```
================================================================================
  ANYDESK SCAM - POST-INCIDENT SWEEP
  Command runbook for the technician
  Prepared by Colin Clohesy at CoolTech Computers
================================================================================

  WHAT THIS IS
  ------------
  A read-only sweep of a Windows machine after a remote-access scam
  (AnyDesk, TeamViewer, ScreenConnect, Supremo, RustDesk, etc.).

  It CHANGES NOTHING. It finds things. You decide what to remove.

  The script is GENERIC - not written for any one customer. Run it on any
  Windows PC. Nothing in it refers to a particular person or machine.


================================================================================
  THE KIT
================================================================================

  Scam-Sweep.ps1              the sweep itself (24 sections, read-only)
  Run-Scam-Sweep.cmd          double-click - sweeps the last 14 days
  Run-Scam-Sweep-DATED.cmd    double-click - asks for the incident date
  txt2pdf.py                  builds the printable PDF at the end
  logo.png                    your logo, used on the PDF header

  ANYDESK-SCAM-SWEEP.pdf      THIS document
  SCAM-JOB-CHECKLIST.pdf      the tick-off checklist
  SCAM-CONTACTS-FOR-CUSTOMER.pdf   hand this to the customer


================================================================================
  HOW TO RUN IT
================================================================================

  EASIEST - double-click a .cmd. It self-elevates (click Yes at UAC).

      Run-Scam-Sweep-DATED.cmd   -> asks for the date, then sweeps
      Run-Scam-Sweep.cmd         -> no date, sweeps the last 14 days

  BY HAND - in an admin PowerShell:

      cd E:\SCAM-KIT
      powershell -ExecutionPolicy Bypass -File .\Scam-Sweep.ps1 -IncidentDate "2026-11-10"

      or, with no date:

      powershell -ExecutionPolicy Bypass -File .\Scam-Sweep.ps1

  SWITCHES
      -IncidentDate "YYYY-MM-DD"   focus the search on a date (+/- 2 days)
      -DaysBack 30                 how far back with no date (default 14)

  DATE FORMAT IS STRICT:  2026-11-10   (year-month-day, dashes)
  Get it wrong and it tells you and exits. It does not guess.

  RUN IT OFF THE STICK. Do not copy it onto the customer's machine.
  If Windows blocks it (came from another computer), either right-click the
  .ps1 > Properties > tick Unblock, or copy the SCAM-KIT folder to their
  Desktop, run it, and DELETE the folder before you leave.
```

```
================================================================================
  WHAT IT LOOKS LIKE WHILE RUNNING
================================================================================

  Numbered steps, [1/24] through [24/24]. Each says what it is doing and how
  long it took:

      [ 8/24] BROWSER HISTORY
              Copies locked browser DBs, then scans them. SLOW on big profiles.
              Chrome / Default  (History is 12.4 MB - copying, then scanning)
              (this can take a while - dots mean it is working) ...... done (1.6s)

  A slow step prints DOTS. Dots mean it is working, not frozen.
  The final TIMING block lists anything that took over 20 seconds.


================================================================================
  WHAT IT PRODUCES
================================================================================

  A folder on the Desktop named  scam-sweep-YYYYMMDD-HHMM  containing:

      REPORT-PRINTABLE.pdf   <- THE ONE TO PRINT. Branded, A4, page numbers.
      REPORT.txt                the raw report
      browser-history.txt       every URL found, plus finance/remote filtering
      downloads-in-window.txt   anything downloaded in the window
      usb-history.txt           every USB storage device ever plugged in
      scheduled-tasks.txt       all non-Microsoft tasks
      firewall-rules.txt        all inbound allow rules
      recent-files.txt          every file touched in the window (can be large)

  recent-files.txt is often 10 MB+ and is NOT included in the PDF - it is
  for reading on screen if you need the detail.


================================================================================
  THE 27 SECTIONS
================================================================================

   0  REGISTRY BACKUP             *** RUNS FIRST. Rollback safety net. ***
   1  Remote-access tools          19 products + port 7070
   2  Autostart Run/RunOnce keys   with file dates
   2b Startup folders              user + all users
   3  Scheduled tasks              non-Microsoft, with file dates + boundaries
   4  Local accounts               new account = smoking gun
   5  Services installed           Event 7045 - THE TIMELINE
   6  Files created/changed        in the window (TIME-BOXED - see below)
   6b Executables created          in the window (the most telling one)
