SOFTSOL · SEPTEMBER 2026

Your password is someone else's breach

Bank, insurer, KYC-vendor and tracker data is already out this year. Reused passwords and shared passwords turn that into your incident. Keep this page.

What happened

MIP Holdings, June 2026 (reported mid-September). Attackers took roughly 400 000 customer records belonging to about 45 South African insurers from a support platform: emails, cellphone numbers, policy numbers with ID numbers. TechCentral reported that the attackers used credentials an employee had reused on an unrelated service that had already been breached. One reused password opened the door. Hollard later said a dark-web claim naming it appears tied to that third-party MIP incident, not a breach of Hollard's own systems.

Third-party KYC notices, mid-September 2026. EasyEquities, Satrix, Cell C Fibre, Bidvest Bank and others warned customers about a verification-supplier incident. They say their own banking and trading systems were not breached. Identity-verification data held by the supplier may still be exposed. Satrix named RelyComply as the provider used via EasyEquities.

Cartrack, late August 2026. The company confirmed ransomware on 26 August, restored its platform, notified authorities, and later said some customer personal information may have been published by the threat actor. Customers were asked to change Cartrack passwords.

Standard Bank, earlier in 2026. The bank confirmed unauthorised access to some administrative data: names, ID numbers, contact details, account numbers. Core banking systems were not accessed. The bank told clients to use strong unique passwords and never share passwords or PINs by phone, SMS or email.

What this means for you

- A leaked email address plus a reused work password is how credential stuffing opens your mailbox.
- A password in WhatsApp or email is a password anyone with that chat history can use later.
- SoftSol will never ask you to type your password into a message or dictate it on a cold call.
- Fake "security" apps and bank lookalikes still circulate in South Africa. Do not install software from SMS or WhatsApp.

What to do

1. Zero password sharing. Never send a password, PIN, or one-time code by email, WhatsApp, SMS, Teams or Slack. Not to SoftSol. Not to a supervisor. If someone asks, stop. Call SoftSol on a number you already have.

2. No password reuse. Work, bank, shopping and personal sites each get their own passphrase. A bank or KYC leak must not open your Microsoft or vendor login.

3. Strong unique passphrases, stored properly. Prefer a long phrase you can remember, kept in a vault — not a sticky note, not a shared spreadsheet, not a chat with yourself.

SoftSol tools that make this easy

Titan vault — titan.softsol.co.za — store unique passphrases so you do not reuse them.

Aegis one-time secrets — aegis.softsol.co.za — share a password once without leaving it in email or WhatsApp forever.

SoftSol agent / Management Suite — your PC should be enrolled and monitored; ask if you are unsure.

Martyria — SoftSol watches for quiet mailbox hijack signs (hidden forwards, odd mail apps).

Midas portal — softsol.co.za/login — get software through SoftSol, not a link in a scare message.

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

Sources

You do not need these to act. They are here if someone asks where this came from.

TechCentral, 15 Sep 2026. MIP / ~45 insurers / reused credentials. https://techcentral.co.za/customers-45-insurers-exposed-cyber-breach/286139/
Hollard statement, 14 Sep 2026. Third-party MIP attribution. https://pubt.io/view/997DF5C90169B762EC617581735CD71782642D13
TimesLIVE, 15 Sep 2026. EasyEquities / Satrix / RelyComply / Cartrack. https://www.timeslive.co.za/news/sci-tech/2026-09-15-cyberattacks-put-south-africans-personal-data-in-the-spotlight/
Cartrack official notice. https://www.cartrack.co.za/platform/resources/news
Connecting Africa. Cell C / EasyEquities / Bidvest Bank notices. https://www.connectingafrica.com/cybersecurity/sa-s-cell-c-easyequities-and-bidvest-bank-warn-customers-of-data-leak
Standard Bank, 14 Apr 2026. https://www.standardbank.co.za/southafrica/news-and-media/newsroom/an-important-data-incident-update-14-april
Absa CIB on fake apps. https://cib.absa.africa/home/insights-and-events/fake-apps-and-mobile-malware/

SoftSol · September 2026 · Matching website article will appear on softsol.co.za when published (not a live promise in this handout).