NOVEMBER 2026 · AI-AMPLIFIED SOCIAL ENGINEERING

Stop. Call. Confirm.

The most common way SoftSol clients get hurt right now is not a clever firewall bypass. It is AI-amplified social engineering: hyper-realistic spear-phishing, deepfake voice or video impersonation, and “ClickFix” lures that trick someone into pasting a malicious command. Attackers aim at human trust — to steal credentials, authorise a payment, or run malware.

Network tools help. They do not replace the habit: **Stop. Call. Confirm.**

What we can stand on

We brief from named public reporting and SoftSol’s operating rules. We do not invent SoftSol client incidents for this page.

ClickFix / paste-and-run

Microsoft Threat Intelligence documented the ClickFix technique: a fake error, CAPTCHA, or “how to fix” prompt that copies a command to the clipboard, then tells the person to open Windows Run, Terminal, or PowerShell and paste. The victim’s own paste-and-enter runs the attack. Microsoft first tracked large campaigns of this style from 2024; MITRE ATT&CK lists the pattern as T1204.004 Malicious Copy and Paste.

A real website, document, or SoftSol process will never ask you to Win+R / paste a command to open a file or prove you are human.

AI writing and deepfake impersonation

The FBI’s 2025 Internet Crime Complaint Center (IC3) annual report recorded more than 22 000 complaints that reported AI-related information, with adjusted losses exceeding US$893 million. It notes AI-generated emails that sound like a CEO, and voice cloning used to request wire payments. Businesses reported more than US$30 million in losses to business-email-compromise scams involving AI in that year.

A message that “sounds exactly like” a director, or a call that “is” their voice, is not proof. Urgency plus secrecy is the tell.

Three rules

1. Stop

Pause on any urgent or unusual ask: pay now, change bank details, share a one-time code, approve MFA you did not start, “fix” a document by pasting a command, or move the chat to a private channel.

2. Call

Use a **secondary channel you already trust** — a phone number or internal chat you already have for that person or for SoftSol. Do not call back a number from the suspicious message. Do not reply in the same thread to “confirm.”

3. Confirm

Only act after the real person or SoftSol confirms the request. Never paste a command into Run, Terminal, or PowerShell because a webpage or attachment told you to. Report unexpected MFA prompts to SoftSol immediately.

How SoftSol makes this practical

- SoftSol agent / Management Suite — managed endpoints so odd paste-and-run activity is not invisible.
- Martyria — mailbox hijack watch after a credential or session steal.
- Titan / Aegis — vault and one-time secrets so panic does not push shared passwords into chat.
- Midas portal — software through SoftSol, not a scare-link.
- M365 session security — related note when the steal is a session rather than a password.

Need help right now? helpdesk.softsol.co.za · support@softsol.co.za · 010 005 0483

Sources

Microsoft Security Blog, 21 August 2025 — Think before you Click(Fix).

https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/

MITRE ATT&CK — T1204.004 Malicious Copy and Paste.

https://attack.mitre.org/techniques/T1204/004/

FBI IC3 2025 Annual Report — AI-related complaints and BEC with AI.

https://www.fbi.gov/file-repository/2025_ic3report.pdf

Prevention, not firefighting. SoftSol monthly security brief — November 2026. Website: https://softsol.co.za/security-briefs/stop-call-confirm