Runbook

CONTENTS

page 2 Runbook

All characters in this printout were printed as written.

Runbook

```
------------------------------------------------------------
================================================================================
  SCAM SWEEP V3  -  RUNBOOK
  How to work a remote-access scam job, start to finish
  CoolTech Computers  -  Colin Clohesy
================================================================================

  THE RULES THAT NEVER CHANGE
    1. A name is not evidence.        A file called "AnyDesk" is a lead, not a verdict.
    2. Nothing is HIGH unless something is dated INSIDE the incident window.
    3. Wording carries confidence.    "Present, no evidence of use in the window"
                                      is a valid, honest result.
    4. The sweep only LOOKS. Only the Remover changes anything, per item.
    5. A clean scan is not an all-clear. You cannot prove what was taken.
    6. Never say "none / clean" unless the check actually succeeded.

--------------------------------------------------------------------------------
  BEFORE YOU TOUCH THE PC
--------------------------------------------------------------------------------
  Ask the customer, and write down:
     * What day and roughly what time did they first speak to the caller?
     * Was a screen blanked? Did they type any code, password or card number?
     * Which banks and accounts? Which did they log in to while connected?
     * Do they still have the caller's number, the website they were sent to?
  Do NOT let them log in to anything on this PC. Tell them to use their phone.
  If money is moving: the BANK FIRST (number on the card), then police/ReportCyber.

--------------------------------------------------------------------------------
  RUNNING THE SWEEP
--------------------------------------------------------------------------------
  1. Extract the kit zip to a stick (never run from inside the zip).
  2. Double-click 1-RUN-SWEEP.cmd, click Yes.
  3. Type the incident date DAY-MONTH-YEAR (05-03-2026). Check the window it echoes back.
  4. Choose drives (Y / N / A = all / 0 = none). Internal disks default to Y; USB sticks,
     external disks and the kit's own drive default to N. Each shows a worst-case time.
  5. Leave it. It takes a few minutes, plus up to ~4 minutes per drive you chose.
  6. At the end it offers to get the recovery tools ready (winget + Windows File Recovery).
     That is done AFTER the sweep so the installer is not mixed into the findings.

  Output: <kit folder>\<COMPUTER NAME>\<date-time>  (opens automatically)\
     FINDINGS.txt           READ FIRST
     REPORT.txt             the evidence trail
     REPORT-PRINTABLE.pdf   print this
     actions.json           what the Remover can do (typed actions, not commands)
     browser-activity.txt   every visit/download in the window, with times
     recent-files.txt       every file changed in the window on the scanned drives
     evidence\              registry/firewall exports, AnyDesk traces if any exist

--------------------------------------------------------------------------------
  READING THE RESULT
--------------------------------------------------------------------------------
  1. Top of FINDINGS.txt: CHECKS THAT COULD NOT RUN. Anything listed there is NOT clean.
     "SKIPPED BY THE TECHNICIAN" is a choice you made: not a failure, and not clean.
  2. TRIAGE: Tier 1 first (inside the window, not routine). Tier 2 next. Tier 3 is routine
     and collapsed - "recognised as routine, not examined further", never "safe".
  3. Each item says who it BELONGS TO and how that is known. Remember:
        * a digital signature PROVES the signer;
        * a "company name" inside a file is only a CLAIM - anyone can write it;
        * a file claiming to be Microsoft/Google/etc. that is not signed by them is Tier 1.
  4. The browser section is the most valuable: a TYPED address, a FORM submitted on it,
     and a DOWNLOAD that followed - with times to the second. The browser records THAT a
     form was sent, never what was typed.
  5. AnyDesk traces (connection_trace.txt, ad.trace) are the best record of sessions. If
     AnyDesk was uninstalled with its settings they are GONE - that does not mean there
     were no sessions. Prefetch, BAM, the firewall log and the Recycle Bin may still show
     it ran, and an older shadow copy may still hold the traces.

--------------------------------------------------------------------------------
  ACTING (only after you have exported the evidence)
--------------------------------------------------------------------------------
  2-RUN-REMOVER.cmd  (add -WhatIf first to preview)
     * shows each typed action; anything unusual is "refused" or "manual";
     * you pick numbers (or all) and type YES;
     * evidence is exported FIRST with SHA-256 hashes, then each change is made, checked,
       and logged as APPLIED or FAILED (never a false "done").
  Cleaning the PC does NOT get the money back and does NOT remove the thief from the
  customer's accounts. That is done FROM THEIR PHONE:
```

```
     * bank - ask for fraud; ask what contact details changed and where each login came from;
     * email first: password, 2FA, SIGN OUT ALL OTHER DEVICES; then banking, then the rest;
     * check new payees, saved cards, forwarding rules, new users on business accounts;
     * Scamwatch, ReportCyber, IDCARE 1800 595 160.
  Warn them: scammers often ring again as "the bank", "the fraud squad" or a "recovery
  service". Hang up and call the number on the card.

--------------------------------------------------------------------------------
  OPTIONAL: GET DELETED EVIDENCE BACK
--------------------------------------------------------------------------------
  4-RECOVER-DELETED.cmd. Needs Microsoft's Windows File Recovery (it offers to install it).
  The destination must be on a DIFFERENT drive from the one searched - no override.
  On an SSD with TRIM on, deleted data is usually gone within moments. Recovered files are
  UNTRUSTED: never open or run them on the customer's PC.

--------------------------------------------------------------------------------
  AFTER THE JOB
--------------------------------------------------------------------------------
  * Copy the report folder to your own storage. It holds customer data.
  * Delete the <COMPUTER NAME> report folder from the kit folder/stick (and C:\ScamKit if you used it): it holds
      customer data.
  * In your job notes: what you ran, when, what you removed, and any tools you added
    (Malwarebytes, winget, Windows File Recovery) - so nobody later mistakes them for the
    scammer's.
================================================================================
```