Your website tells a cybercriminal more than you think.

```
secont ingt: Beiteleeber:
Cinquariantending (itangolatedone)
meane isnaint iconcilisaon. Byi inste
Derrat = Dest | STA
בין ני נישם ביים ווני לומיוני ביונים ב
daith-7alasilanganiter; sisictonar: recepst: ion-ore Opt;)
ation_container {float: left; }
size: 82% !important;}
ct {width: 110px;}
st {width: 110px;}
h: 701px !important;}
{width:701px !important; height: 73px !important;}
(line-height: 25px !important; height: 225px; padding: 5px 0px !important; border: 1px sol
delete {height: 25px !important;}
delete i {line-height: 25px !important;}
spacer {width: 10px !important;}
s:hover {cursor: pointer; transform: rotate(180deg); transition:
                                                                     0.5s ease-out 0s;}
container {width: /28/0px;}
xey {width: 400px;}
value {width: 50px;}
{text-decoration: none !important;}
gs {padding: 10px !important;}
gs-container {margin-bottom: 5px !important;}
late_api_info {font-size: 10px; margin-left: 35px;}
ment {font-size: 106x;}
.badge {margin-left: 3px; border-radius: 5px !important;}
: 0 !important;}
slate {font-size: 10px;}
arrow-background {border-top-color: #fff !important;}
arrow{height:10px !important;}
                                                                               Your Business Technology Partner
```

