SEPTEMBER 2026 · ACCOUNT & CREDENTIAL SECURITY

Your password is someone else's breach

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. A matching SoftSol website article is being prepared separately; do not promise a live URL in the room.

Inside

1. How to deliver this (timing, do and don't)
2. Spoken script (about 100 seconds)
3. If someone asks about sharing passwords with IT
4. Leave-behind style content (also in the staff handout)
5. Sources you can stand on

Audience: client-agnostic. Works for any SoftSol MSP client. No client names in the body.

Angle: bank, insurer, KYC-vendor, and tracker data is already out this year. Reused passwords and shared passwords turn someone else's breach into your incident. Prevention, not firefighting. Plain language.

1. How to deliver this

Speak it. Do not read every source out loud. The story is one line: the password you reused, or the password you emailed to a colleague, is how a vendor or bank leak becomes your company's problem.

- Time: 90 to 110 seconds. If you run long, cut Standard Bank detail, keep MIP (reused credentials) and the three rules.
- Tone: calm ops briefing, not a scare talk. Office, ops, and technical staff.
- Close: leave the staff handout. Point people to SoftSol if they need a vault, a one-time secret link, or help resetting something safely.
- Products: do not pitch. The leave-behind quietly names Titan, Aegis, the SoftSol agent, Martyria, and Midas as the tools already in place.
- Never invent. Distinguish company notices from ransomware leak-site claims.

Keep claims and confirmations apart

Confirmed (company or named executives on the record): MIP Holdings told TechCentral that ~400 000 insurer-customer records were taken in June after attackers used credentials an employee had reused on an unrelated breached service. EasyEquities, Satrix, Cell C Fibre, Bidvest Bank and Peregrine issued mid-September notices about a third-party KYC / verification incident (RelyComply named in some reporting; Satrix named RelyComply). Cartrack confirmed ransomware discovered 26 August 2026 and later said some customer data may have been published. Standard Bank confirmed unauthorised access to some administrative data from late February 2026.

Leak-site / actor claims (not the same as a company notice): The Gentlemen listed Hollard in September; Hollard said its own systems show no compromise and attributes the claim to the MIP third-party incident. Direwolf listed Cartrack and has been reported claiming RelyComply volumes. Treat volumes and dark-web listings as claims until a company or regulator confirms them.

2. Spoken script

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

This month is about the password that already leaked.

In June, attackers got into a support platform at MIP Holdings, a software supplier to roughly forty-five South African insurers. About four hundred thousand customer records came out: emails, cellphone numbers, policy numbers with ID numbers. TechCentral reported this mid-September. The important part for us: the attackers did not break the front door with some exotic exploit. They used a password an employee had reused on an unrelated service that had already been breached. One reused password, and insurer customer data was in play.

Closer to this week. EasyEquities, Satrix, Cell C Fibre, Bidvest Bank and others wrote to customers about a third-party KYC verification incident. Their own trading and banking systems, they say, were not breached. The data sitting with the verification supplier may still be. Cartrack confirmed ransomware at the end of August and asked customers to change passwords. Earlier this year Standard Bank confirmed some client names, ID numbers and account numbers out of administrative systems. That is fuel for phishing and credential stuffing.

So three rules for us. One: never share a password by email, WhatsApp, SMS, or chat. Not with a supervisor, not with SoftSol, not with anyone who phones claiming to be IT. SoftSol will never ask you to type your password into a message. Two: never reuse a work password on a bank, shop, or personal site. Three: store strong unique passphrases in a proper vault, and if you must hand someone a secret once, use a one-time link, not a chat thread.

If mail looks off, or someone asks you for a password, stop and tell SoftSol. I have a short handout with the checks and the sources.

3. If someone asks about sharing passwords with IT

Suggested answer

No. SoftSol will never ask you to email, WhatsApp, or SMS a password, PIN, or one-time code. Neither should a supervisor. If someone claiming to be SoftSol or your manager asks for a password in a message or on a call you did not start, hang up and use the SoftSol contacts you already have.

If SoftSol needs to help with a login, we reset or walk you through a secure path. We do not collect your existing password in chat. For handing a secret to a colleague once, use a one-time secret link (Aegis), not a WhatsApp thread that lives forever.

If you already sent a password in chat, change it now on every place you reused it, then tell SoftSol so we can check for follow-on mailbox or account abuse.

4. Leave-behind: for every user

The rest of this document can be circulated. Prefer the separate two-page staff handout as the physical leave-behind.

What happened, that we can stand on

MIP Holdings / The Gentlemen, June 2026 (reported 15 September 2026). TechCentral interviewed MIP CEO Richard Firth. Intruders spent about three weeks in a support (Atlassian) platform being decommissioned. Roughly 400 000 records affecting customers of about 45 insurers (mostly life) were copied: email addresses, cellphone numbers, policy numbers with identity numbers, a small number of residential addresses. Core administration systems were not touched. Root cause on the record: credentials reused by an employee on an unrelated service that had itself been breached, then used from a personal laptop to reach the support platform. MIP reported paying a substantial ransom for a destruction undertaking; The Gentlemen later listed Hollard on a leak site (7 September). Hollard's 14 September statement: no evidence of compromise inside Hollard's environment; claim appears attributable to the June MIP third-party incident.

Third-party KYC / verification notices, mid-September 2026. Bidvest Bank, Cell C Fibre, EasyEquities, Satrix and Peregrine issued customer notices about a cybersecurity incident at a third-party verification / KYC provider. EasyEquities and Satrix stressed their own systems and investment platforms were not compromised; potentially affected data is identity-verification information. Satrix named RelyComply as the verification provider used via EasyEquities. Cell C described Fibre-related fields such as names, emails, mobile numbers and Fibre account numbers. Company notices remain the primary source; treat ransomware-group volume claims as unverified.

