CYBEREADY

Your ‘how-to guide’ for

Working from home

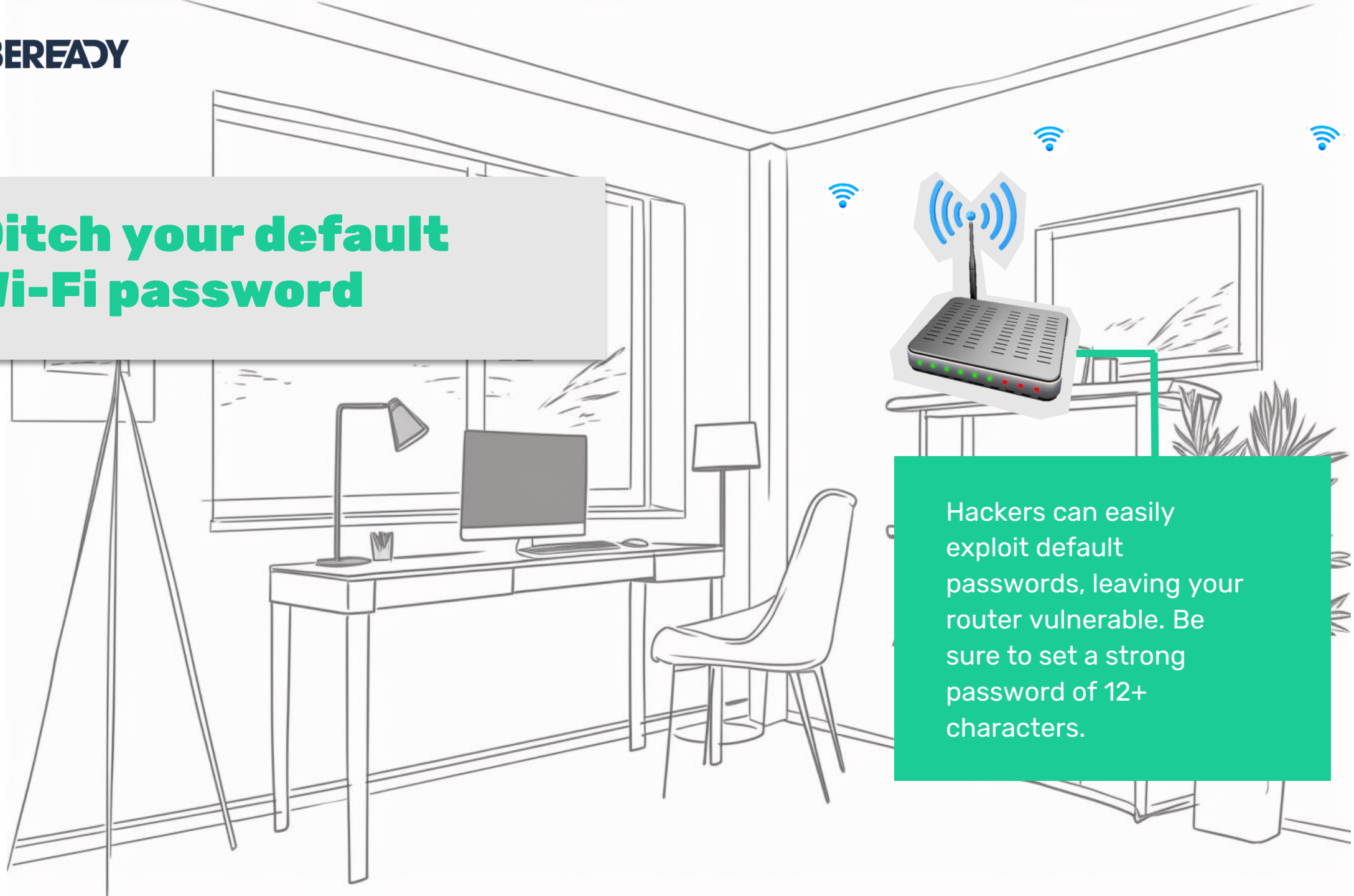
CYBEREADY

Working remotely totally redefines your security landscape.
We'll show you how to stay safe across the following topics:

