NOVEMBER 2026 · AI-AMPLIFIED SOCIAL ENGINEERING

# Stop. Call. Confirm.

AI-amplified social engineering targets human trust: realistic spear-phishing, deepfake impersonation, and ClickFix paste-and-run. Keep this page.

## What is going on

Attackers use AI-written messages and cloned voices to push payments or credentials. ClickFix lures show a fake error or CAPTCHA, copy a command to the clipboard, and tell you to paste it into Windows Run, Terminal, or PowerShell. You become the installer. Microsoft documented ClickFix; MITRE lists it as T1204.004. The FBI IC3 2025 report recorded large AI-related fraud losses, including voice cloning used in payment requests.

## What to do

1. Stop — any urgent or unusual payment, bank-detail, MFA, or paste-this request.

2. Call — a phone number or SoftSol contact you already have. Not the number in the message.

3. Confirm — only act after the real person or SoftSol confirms. Never paste a command to open a file or pass a CAPTCHA. Report unexpected MFA prompts to SoftSol immediately.

## SoftSol contacts

helpdesk.softsol.co.za · support@softsol.co.za · 010 005 0483

## SoftSol tools that support this habit

SoftSol agent / Management Suite — your PC should be enrolled. Martyria — mailbox hijack watch. Titan — titan.softsol.co.za. Aegis — aegis.softsol.co.za. Midas — softsol.co.za/login.

## Sources

Microsoft ClickFix analysis (21 Aug 2025). MITRE T1204.004. FBI IC3 2025 Annual Report.

SoftSol article: https://softsol.co.za/security-briefs/stop-call-confirm

SoftSol · November 2026 · Stop. Call. Confirm.