# Scam job checklist

**CONTENTS**

page 2 Scam job checklist

All characters in this printout were printed as written.

**Scam job checklist**

```
------------------------------------------------------------
================================================================================
  SCAM JOB CHECKLIST  -  V3          CoolTech Computers
================================================================================
  Customer: _____________________   PC: _____________   Date: _______________
  Incident date (DD-MM-YYYY): _______________   Time they first spoke to the caller: ________

  ASK FIRST
  [ ] Day and rough time the caller first rang / the customer went to a website
  [ ] Screen blanked?  [ ] Typed codes / passwords / card numbers?  What?
  [ ] Which banks and accounts? Logged in while connected?
  [ ] The caller's number, any website address they were given
  [ ] Is money still moving?  -> BANK FIRST, number on the card, from the phone
  [ ] Customer told: do NOT log in to anything on this PC

  RUN
  [ ] Kit extracted from the zip, running from the stick
  [ ] 1-RUN-SWEEP.cmd  (Yes at the permission prompt)
  [ ] Date typed DD-MM-YYYY, window echoed back and confirmed
  [ ] Drives chosen: _____________________   (skipped by choice: _______________ )
  [ ] Recovery tools prepared at the end?   Y / N   (note it in job notes if Y)

  READ
  [ ] Top of FINDINGS.txt: checks that could not run / failed / partial: _________________
  [ ] Tier 1 items reviewed: ____________________________________________
  [ ] Browser section: typed address _____________  form _________  download _________
  [ ] Remote tool evidence inside the window? (name + time) _____________________
  [ ] Anything in the Recycle Bin / shadow copies worth recovering?

  ACT  (2-RUN-REMOVER.cmd  -WhatIf first)
  [ ] Evidence exported and hashed BEFORE any change
  [ ] Only items the customer agrees to; nothing deleted that the bank/police may want
  [ ] REMOVAL-LOG.txt saved

  PROTECT THE CUSTOMER  (from their PHONE, not this PC)
  [ ] Bank told; asked: changed contact details? where did each login come from?
  [ ] Email: password, 2FA, SIGN OUT ALL OTHER DEVICES
  [ ] Banking, then everything saved in the browser, then business accounts (advertising, accounting)
  [ ] New payees, saved cards, forwarding rules checked
  [ ] Scamwatch / ReportCyber / IDCARE 1800 595 160
  [ ] Customer warned about the follow-up "fraud squad" / "recovery" call

  BEFORE YOU LEAVE
  [ ] Report folder copied off the PC (customer data)
  [ ] Report folder (<COMPUTER NAME>) removed from the kit folder/stick.   C:\ScamKit deleted if it was used.
  [ ] Job notes: tools added (Malwarebytes / winget / Windows File Recovery) and when
================================================================================
```