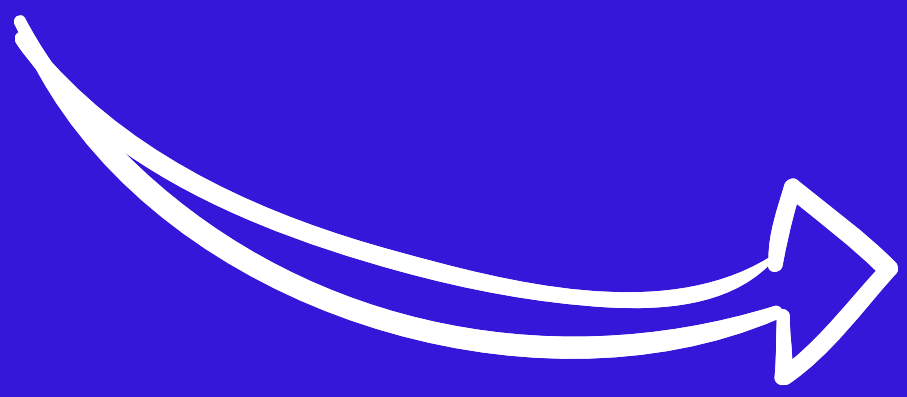
Now they know who moves money—and who to fool.

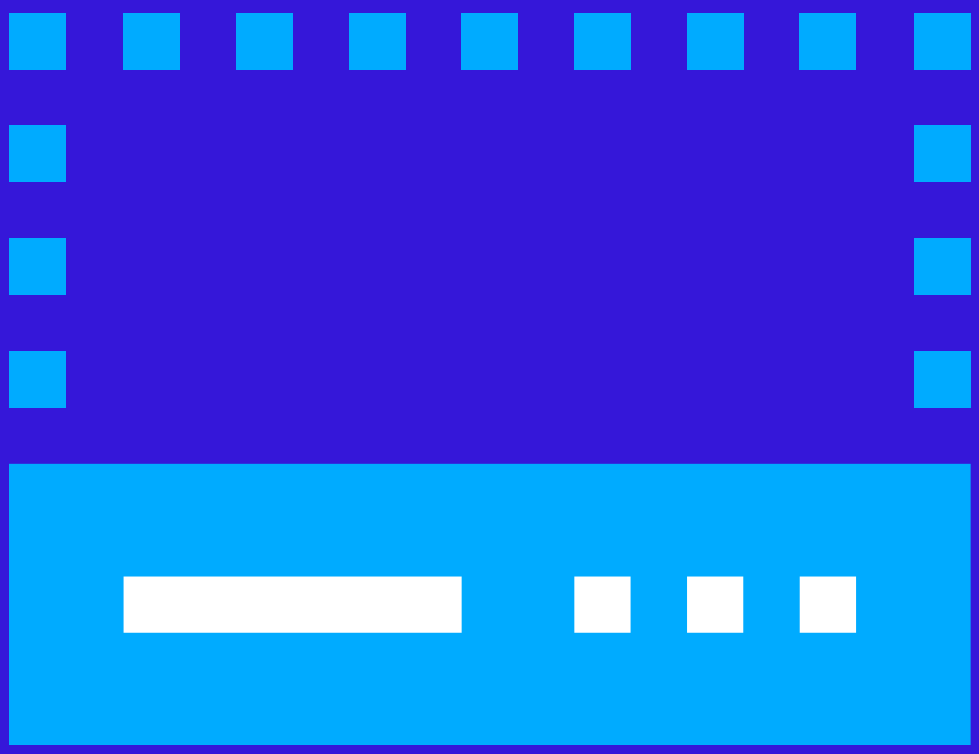


Login Links = Attack Map:

“Staff Login.” “Admin.” “Client Portal.”

Congrats—you just marked the doors they’ll try to pick.





Your Tech Stack, Public:

“Powered by WordPress”

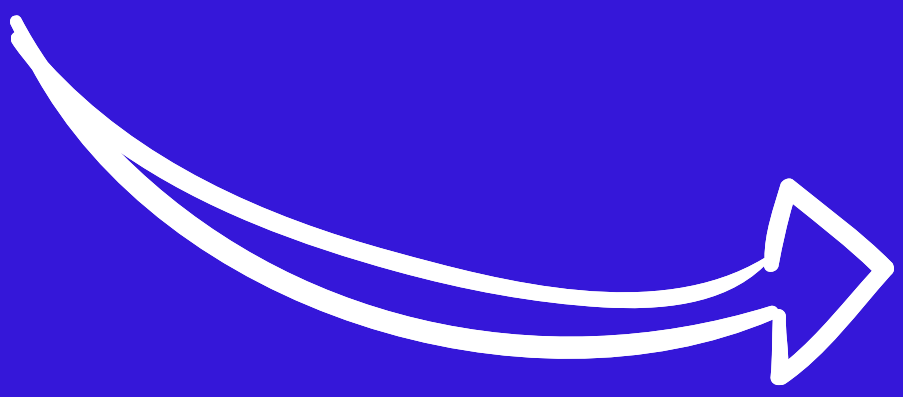
“Built on XYZ CRM”

That tells attackers exactly which exploits to test.

“We’re moving next week”

“New team members!”

Translation for criminals: distractions and process changes = opportunity.



They now know:

- ✗ **Who works there**
- ✗ **Who’s important**
- ✗ **What systems you use**
- ✗ **When you’re vulnerable**

And all from public info.

Think before you post - does that info help hackers?

Limit what's on your website

Hide portals behind extra security (SSO/MFA), not front-page links

- **Keep** software up to date
- **Use** strong, unique passwords (or a password manager)
- **Get** your team cyber-aware

It’s small steps that stop big problems.

Chicagoland healthcare clinics, schools, insurers, local agencies, and nonprofits—**we'll assess what your website is giving away and fix it fast?**

Get in touch.

REINTIVITY
technology solutions

Serving Chicagoland