

**Your website tells a cybercriminal
*more than you think.***



In 2 minutes

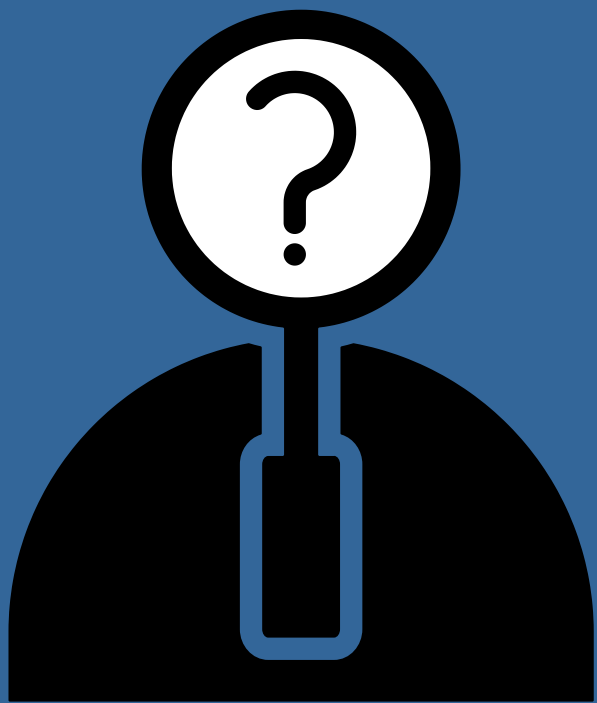
**they can gather
what they need to
launch an attack.**



A hacker

lands on your website.





Your About Us page

**tells them staff
names and job titles.**

***That's perfect for spear
phishing (targeted
scams) and fake emails
that look like they're
from your CEO.***





Your team list says:

Sarah Jones – CFO

Tom Smith – Office Manager

***Now the hacker knows
who handles payments...
and who to trick first.***



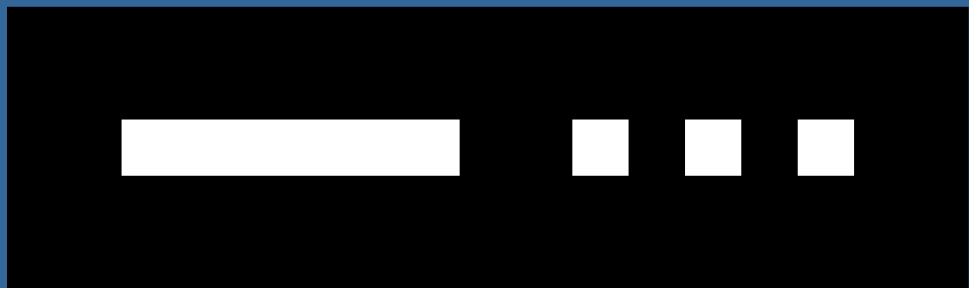


Spotted on your site:

**Staff login / Admin area /
Client portal**

***Now they know where to
target with password-
guessing attacks.***





Footer:

"Powered by WordPress"

"Built on XYZ CRM"

***Hackers take notes
because they know
what exploits to try.***





“We’re moving office next week”

“New team members joining soon”

***Criminals see that you’re
distracted, and your
processes might change.***



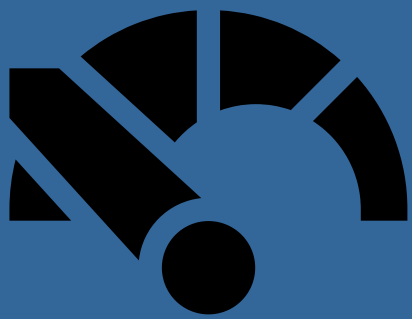
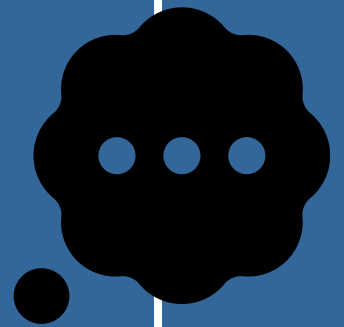
They now know:

- X Who works there**
- X Who's important**
- X What systems you use**
- X 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 staff portals behind extra security





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.



Not sure what your
website's giving away?

We can help. Let's
review it together.

Get in touch.