```
================================================================================
  ANYDESK SCAM - JOB CHECKLIST
  The customer's machine. Print this and tick it off as you go.
  Companion to: ANYDESK-SCAM-SWEEP.txt (the detailed command runbook)
================================================================================
```

**BEFORE YOU LEAVE THE HOUSE**

```
--------------------------------------------------------------------------------
[ ] USB stick with these files:
      Scam-Sweep.ps1
      Run-Scam-Sweep.cmd
      Run-Scam-Sweep-DATED.cmd
      ANYDESK-SCAM-SWEEP.txt   (print this - don't read off a screen)
      THIS CHECKLIST
[ ] Ask her: WHEN did it happen? (you'll want the date for the sweep)
[ ] Ask her: what did she see? AnyDesk? A phone number? A website?
[ ] Ask her: is her bank already rung? (if not, IN PERSON, DO THAT FIRST -
    ring the number on the card. Speed matters for getting money back.)
[ ] Ask her: whose phone/computer are we using to change passwords? (NOT hers)
[ ] YOUR OWN laptop or phone for the password work
```

**AT THE HOUSE - FIRST 5 MINUTES**

```
--------------------------------------------------------------------------------
[ ] ASK HER NOT TO TOUCH THE MACHINE WHILE YOU WORK
[ ] Take PHOTOS of the screen if anything dodgy is still open
      (AnyDesk window, a popup, a "tech support" number)
[ ] Ask if anything was plugged in (USB drives they "tested")
[ ] Unplug the network cable / turn off Wi-Fi while you work
[ ] Set the incident date aside for the -IncidentDate switch
```

**THE SWEEP - 10 MINUTES, CHANGES NOTHING**

```
--------------------------------------------------------------------------------
[ ] Double-click  Run-Scam-Sweep-DATED.cmd  (type the date), OR
      Run-Scam-Sweep.cmd  (no date, last 14 days)
[ ] Read the REPORT.txt it writes to the Desktop
[ ] Look for the [IN WINDOW] flags - those are the suspects
[ ] Screenshot everything before you delete anything (evidence for her bank)
```

**REMOVE THE REMOTE ACCESS**

```
--------------------------------------------------------------------------------
[ ] Is AnyDesk running?          tasklist | findstr /i anydesk
[ ] What IP was connected?       netstat -ano | findstr 7070     (NOTE IT DOWN)
[ ] Stop service                 net stop AnyDesk
[ ] Kill processes               taskkill /f /im AnyDesk.exe
[ ] Uninstall via Settings > Apps, or
      winget uninstall AnyDesk.AnyDesk
[ ] DELETE THE LEFTOVERS (the important bit - saved unattended password lives here):
      rmdir /s /q "C:\ProgramData\AnyDesk"
      rmdir /s /q "%APPDATA%\AnyDesk"
      rmdir /s /q "%LOCALAPPDATA%\AnyDesk"
      rmdir /s /q "C:\Program Files (x86)\AnyDesk"
      rmdir /s /q "C:\Program Files\AnyDesk"
[ ] Check Run keys for any AnyDesk entry and delete it
[ ] VERIFY GONE:
      tasklist | findstr /i anydesk        (should be empty)
      sc query AnyDesk                     (should not exist)
      netstat -ano | findstr 7070          (should be empty)
```

**CHECK FOR OTHER THINGS THEY TOUCHED**

---

[ ] Other remote tools?  TeamViewer / ScreenConnect / Supremo / Ammyy /
    RustDesk / Remote Utilities / Zoho Assist - uninstall any found
[ ] Scheduled tasks    - anything pointing at AppData/ProgramData/Temp?
[ ] Startup folders    - look inside both
[ ] RUN KEYS           - anything you don't recognise?
[ ] HIDDEN ADMIN ACCOUNT - THIS ONE MATTERS:
    net user
    net localgroup Administrators
    ANY account you don't recognise = delete:  net user <name> /delete
[ ] New services installed (the sweep lists these with dates)
[ ] Browser extensions she doesn't recognise
    chrome://extensions   /   edge://extensions
[ ] Browser signed-in account - is a strange account logged in?
[ ] Turn OFF Remote Desktop if it's on

**SCAN IT**

---

[ ] Microsoft Defender full scan (admin PowerShell):
    Update-MpSignature
    Start-MpScan -ScanType FullScan
[ ] Malwarebytes Free - full scan
    ***** DO NOT just click "Quarantine All". READ THE LIST FIRST. *****
    ***** On a technician's or normal PC, half of it may be legitimate. *****
[ ] HitmanPro - second opinion
    ***** Decline anything asking for a licence or email address *****
[ ] If either finds a LOADER or STEALER, treat this as compromised:
    consider a rebuild rather than a clean-up

**>>> THE PART THAT ACTUALLY PROTECTS HER <<<**

---

Say this to her out loud:
  "Cleaning the computer does not get your money back, and it does not
   remove them from your accounts. What stops them getting back in is
   changing your passwords - and you must do that from your PHONE."