1. Wi-Fi password
2. Devices
3. Workspace
4. Traveling
5. Tech support
6. Security backup

CYBEREADY

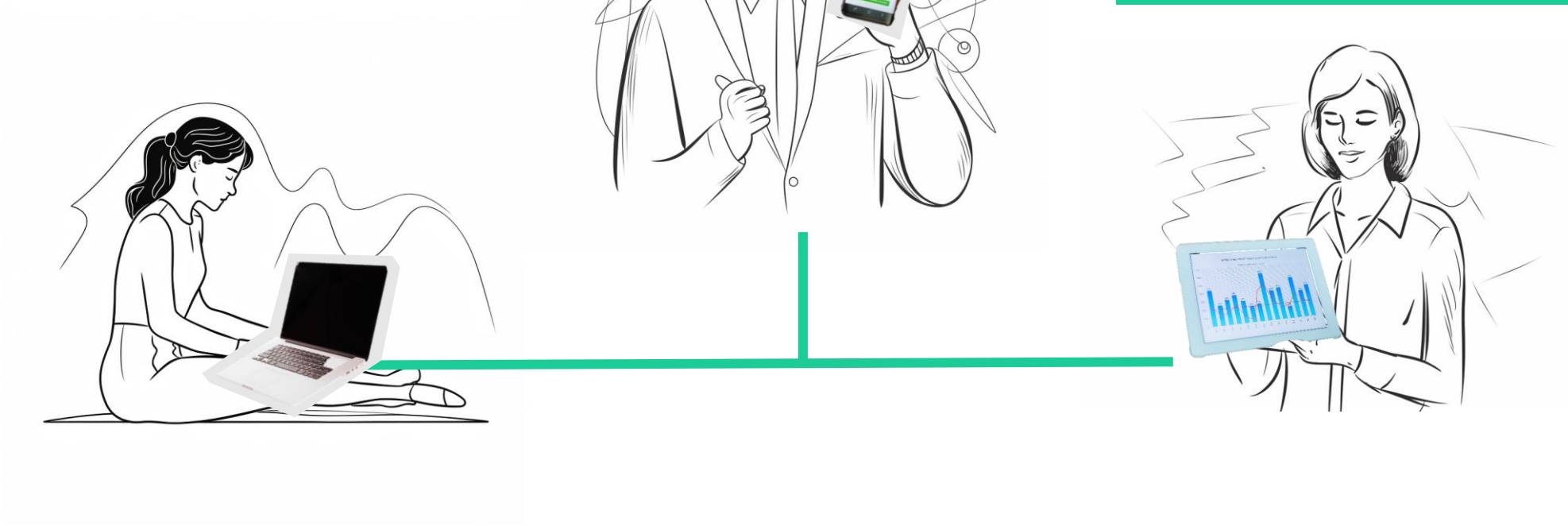
Ditch your default Wi-Fi password



Hackers can easily exploit default passwords, leaving your router vulnerable. Be sure to set a strong password of 12+ characters.

