# RANSOMWARE
# READINESS CHECKLIST

Last reviewed: _____

## Backups (3-2-1)

- Confirm you keep 3 copies of important files: primary + 2 backups (one offline/offsite).
- Run a fresh backup to an external drive, then unplug/power it off (air-gapped).
- Check your cloud backup (iCloud/Google/OneDrive/Backblaze) shows a recent timestamp.
- Test-restore one file/folder and open it to verify integrity.

## Accounts & Devices

- Turn on MFA for email, banking, password manager, and key social accounts.
- In your password manager, fix at least 3 weak or reused passwords.
- Update phones, tablets, and computers; enable auto-updates.
- Update home router firmware; confirm WPA2/3, changed admin password, WPS off.
- Remove unused apps/extensions and review permissions.

## Awareness & Safety

- Do a 10-minute phishing refresher with the household; review real examples.
- Agree on an emergency plan: if something looks wrong, disconnect Wi-Fi and power off the device.
- Print/update a sealed emergency sheet with key contacts, account recovery codes, and device PINs.

## Monthly Notes / Follow-ups:

*Use this every month to reduce ransomware risk. Keep a copy offline.*