   6c Hidden + drop locations      ProgramData, Public, Temp, Recycle Bin
   7  Browser profiles             every profile + extension IDs
   8  Browser history              URLs + finance/remote-access filtering
   9  Downloads in the window      all users
  10  USB history                  every removable device ever attached
  11  Network drives / shares      anything mapped out
  12  Printers                     fake PDF printers are a known trick
  13  Remote Desktop settings      RDP + Remote Assistance state
  13b FIREWALL RULES               inbound allow rules - see the warning below
  14  Recently opened documents    what was opened in the window
  15  System restore points        rollback possible? or deliberately gone?
  16  Antivirus status             Defender state + detection history
  17  Software installed           in the window
  18  OneDrive / cloud sync        *** SIGNED IN OR NOT? see below ***
  19  DEEP REGISTRY AUTOSTART      Winlogon, IFEO, AppInit, BHO, COM, LSA, etc.
```

```
  20  WMI PERSISTENCE              fileless. should be empty.
  --  SUMMARY + TIMING + PRINTABLE PDF


================================================================================
  SECTION 6 - FILES IN THE WINDOW (time-boxed, and why)
================================================================================

  This is the slowest section. It walks the folders where things actually get
  dropped and looks for files touched inside the incident window.

  IT IS TIME-BOXED. Each folder gets a budget in seconds. If a folder hits
  its limit the scan stops and THE REPORT SAYS SO:

      AppData (Local): 46935 files in 1204 folders  *** PARTIAL - TIME LIMIT ***
      ProgramData:     12332 files in 2962 folders  (8.8s, complete)

  WHY: measured on a real workstation, walking everything took over 9 minutes
  with no output and the script looked frozen. Real numbers:

      AppData (Local)    329,016 files   245 s
      User Documents      92,505 files    66 s
      User Desktop        55,670 files    29 s
      User Downloads      49,419 files    29 s
      AppData (Roaming)   35,962 files    21 s
      ProgramData         12,323 files     8 s
      FULL user profile  778,129 files   550 s

  A bounded, HONEST partial result beats an unbounded silence. The report
  never claims a folder was fully checked when it was not.

  IF YOU NEED THE FULL WALK: set  $deepScan = $true  near the top of the
  section. It takes 5-10 minutes and includes the whole user profile. The
  report will say the scan was extended.

  WHERE IT LOOKS (drop points, not the whole disk):
      AppData Roaming, AppData Local, ProgramData, Windows Temp,
      User Downloads, User Desktop, User Documents, C:/Users/Public

  WHAT IT SKIPS (huge and irrelevant): OneDrive, node_modules, .git, .svn,
  WindowsApps, Package Cache.

================================================================================
  SECTION 0 - REGISTRY BACKUP (runs automatically, first)
================================================================================

  Before it scans anything, the sweep exports the persistence-relevant parts of
  the registry to  <report-folder>\registry-backup\  as timestamped .reg files:

      HKLM-Run.reg  HKCU-Run.reg  Winlogon.reg  IFEO.reg  AppInit-Windows.reg
      BHO.reg  SessionManager.reg  Lsa.reg  PrintMonitors.reg  Services.reg
      FirewallPolicy.reg  HKCU-CLSID.reg  ... and more

  Plus system-state.txt - a written snapshot of services, scheduled tasks,
  local accounts and firewall rules.

  ROLL BACK ANY CHANGE:
      Double-click the .reg file,   or:   reg import "<file>.reg"

  HONEST LIMIT: a .reg export restores VALUES, not permissions. It is a good
  safety net, not a full System Restore point.
```

```
================================================================================
  SECTION 19 - DEEP REGISTRY AUTOSTART
================================================================================

  The locations Run keys and the Startup folder do NOT cover:

   19a  Winlogon Shell / Userinit / Notify    runs before almost anything
   19b  IFEO Debugger                         THE SNEAKIEST ONE
   19c  AppInit_DLLs                          injects into every process
   19d  Browser Helper Objects                browser hijack
   19e  COM hijack (HKCU shadowing HKLM)      CLSID substitution
   19f  LSA / BootExecute / SecurityProviders  security-level hooks
   19g  Screensaver hijack + cmd AutoRun      .scr and every cmd.exe
   19h  WOW6432Node Run keys                  32-bit mirror of the Run keys
   19i  Print monitors                        loads a DLL into the spooler

  WHAT "NORMAL" LOOKS LIKE
      Winlogon Shell        = explorer.exe
      Winlogon Userinit     = C:\Windows\system32\userinit.exe,
      IFEO Debugger         = NO Debugger values anywhere
      AppInit_DLLs          = empty, LoadAppInit_DLLs = 0
      BootExecute           = autocheck autochk *
      SecurityProviders     = credssp.dll
      cmd AutoRun           = not set
      COM shadowing         = 0 entries

  IFEO IS THE ONE TO UNDERSTAND. It attaches a "debugger" to any program. Set
  it on notepad.exe and launching Notepad launches their payload. A Debugger
  value on a normal Windows binary is essentially never legitimate.

