ASP MOVEMENT

ALL SHALL PROSPER

ASP Trends

Cyber Security Hardening Basics | A Practical Guide for South African Businesses in 2026

Before We Begin: About That Download

You just downloaded this file. Stop and think about why you felt safe doing it: you were reading an article on a website you know and trust, you navigated there yourself, and the download was clearly described. That was reasonable, safe behaviour — and you did nothing wrong.

> **Here's the uncomfortable part:** cyber criminals succeed by counterfeiting exactly this kind of trust. A convincing email that looks like it came from your bank, a fake invoice from a "supplier", a link shared by a colleague whose account has been hijacked — the attack works because it feels like this download felt. This guide is about learning to tell the difference.

Why Small Businesses Are Prime Targets

There is a persistent myth that cyber criminals only chase banks and big corporates. In reality, small and medium businesses are attacked constantly — precisely because they hold valuable data (customer details, banking information, invoices) but rarely have dedicated IT security staff. South Africa consistently ranks among the most targeted countries on the continent for phishing and ransomware.

The encouraging news: the overwhelming majority of successful attacks exploit basic weaknesses — weak passwords, unpatched software, and human trust. Fixing the basics eliminates most of your risk, and almost none of it requires an enterprise budget.

1. Passwords and Multi-Factor Authentication

The single biggest win

Stolen and reused passwords remain the most common way into a business. If you do only one thing after reading this guide, do this:

- **Use a password manager** (Bitwarden, 1Password, or similar) so every account has a long, unique password you never have to remember.
- **Turn on multi-factor authentication (MFA)** everywhere it is offered — email first, then banking, then everything else. An authenticator app is stronger than SMS codes.
- **Never reuse passwords** between accounts. One breached website should never unlock your email.

Author Details:

Nikolai Lombaard | Technical Director, ANTI.Social Collective (Pty) Ltd | +2773 409 7444 | nikolai@antisocialcreative.com

- **Protect your email account above all.** Whoever controls your email can reset the passwords to everything else.

2. Keep Everything Updated

Software updates are not just new features — they patch security holes that criminals actively scan for. Attackers routinely exploit vulnerabilities that were fixed months or years earlier, counting on businesses that never updated.

- Enable **automatic updates** on Windows, macOS, phones, and browsers.
- Update **routers and Wi-Fi equipment** — the forgotten devices are the vulnerable ones.
- If you run a website (especially WordPress), keep the **core, themes, and plugins** updated, and remove plugins you no longer use.
- Retire software and systems that no longer receive security updates

3. Phishing: Recognising Counterfeit Trust

Remember the download at the start of this guide? Phishing is the criminal imitation of that moment of trust. Most breaches begin with a message designed to make you click, download, or hand over credentials without thinking.

Warning signs

- **Urgency and pressure:** "Your account will be suspended in 24 hours." Legitimate organisations rarely threaten you into immediate action.
- **Unexpected attachments or links** — even from people you know. Hijacked accounts send convincing messages to everyone in the contact list.
- **Mismatched details:** hover over links before clicking and check the sender's actual email address, not just the display name.
- **Requests for credentials or payment changes:** no legitimate supplier changes banking details via a casual email.

The golden rule

> **Verify through a separate channel.** If an email claims to be from your bank, phone the bank using the number on your card — not the number in the email. If a supplier asks you to change payment details, call the person you know at that company. Thirty seconds of verification defeats almost every phishing attack.

4. Backups: Your Ransomware Insurance

Ransomware encrypts your files and demands payment to unlock them. A tested backup turns a business-ending crisis into an inconvenient afternoon.

Author Details:
Nikolai Lombaard | Technical Director, ANTI.Social Collective (Pty) Ltd | +2773 409 7444 | nikolai@antisocialcreative.com

ASP Trends

- Follow the **3-2-1 rule**: three copies of your data, on two different types of storage, with one copy off-site (cloud or a drive kept elsewhere).
- Keep at least one backup **disconnected** from your network — ransomware encrypts connected backup drives too.
- **Test your restores**. A backup you have never restored from is a hope, not a plan.

5. Devices, Networks, and Everyday Habits

- Use **screen locks** and full-disk encryption (BitLocker / FileVault) on all laptops and phones.
- Give staff **standard user accounts**, not administrator rights, for daily work.
- Change the **default password on your router** and use WPA2/WPA3 with a strong Wi-Fi passphrase; run a separate guest network for visitors.
- Be cautious on **public Wi-Fi** — avoid banking and sensitive logins, or use a reputable VPN.
- **Remove access immediately** when staff leave — email, cloud accounts, shared passwords, and website logins.
- Only install software from **official sources**, and be sceptical of "free" versions of paid tools.