Cartrack South Africa, ransomware discovered 26 August 2026. Cartrack's published notice: ransomware on certain systems; platform restored; investigation ongoing; authorities including the Information Regulator notified. Later update: personal information relating to certain customers may have been published on a restricted-access threat-actor site; customers prompted to update Cartrack passwords. Direwolf listed Cartrack Holdings on leak-site trackers around 2 September — that listing is an actor claim; Cartrack's own notice is the confirmation to brief.

Standard Bank, late February – April 2026. Official updates: unauthorised access to internal administrative and document filing systems. Names, ID or registration numbers, contact details and account numbers among affected fields; core transactional banking not accessed. Bank advised clients to use strong unique passwords and never share passwords or PINs by phone, SMS or email.

Fake apps / credential theft (ongoing SA pattern). Absa CIB has warned that fake apps lure people into enrolling biometrics or banking credentials. SABRIC's 2025 crime statistics (published 2026) show digital banking crime driven mainly by social engineering and customer compromise, not by banks' core systems being hacked. Useful context for "do not install from a message."

Why this becomes your incident

Leaked emails, ID numbers and phone numbers do not open your Microsoft 365 tenant by themselves. Reused passwords, shared passwords, and phished one-time codes do. Credential stuffing tries yesterday's bank or shop password against today's work login. Shared passwords in chat mean one compromised phone compromises the whole team. A password emailed "just this once" is forever in someone's mailbox archive.

- **Reuse.** MIP's own account of the insurer-data theft starts with an employee password reused on an unrelated breached service.
- **Sharing.** Anyone who can read the chat can become "you" on that system. SoftSol will never ask for your password in a message.
- **Weak or memorable-only secrets.** Short passwords and family names fail against stuffing and guessing once your email is on a leak list.
- **Mailbox follow-on.** Stolen credentials often lead to hidden mail forwards and lookalike "IT" messages. That is how one account becomes a company-wide phish.

How you prevent it

1. Zero password sharing. Never send a password, PIN, or OTP by email, WhatsApp, SMS, Teams, or Slack. Not to SoftSol. Not to a supervisor. If someone asks, stop and verify out-of-band.

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

3. Strong unique passphrases, stored properly. Long memorable phrases beat short clever passwords. Keep them in a vault, not a notebook next to the screen and not a shared spreadsheet.

The tools already behind this brief (do not pitch — just know they exist)

After a wave of SA data incidents, most organisations tell staff to "be careful" and stop there. SoftSol's quieter stack for credentials:

1. Titan vault (titan.softsol.co.za): store strong unique passphrases so people do not reuse or write them on sticky notes.
2. Aegis one-time secrets (aegis.softsol.co.za): hand a password or API key to someone once, without leaving it forever in email or WhatsApp.
3. SoftSol agent / Management Suite enrollment: the machine in front of you is actually managed, so weak local habits and missing agents get caught.
4. Martyria: watch mailboxes for the quiet signs of hijack (hidden forwards, odd mail apps) while Outlook still looks normal.
5. Midas portal (softsol.co.za/login): software and tools come through SoftSol, not a link in a "security alert" message.

If you want those checks done rather than described, ask the person who sent you this pack. Helpdesk: helpdesk.softsol.co.za · support@softsol.co.za · 010 005 0483

5. Sources you can stand on

Primary or contemporaneous public sources. Do not treat ransomware leak-site volumes as confirmed. Do not invent client-specific impact.

TechCentral, 15 September 2026. MIP Holdings / ~45 insurers / ~400 000 records; reused credentials root cause; The Gentlemen. https://techcentral.co.za/customers-45-insurers-exposed-cyber-breach/286139/

Hollard statement, 14 September 2026 (via Public). No evidence of Hollard environment compromise; claim attributed to June MIP third-party incident. https://pubt.io/view/997DF5C90169B762EC617581735CD71782642D13

LegalWise notice (MIP third party), 6 July 2026. Example insurer/operator customer notice pointing at MIP.
https://legalwise.co.za/articles/important-update-regarding-a-third-party-cybersecurity-incident

TimesLIVE, 15 September 2026. EasyEquities / Satrix (RelyComply named) and Cartrack customer-data risk.
https://www.timeslive.co.za/news/sci-tech/2026-09-15-cyberattacks-put-south-africans-personal-data-in-the-spotlight/

Cartrack official news notice. Ransomware 26 August 2026; later note on possible publication of personal information; password updates.
https://www.cartrack.co.za/platform/resources/news

Connecting Africa, September 2026. Cell C Fibre, EasyEquities, Bidvest Bank third-party notices.
https://www.connectingafrica.com/cybersecurity/sa-s-cell-c-easyequities-and-bidvest-bank-warn-customers-of-data-leak

Standard Bank incident update, 14 April 2026.
https://www.standardbank.co.za/southafrica/news-and-media/newsroom/an-important-data-incident-update-14-april

Absa CIB: fake apps and mobile malware. https://cib.absa.africa/home/insights-and-events/fake-apps-and-mobile-malware/

SoftSol. https://softsol.co.za/ · Titan: https://titan.softsol.co.za/ · Aegis: https://aegis.softsol.co.za/ · Portal: https://softsol.co.za/login

Prepared 16 September 2026 (Africa/Johannesburg). Light layout for print. SoftSol logo used in its original blue-on-white colours from the registered artwork, not recolored. Client-agnostic body text.