  NOTE ON COM (19e): a per-user CLSID on its own is NORMAL - OneDrive, Teams
  and Dropbox all register in the user hive. Only an HKCU CLSID that SHADOWS
  a different HKLM one is a hijack. The check compares both and only reports
  the shadowing case.

  NOTE ON PRINT MONITORS (19i): judged by DRIVER PATH, not by name. Vendor
  drivers in  C:\Windows\System32\spool\drivers\x64\3\  are NORMAL. Anything
  loading from a user folder, Temp or ProgramData is the red flag.


================================================================================
  SECTION 20 - WMI PERSISTENCE
================================================================================

  WMI can run code when a system event fires. No file on disk, nothing in Run
  keys, nothing in Task Scheduler. Fileless, and survives almost everything.

  It checks __EventFilter, __EventConsumer, __FilterToConsumerBinding, and
  names ActiveScriptEventConsumer / CommandLineEventConsumer explicitly.

  WHAT NORMAL LOOKS LIKE: exactly one Microsoft built-in -
      Filter   : SCM Event Log Filter
      Consumer : SCM Event Log Consumer (NTEventLogEventConsumer)
      Binding  : 1

  Anything else is suspicious until proven otherwise. Legitimate software
  almost never uses WMI event subscriptions.

  REMOVING IT (only if you actually find it):
      Binding first, then consumer, then filter.
      Get-CimInstance -Namespace root\subscription -ClassName __FilterToConsumerBinding |
        Where-Object { $_.Filter -match 'NAME' } | Remove-CimInstance
      Get-CimInstance -Namespace root\subscription -ClassName __EventConsumer |
```

```
      Where-Object Name -eq 'NAME' | Remove-CimInstance
    Get-CimInstance -Namespace root\subscription -ClassName __EventFilter |
      Where-Object Name -eq 'NAME' | Remove-CimInstance
```

```
================================================================================
  THREE THINGS TO LOOK AT FIRST
================================================================================

  1. SECTION 13b - FIREWALL RULES
  --------------------------------
  THIS IS THE ONE PEOPLE MISS. Uninstalling AnyDesk removes the SERVICE but
  often LEAVES THE INBOUND FIREWALL RULES behind. Those rules are open and
  waiting if anything reinstalls.

  Seen in the field: nine inbound AnyDesk rules still present after the
  service was already gone.

  Remove them:
      Get-NetFirewallRule -DisplayName "*AnyDesk*" | Remove-NetFirewallRule
  Then verify:
      Get-NetFirewallRule -DisplayName "*AnyDesk*"
  Or use the GUI:  wf.msc  ->  Inbound Rules  ->  delete the AnyDesk entries
  Check OUTBOUND rules too.

  2. SECTION 18 - ONEDRIVE / CLOUD SYNC
  ---------------------------------------
  THE QUESTION THAT DECIDES EVERYTHING: is an account SIGNED IN?

  Installed-but-never-signed-in is harmless. Windows ships with it and most
  people ignore it - they will honestly say "no, I don't use OneDrive" and be
  right, while the folder and three scheduled tasks still exist.

  SIGNED IN is different. If a scammer signed into THEIR OWN Microsoft
  account, the customer's Desktop/Documents/Pictures sync straight to them.
  Silent, clean, and invisible to every other check.

  READ THE ACCOUNT NAMES in section 18b. If any is not the customer's, that
  is a live cloud sync to someone else's storage.

  3. SECTION 5 - THE SERVICE TIMELINE
  -----------------------------------
  Event 7045 with timestamps. This is the main evidence. An AnyDesk service
  install with an auto-start trigger and LocalSystem account, timestamped
  inside the incident window, is about as clear as it gets.


================================================================================
  REMOVING REMOTE ACCESS - THE SEQUENCE
================================================================================

  Do it in this order. Doing it out of order leaves things behind.

  1. KILL THE PROCESS
       Get-Process AnyDesk -ErrorAction SilentlyContinue | Stop-Process -Force

  2. UNINSTALL
       AnyDesk.exe --remove (or Settings > Apps)
       Other tools: check Settings > Apps, and Program Files / Program Files (x86)

  3. DELETE THE LEFTOVERS - THIS IS THE IMPORTANT BIT
     The uninstaller leaves these. The config folder is where a saved
     UNATTENDED ACCESS PASSWORD lives - that is what lets them straight back in.
