Has our practice received the "shared a file" attack email?

Run this sweep now, then monthly. One person searches; everyone answers. No blame — speed matters more than fault. · phishwatch.parkrddental.com.au

STEP 1 — Search the practice mailbox (search "All Mail", not just Inbox)

```
Gmail / Outlook search:  "shared a file with you" OR "shared a folder with you" OR "shared a file for you"
```

Suspect matches: from a real clinic, link only (no attachment), odd web address (often .vu), "open on your desktop / Windows laptop", sent at odd hours, BCC'd.

▼

Any matching emails found?

NO

You're clear for now

- Show every staff member the DO-NOT-OPEN poster
- Re-run this sweep monthly and after any warning from a colleague

YES

Do NOT click the link. Ask ALL staff, out loud, no blame:

- "Did anyone open this link, on any computer?"
- "Has any PC shown a strange **Windows Update** screen, a mouse moving by itself, or run hot while idle?"
- "Has any colleague asked about an email we don't remember sending?"

▼

What did the answers reveal?

NOBODY OPENED IT

Contain & report

1. Save the email as evidence (Gmail: ⋮ → Download message)
2. Report it — phishwatch site form (the sender clinic is a victim and gets a private phone call)
3. Delete the email; warn the team at huddle

LINK OPENED — NOTHING RAN

Precautionary lockdown

1. From a DIFFERENT device: change the email password, turn on 2-factor, sign out all sessions
2. Check mail settings for forwarding rules / filters you didn't create
3. Watch that PC for symptoms; report the email as at left

SOMETHING RAN / SYMPTOMS / COLLEAGUE ASKED

Treat as infected — act now

1. **Unplug that PC from network/Wi-Fi**; stop using it
2. Wipe & reinstall Windows (antivirus is not enough)
3. From a clean device: email password + 2-factor + sign out everywhere; audit mail rules
4. Change browser-saved passwords — banking first; call the bank if card details were saved
5. Warn your contacts; call your indemnity provider re patient data (OAIC)
6. Report: cyber.gov.au/report + the phishwatch site

Verify by phone before opening ANY share link — even from someone you trust. Never verify by email reply: the intruder answers their email.