SoftSol · Monthly security brief · November 2026

NOVEMBER 2026 · AI-AMPLIFIED SOCIAL ENGINEERING

Stop. Call. Confirm.

A one-to-two minute security brief for any SoftSol-supported workplace.

This pack is for the person delivering the brief. Read the spoken script once or twice. After you finish, leave the staff handout. Matching website article: softsol.co.za/security-briefs/stop-call-confirm.

Inside

- How to deliver this
- Spoken script (about 100 seconds)
- If someone asks about a 'real' voice or video call
- Leave-behind / staff handout content
- Sources you can stand on

Audience: client-agnostic. No client names in the body.

Angle: AI-amplified social engineering — spear-phishing, deepfake impersonation, and ClickFix paste-and-run — bypasses network tools by targeting human trust. Habit: Stop. Call. Confirm.

1. How to deliver this

Speak it. One line: if the ask is urgent or unusual, do not act in that channel — stop, call a number you already have, confirm, then act. Never paste a command to 'open' a file or CAPTCHA.

- Time: 90 to 110 seconds.
- Tone: calm ops briefing.
- Close: leave the handout. Point people to SoftSol for unexpected MFA or payment pressure.
- Do not pitch products. Titan, Aegis, Martyria, and Midas stay in the leave-behind only.

What we can stand on

Microsoft (21 August 2025) documented ClickFix: fake fix/CAPTCHA prompts that copy a command and tell the user to paste it into Windows Run, Terminal, or PowerShell. MITRE ATT&CK; lists this as T1204.004 Malicious Copy and Paste. The FBI IC3 2025 annual report recorded more than 22 000 AI-related complaints (adjusted losses over US$893 million) and more than US$30 million in business losses to BEC involving AI, including voice cloning for wire requests.

2. Spoken script

Read this as written. About 100 seconds at a normal briefing pace.

This month is Stop. Call. Confirm.

Attackers are not mainly trying to break SoftSol's network edge. They are targeting people: AI-written emails that sound like a director, cloned voices on the phone, and fake 'fix this document' or CAPTCHA screens that tell you to press Win+R and paste a command. That last pattern is called ClickFix. Microsoft and MITRE have documented it. You become the installer.

So three rules. One: Stop on any urgent or unusual ask — payments, bank-detail changes, MFA codes you did not request, or paste-this-to-continue. Two: Call on a secondary channel you already trust — a phone number or SoftSol contact you already have, not the number in the message. Three: Confirm before you act. SoftSol will never ask you to paste a command to open a file or prove you are human. Report unexpected MFA prompts to SoftSol immediately.

I have a short handout with the checks and the sources.

3. If someone asks about a 'real' voice or video

Suggested answer

Sounding or looking real is not enough. AI can clone voices and faces from public video. The control is out-of-band confirmation: hang up, call the person or SoftSol on a number you already have, and only then move money or share access.

4. Leave-behind

Prefer the separate staff handout as the physical leave-behind.

How you prevent it

- Stop — pause urgent/unusual payment, access, MFA, or 'paste this' asks.
- Call — secondary channel you already trust (not the message's callback).
- Confirm — never paste into Run/Terminal/PowerShell because a page told you to; report unexpected MFA to SoftSol.

Tools already behind this brief (do not pitch)

- SoftSol agent / Management Suite — managed endpoints.
- Martyria — mailbox hijack watch.
- Titan / Aegis — vault and one-time secrets.
- Midas portal — software through SoftSol.

5. Sources

Microsoft Security Blog, 21 Aug 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 / BEC with AI.

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

Prepared 10 November 2026 (Africa/Johannesburg). SoftSol print lockup (YOUR IT DEPARTMENT. FULLY MANAGED.) in original colours on white paper. Client-agnostic body text.