ClickFix for CISOs: How to Stop Running With Scissors

Seven steps to defend the enterprise

flyingpenguin.com · 16 September 2026

The danger of ClickFix is how it exploits user behavior. A user will run with scissors if running is allowed and ClickFix says go faster. Windows ships with three such behaviors allowed that no standard user needs. Close them.

Seven practices. Each has a Do, a How, and a Check an auditor can run in minutes. They apply to the Users OU on physical desktops and to the session host image on VDI and thin-client estates.

1 Disable Run

DO Remove the Run dialog for every standard user.

HOW Group Policy, User Configuration > Administrative Templates > Start Menu and Taskbar > **Remove Run menu from Start Menu**: Enabled. Apply to the Users OU. The same policy removes New Task from Task Manager and blocks UNC paths and drive letters typed into the Explorer address bar; test file-share workflows first.

CHECK As a standard user, Win+R does nothing. `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoRun` returns 0x1.

---

2 Disable Win+X

DO Remove the Win+X terminal shortcut for standard users.

HOW Group Policy Preference, User Configuration > Preferences > Windows Settings > Registry: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`, string value `DisabledHotkeys = RX`. Win+E and Win+D keep working. Confirmed on Windows 10; test on Windows 11 before rollout. The blunt alternative removes every Windows-key combination: User Configuration > Administrative Templates > Windows Components > File Explorer > **Turn off Windows Key hotkeys**: Enabled.

CHECK After sign-out, Win+X does nothing.

---

3 Deny interpreters to standard users

DO Block `powershell.exe`, `pwsh.exe`, `cmd.exe`, `mshta.exe`, `wscript.exe` and `cscript.exe` for the Users group. Allow them to one named group.

HOW AppLocker scopes rules to users and groups: publisher rules, deny on Users, allow on the named group, executable and script collections both enforced, Application Identity service set to Automatic. App Control for Business is the stronger enforcement and is device-wide, so the named group's machines get their own policy. Both run on Pro, Enterprise and Education from Windows 10 version 2004. Two weeks in audit mode, read events 8003 and 8006, then enforce. Remove the PowerShell 2.0 engine: `Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root`.

CHECK As a standard user, `powershell.exe` and `cmd.exe` are refused. In any PowerShell host that still opens, `$ExecutionContext.SessionState.LanguageMode` returns `ConstrainedLanguage`. `Get-WindowsOptionalFeature -Online` shows the V2 engine Disabled.

---

4 Keep the paste warning

DO Leave the Windows Terminal paste warnings on.

HOW Both ship enabled. settings.json: `"multiLinePasteWarning": true` and `"largePasteWarning": true`. No policy exists; a user can turn them off. macOS 26.4 Terminal warns on a pasted command, once per session, with an override.

CHECK Paste two lines into Windows Terminal. The warning appears.

---

5 Log the attempt

DO Enable script block logging and command-line auditing. Ship both to the SIEM.

HOW Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell > **Turn on PowerShell Script Block Logging**: Enabled. Computer Configuration > Administrative Templates > System > Audit Process Creation > **Include command line in process creation events**: Enabled. Advanced Audit Policy > Detailed Tracking > **Audit Process Creation**: Success. Two alerts: `powershell.exe` with `explorer.exe` as parent; `Invoke-RestMethod` piped to `Invoke-Expression`.

CHECK `Microsoft-Windows-PowerShell/Operational` shows Event 4104. Security shows Event 4688 with a command line. A member of the named group pipes `irm` of an internal URL to `iex`; the alert fires within five minutes.

---

6 Name the exceptions

DO Put every account that needs Run, Win+X or an interpreter into the named group.

HOW Ticket, owner, 90-day review, membership change logged.

CHECK The group has an owner and every member has a ticket.

---

7 Train last

DO Tell users a captcha never asks them to press Windows keys or paste into a terminal.

CHECK The phishing simulation includes one ClickFix lure a quarter.

Berlin, August 2026: one paste into Windows Terminal, interpreters open to every user, egress unmonitored, 5.8 terabytes out in five days, 1.44 million files published.

flyingpenguin.com/the-microsoft-click-that-hacked-berlin