```

```
      Remove-Item "C:\ProgramData\AnyDesk" -Recurse -Force
      Remove-Item "$env:APPDATA\AnyDesk" -Recurse -Force
      Remove-Item "C:\Program Files (x86)\AnyDesk" -Recurse -Force
   Also check:  %LOCALAPPDATA%\AnyDesk, C:\Program Files\AnyDesk

4. REMOVE THE FIREWALL RULES
     Get-NetFirewallRule -DisplayName "*AnyDesk*" | Remove-NetFirewallRule

5. VERIFY - ALL FIVE MUST COME BACK CLEAN
     Get-Service *AnyDesk*              -> nothing
     Get-Process AnyDesk                -> nothing
     netstat -ano | findstr :7070       -> nothing
     Get-NetFirewallRule -DisplayName "*AnyDesk*"   -> nothing
     Test-Path "C:\ProgramData\AnyDesk" -> False

Then re-run the sweep and confirm section 1 and 13b are clean.


================================================================================
```

SCAN IT

```
================================================================================

In this order:

 1. Defender full scan
      Start-MpScan -ScanType FullScan

 2. Malwarebytes Free          https://www.malwarebytes.com/mwb-download
 3. HitmanPro                  https://www.hitmanpro.com
 4. MSERT (Microsoft Safety Scanner) - standalone, no install
 5. KVRT (Kaspersky Virus Removal Tool) - independent third engine
 6. AdwCleaner - browser extensions/hijackers. Good after a remote-access scam.

AUTHORUNS (Sysinternals) - the best "is it really gone" pass. Shows EVERY
autostart location in one list. Set Options > Hide Microsoft entries to cut
the noise to almost nothing.

THREE SCANNERS IS THE LIMIT. Defender + Malwarebytes + one more. More engines
on a normal machine is noise, not safety. Peace of mind comes from the
removal being VERIFIED, not from running more scanners.


================================================================================
THE PART THAT ACTUALLY PROTECTS THE CUSTOMER
================================================================================

Cleaning the PC does NOT get the money back and does NOT remove the thief
from the customer's accounts. Do this from THEIR PHONE, not the PC.

ORDER MATTERS - email FIRST, because every other reset link goes there.

 1. Bank - ring the number ON THE CARD. Ask for the fraud team.
 2. EMAIL - change the password, turn on 2FA, SIGN OUT ALL OTHER DEVICES.
 3. Banking + everything saved in the browser - same treatment.
 4. Turn on 2FA everywhere it is offered.
 5. Check for new payees / saved cards / forwarding rules added to email.
 6. Report: Scamwatch, ReportCyber, and IDCARE (1800 595 160).

*** A STOLEN SESSION COOKIE MEANS THEY ARE ALREADY LOGGED IN. ***
Changing the password alone does NOT kick them out, and 2FA does not stop it.
"Sign out of all other devices" is the step that actually evicts them.

NEVER type a new password on the infected machine. Use her phone or yours.
```

```
================================================================================
  HONEST LIMITS - SAY THESE OUT LOUD
================================================================================

  * YOU CANNOT PROVE WHAT WAS TAKEN. Infostealers exfiltrate and leave
    nothing behind. Finding no loot files proves nothing either way.

  * A CLEAN SCAN IS NOT AN ALL-CLEAR. If the story is unclear, or you find
    persistence you cannot explain, REBUILD IT. Back up data only - never
    AppData, never Downloads, never Program Files.

  * THE SWEEP CANNOT SHOW WHAT WAS MERELY OPENED OR READ. Windows does not
    record that. It shows what was CREATED, INSTALLED, and CHANGED.

  * BROWSER HISTORY gives URLs but not exact visit times (the databases are
    locked while the browser runs). For exact times, check in the browser:
    chrome://history   edge://history


================================================================================
  WHAT YOU CAN HONESTLY SAY TO HER
================================================================================

  "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 is true AND reassuring, because it is accurate. What you can say: the
  remote tool is removed and verified gone, autostart/tasks/services/accounts
  are clean, scans are clean. What you cannot say: "nothing was taken."


================================================================================
  IDCARE - 1800 595 160
================================================================================

  Free Australian service for scam victims. They handle the "what do I do now,
  and how do I stop feeling like an idiot" part. Mon-Fri 8am-5pm.

  Worth knowing about, because the technical job is the easy part. The person
  in front of you has had money taken and will feel stupid about it. That
  happens to thousands of Australians a week and it is not something a script
  fixes.

================================================================================
```