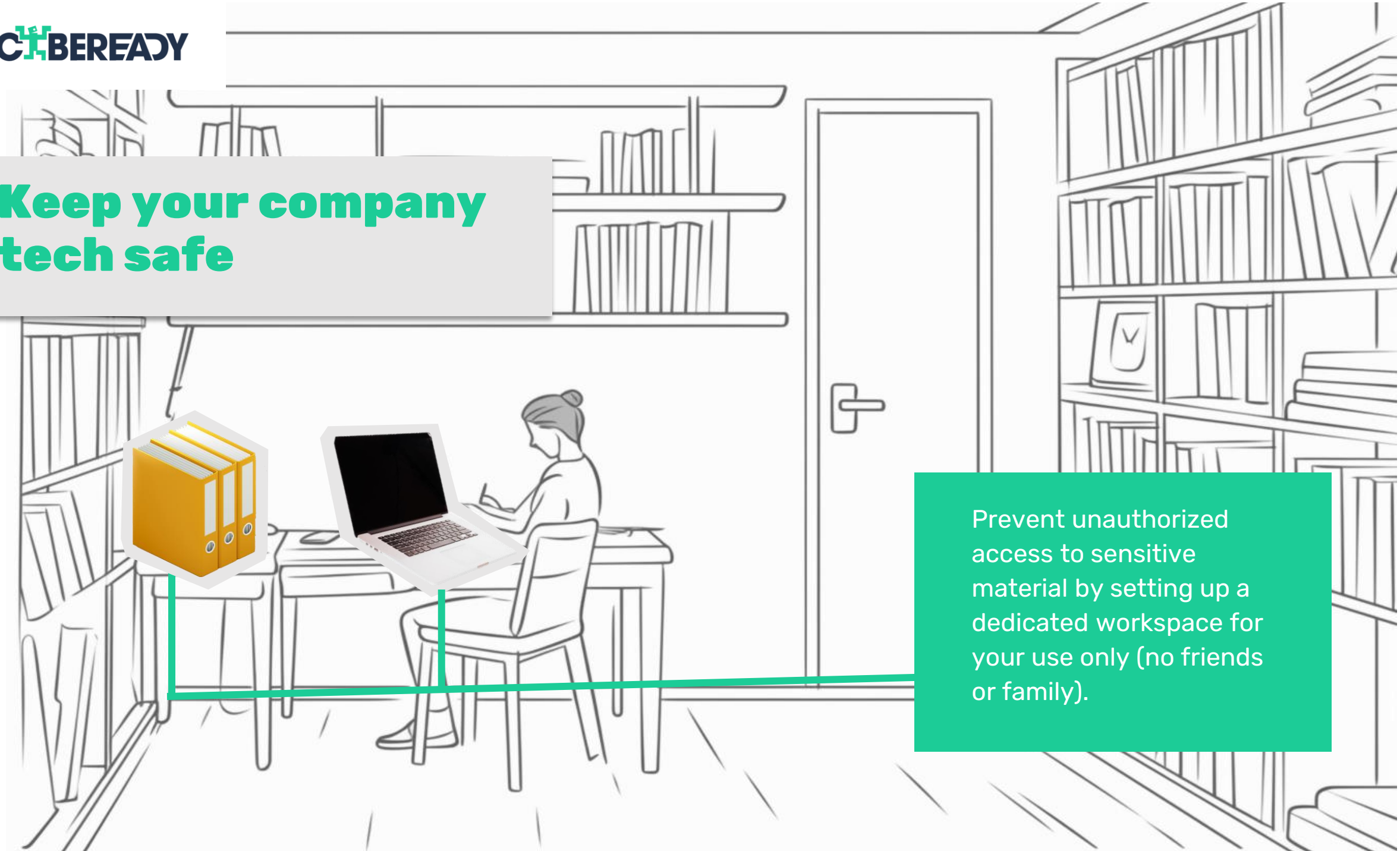
Work only on company-issued devices

Personal devices are no place for work-related documents! (They typically lack robust security features.) If accessing your calendar, email and instant messaging apps on your personal smartphone is a must, avoid sharing sensitive data.



CYBERREADY

Keep your company tech safe



Prevent unauthorized access to sensitive material by setting up a dedicated workspace for your use only (no friends or family).