www.inland-prod.com

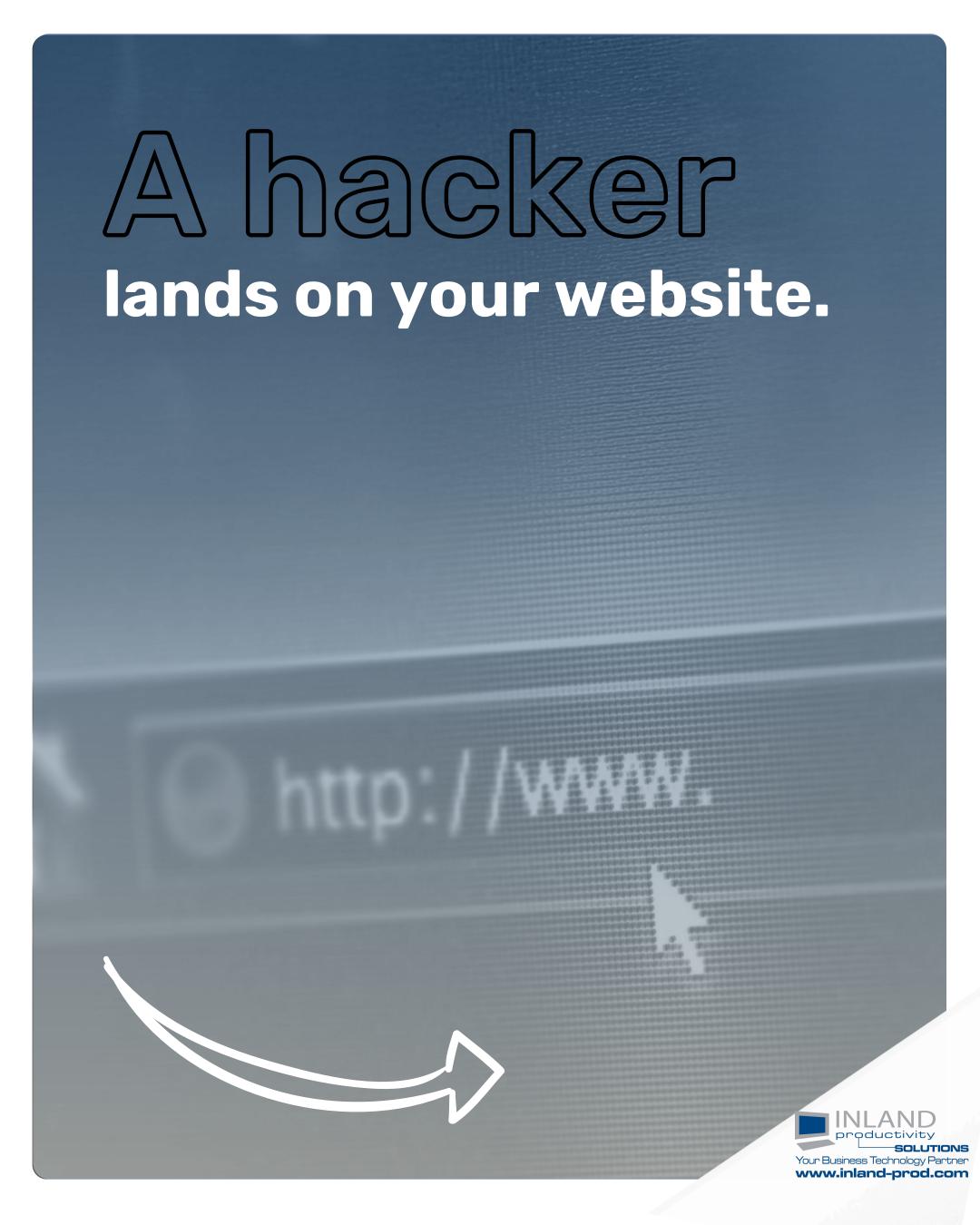


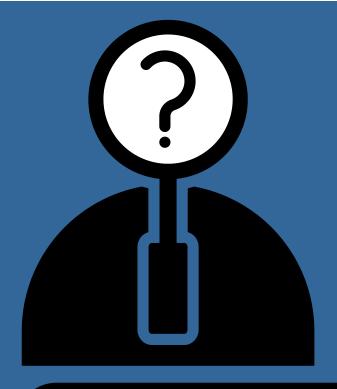
In 2 minutes

they can gather what they need to launch an attack.









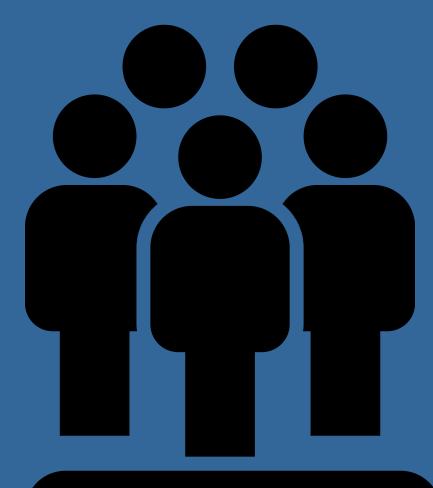
Your About Us page

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:

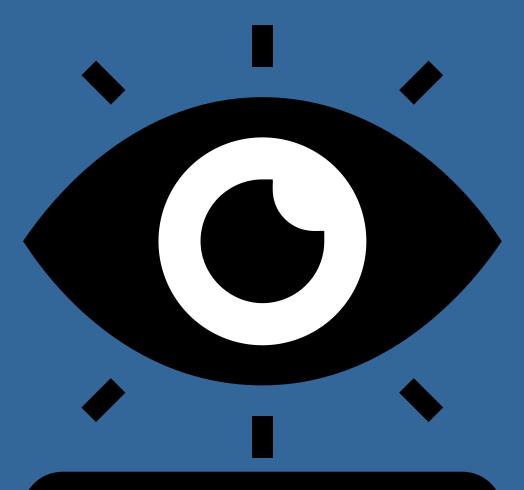
Sarah Jones - CFO

Tom Smith - Office Manager

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







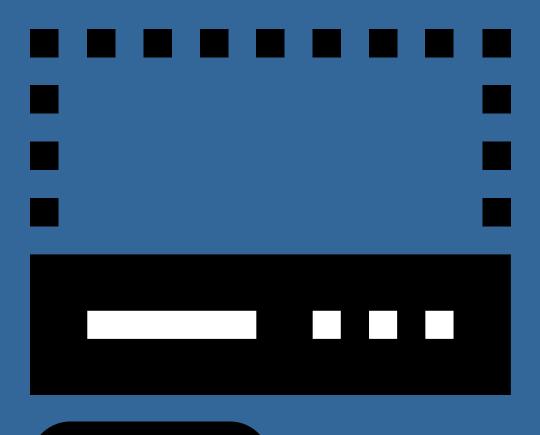
Spotted on your site:

Staff login / Admin area / Client portal

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







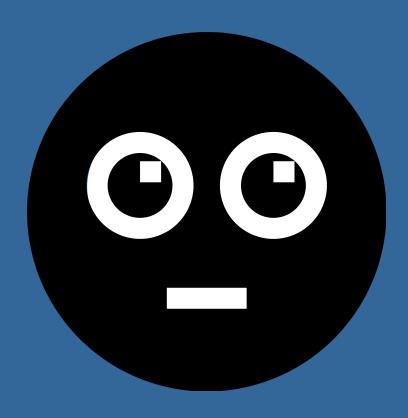
Footer:

"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:

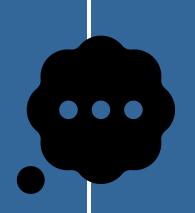
- Who works there
- Who's important
- What systems you use
- **When** you're vulnerable

And all from public info.





Think before you post - does that info help hackers?





Limit what's on your website

Hide 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.