[ ] SHE rings the BANK on the number printed on her card
    (not a number from an email, not a popup)
[ ] SHE changes her EMAIL password FIRST, then "sign out of all other
    devices / sessions" in that account
[ ] SHE changes BANKING + payment app passwords, same sign-out-all-devices
[ ] SHE changes everything saved in the browser:
    chrome://password-manager/passwords   (or edge://settings/passwords)
[ ] SHE turns ON 2-factor on email and banking
[ ] SHE checks her bank for any NEW payees / direct debits they added
[ ] SHE reports it:
    Scamwatch    https://www.scamwatch.gov.au/report-a-scam
    ReportCyber  https://www.cyber.gov.au/report-and-recover
[ ] All of the above FROM HER PHONE OR YOUR LAPTOP - never on her PC

**BEFORE YOU LEAVE**

---

[ ] Give her a written note of what you found and removed
[ ] Give her the bank / Scamwatch / ReportCyber details on paper
[ ] Leave her a printed password-change order (email first)
[ ] Tell her: "I can't prove what they took - nobody can. What I CAN say
    is the remote access is gone and the machine is clean."
[ ] Ask her to ring you if ANYTHING odd happens in the next few days
[ ] Consider: is her router OK? Did they get into anything else?
[ ] Document your own notes for your records

```
================================================================================
  FREE TOOLS THAT HELP - WHO / WHAT / WHY
================================================================================

  ALREADY COVERED BY THE SWEEP (no download needed)
  ------------------------------------------------------------------------------
  * Scam-Sweep.ps1        - the whole read-only diagnosis
  * netstat / tasklist    - what's running, what's connected
  * schtasks              - scheduled tasks
  * Event Viewer          - what happened, and when
  * Defender              - built into Windows, free

  SCANNERS - BRING ON THE STICK
  ------------------------------------------------------------------------------
  * Malwarebytes Free
      https://www.malwarebytes.com/mwb-download
      Best second-opinion scanner. Free version (no real-time) is what you
      want - do NOT let the onboarding wizard arm the Premium trial.
      WHY: catches things Defender's signature set misses.

  * HitmanPro (Sophos)
      https://www.hitmanpro.com/
      Great for "I just want a second opinion" - cloud-based, very fast.
      WHY: different detection approach entirely; good for a confidence check.
      NOTE: free trial works. Decline anything wanting a licence/email.

  * Microsoft Safety Scanner (MSERT)
      https://learn.microsoft.com/microsoft-365/security/intelligence/safety-scanner-downloa
      d
      Single .exe, no install, 10-day expiry. Good for a one-off deep scan.
      WHY: Microsoft's own standalone, runs alongside nothing.
      CAUTION: Defender must be functioning for it. If a third-party AV is
      installed and Defender is off, MSERT can fail (0x8007138F).

  * Kaspersky Virus Removal Tool (KVRT)
      https://www.kaspersky.com/downloads/free-virus-removal-tool
      Free, no install, no licence. Runs one scan and exits.
      WHY: a completely independent engine - useful third opinion.
      NOTE: some people won't want Kaspersky on principle; ask first.

  * ESET Online Scanner
      https://www.eset.com/au/home/online-scanner/
      Free, thorough, uses ESET's cloud.
      WHY: another independent engine.

  * AdwCleaner (Malwarebytes)
      https://www.malwarebytes.com/adwcleaner
      Targets adware / browser hijackers / unwanted extensions specifically.
      WHY: if the browser was messed with, this cleans extensions and
           search settings properly. Very good after a remote-access scam.

  * Farbar Recovery Scan Tool (FRST)
      https://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/
      Writes a full log of everything persisted on the machine.
      WHY: the thorough version of what the sweep does. Post the log to
           bleepingcomputer's forum and a human analyst reads it free.
      NOTE: for complex cases. Overkill for a simple AnyDesk removal.

  * Autoruns (Sysinternals / Microsoft)
      https://learn.microsoft.com/sysinternals/downloads/autoruns
      Shows EVERY autostart location Windows has - more than the sweep.
```

```
      WHY: nothing hides from it. Great for a final "is it really gone" pass.
      TIP: Options > Hide Microsoft Entries, then look at what's left.

  * Process Explorer (Sysinternals)
      https://learn.microsoft.com/sysinternals/downloads/process-explorer
      Better Task Manager. Shows what each process is, who signed it, and
      which network connections belong to it.
      WHY: if something odd is running, this tells you what it actually is.

  * GlassWire (free tier)
      https://www.glasswire.com/
      Shows which program is talking to the internet, in plain English.
      WHY: peace of mind - you can literally watch nothing suspicious
           phoning home. Nice to show the customer.

  SUGGESTED THREE SCANNERS (don't go overboard)
  ------------------------------------------------------------------------------
    1. Defender full scan        (already there, runs first)
    2. Malwarebytes Free         (second opinion - the standard one)
    3. HitmanPro OR KVRT         (third opinion if you're still unsure)

  More than three engines on a normal machine produces nothing but noise.
  If two clean engines find nothing, that's as good as you can get with
  scanning. Peace of mind comes from the removal being VERIFIED, not from
  running more scanners.


==============================================================================
  THE HONEST BIT - WHAT YOU CAN AND CAN'T PROMISE
==============================================================================

  YOU CAN say:
    - "The remote access tool is removed and verified gone."
    - "I checked autostart, tasks, services and accounts, and cleaned them."
    - "Scans are clean."
    - "No new admin account, no new service from that day."

  YOU CANNOT say:
    - "Nothing was taken."      (stealers leave no trace - unprovable)
    - "She's completely safe."  (only password rotation does that)

  THE LINE THAT'S BOTH TRUE AND REASSURING:
    "The way they got in is closed, and I've checked everything they could
     have left behind. The computer itself is clean. The thing that decides
     whether they can come back is your passwords - so let's do those now,
     from your phone, and then they're locked out."

  That's honest AND it gives her the peace of mind - because it's true.

==============================================================================
  END OF CHECKLIST
==============================================================================
```