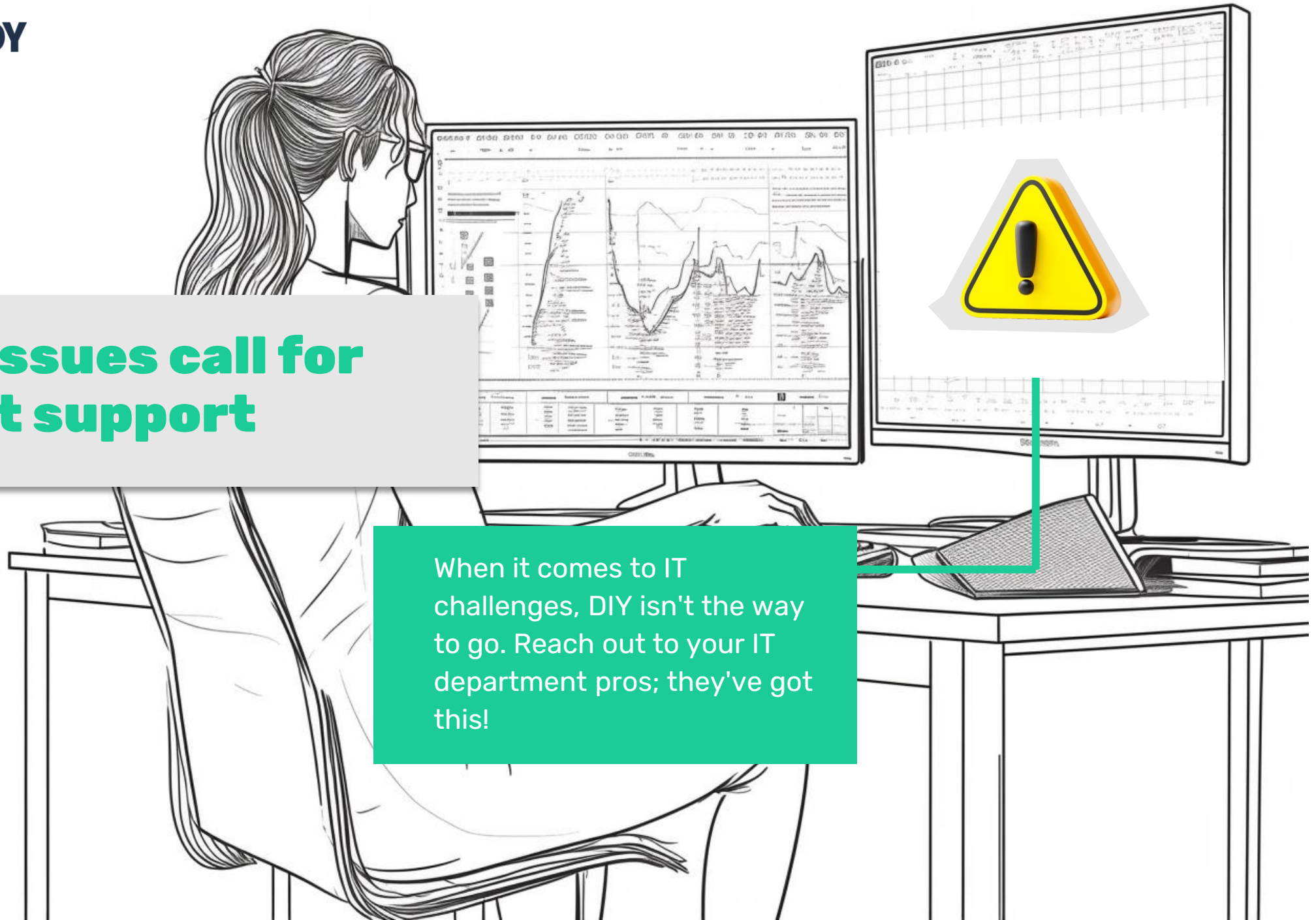
CYBEREADY

Protect your devices while traveling

Leaving home for 48 hours or more? Store work devices securely or ensure they're protected while on the move.

CYBERREADY

Tech issues call for expert support



When it comes to IT challenges, DIY isn't the way to go. Reach out to your IT department pros; they've got this!

CYBERREADY

Security concerns? Reach out to us.

No need to stress! The security team is here for you. We've got the expertise to safeguard your devices and data, no matter the scenario.