Sandbox Risky Files With A Virtual Machine — Checklist

Print and tick off. ~90 minutes for full setup.

Date completed: _____
Re-run this quarterly. Each pass takes about 12 minutes.

Beginner — do these in order

- ☐ 1. **VirtualBox or UTM installed on host**
  virtualbox.org / getutm.app
- ☐ 2. **Guest OS ISO downloaded + verified**
  Win11 Eval or Ubuntu LTS
- ☐ 3. **VM created with 4GB+ RAM, 40GB disk**
  Fixed disk preferred
- ☐ 4. **Network mode set to NAT**
  NOT bridged
- ☐ 5. **Shared folders DISABLED**
  Use clipboard only
- ☐ 6. **Guest OS hardened + Windows Defender on**
  All updates installed
- ☐ 7. **Sysinternals tools installed inside VM**
  Process Explorer, TCPView
- ☐ 8. **CLEAN snapshot taken**
  Named clearly
- ☐ 9. **Revert-tested by making a change then reverting**
  Confirm snapshot works

Advanced — if you want to go further

- ☐ Separate 'Browse' vs 'Burn' VMs
- ☐ Wireshark for network traffic capture
- ☐ VirusTotal / Hybrid Analysis pre-screening
- ☐ REMnux for reverse engineering
- ☐ Whonix for Tor-routed analysis
- ☐ Snapshot-revert automation