PHISHING & WEBSITE CONTACT INFO

WHY TOO MUCH TRANSPARENCY CAN GET YOU HOOKED

TOO MUCH INFO = EASY TARGET 🎯

- Contact pages with direct emails = gold mine for phishers.

- Scammers scrape your site with bots… and bait the hook.

- Even basic info like roles (e.g. 'Finance Director') attracts targeted scams.

EMAIL OVERLOAD: THE SPAM AVALANCHE 📧⛰️

- Public emails often get harvested by bots for phishing lists.

- Fake invoices, spoofed senders, and malware links follow.

- Staff may click things just trying to clear their inbox. Oof.

PHONE NUMBER FISHING 🕵️‍♀️ ☎️

- Bad actors use listed numbers to gather intel or impersonate.

- They spoof caller ID to make it look like internal staff.

- Voicemail messages can reveal too much — keep it vague!

AVOID THE OVERSHARE: SMART CONTACT OPTIONS 💡

- Use generic contact forms instead of email addresses.

- Create a single point of contact: info@ or support@

- Limit names/titles on your site unless absolutely necessary.

KEEP IT SIMPLE, KEEP IT SAFE 🔒😎

- Train staff to recognize phishing — regular reminders work.

- Audit your site: what info are you giving away?

- Less is more. Protect your people AND your reputation.