6. Protecting Customer Data (and POPIA)

Under the Protection of Personal Information Act (POPIA), South African businesses have a legal duty to safeguard the personal information they hold, and to report breaches to the Information Regulator and affected individuals. Beyond compliance, a data breach destroys the customer trust that small businesses depend on.

- Collect and keep only the personal data you genuinely need.
- Limit who in your business can access customer information.
- Use encrypted, reputable services for storing and sending sensitive documents.
- Know who to call — your IT provider, your bank, your insurer — *before* an incident happens.

7. Social Media: Own Your Digital Assets

For many SMMEs, social media starts informally: an employee, freelancer, or "someone who understands social media" quickly sets up the Facebook Page, Instagram account, or Google Business Profile — often under their own personal email address or profile. It seems harmless. Then that person leaves, the relationship changes, or their account is hacked, and the business discovers it doesn't actually control its own public voice.

Your social media pages are not just marketing tools — they are business assets holding brand equity, customer conversations, reviews, followers, and advertising history. Losing access can mean losing customer enquiries, credibility, and in the worst case, watching an unauthorised person post in your company's name.

Ownership and access

Author Details:
Nikolai Lombaard | Technical Director, ANTI.Social Collective (Pty) Ltd | +2773 409 7444 | nikolai@antisocialcreative.com

ASP Trends

- **The business must own the account** — never an employee's or supplier's personal email or profile. Know which email address, recovery number, and MFA device is attached to every account.
- **At least two trusted senior people** (directors, owners, or senior managers) should hold full administrator access, so the business never depends on a single person.
- **Never share the main username and password.** Shared logins let anyone change the password, recovery details, or MFA — and destroy accountability, since nobody knows who posted or changed what.
- **Use each platform's business tools instead:** Meta Business Suite (Facebook/Instagram), LinkedIn Page admin roles, YouTube channel permissions, Google Business Profile owners and managers, TikTok Business Center, and X Delegate all let you grant people their own access at the right level — without handing over a password.

Simple governance

- Give freelancers, agencies, and staff **only the access they need** to do their work.
- **Review access regularly,** and remove it immediately when someone leaves or a supplier changes.
- Keep a **secure internal record** of every platform: who owns it, which email is attached, and who has access.

> **The principle is simple:** employees, freelancers, and agencies can all be given access to help manage social media — but ownership must sit with the business. Social media security is not a marketing issue; it is a business continuity issue.

The 15-Minute Hardening Checklist

Work through this list with your team. Every box ticked meaningfully reduces your risk.

- ☐ MFA enabled on all email accounts
- ☐ Password manager in use; no reused passwords
- ☐ Automatic updates enabled on all computers and phones
- ☐ Router default password changed; guest Wi-Fi separated
- ☐ Website CMS, themes, and plugins up to date
- ☐ 3-2-1 backups in place, with one copy offline
- ☐ Backup restore tested in the last 3 months
- ☐ Staff briefed on phishing and the “verify through a separate channel” rule
- ☐ Payment detail changes always confirmed by phone
- ☐ Screen locks and disk encryption on all devices

ASP MOVEMENT

ALL SHALL PROSPER

Author Details:

Nikolai Lombaard | Technical Director, ANTI.Social Collective (Pty) Ltd | +2773 409 7444 | nikolai@antisocialcreative.com

- [ ] Staff use standard (non-admin) accounts day to day
- [ ] Leaver process removes all access on the last day
- [ ] Customer data access limited to those who need it
- [ ] Social media accounts owned by the business, not personal profiles
- [ ] At least two senior administrators on every social platform
- [ ] Platform business tools used instead of shared logins
- [ ] Internal record kept of every account, its email, and who has access
- [ ] Incident contacts (IT, bank, insurer) written down and accessible

A Final Word

Cyber security is not about paranoia or expensive tools — it is about habits. The download that opened this guide was safe because of context: a trusted site, a clear source, your own deliberate action. Bring that same deliberateness to every email, link, and attachment, get the basics above in place, and your business will be harder to attack than the vast majority of its peers. Criminals are opportunists — they move on to easier targets.

About the Authors

Nikolai Lombaard and **Lynette Lombaard** are the co-owners and directors of **ANTI.Social Collective (Pty) Ltd**, a Durban-based creative, technology and AI systems partner supporting clients across South Africa, the United Kingdom, the United States and other international markets.

Nikolai serves as Technical Director, with extensive experience in software development, systems architecture, integrations, automation and digital infrastructure. Lynette serves as Strategic Director, with a strong background in business strategy, positioning, communication, user experience and digital governance.

Through ANTI.Social Collective, they help growing businesses align brand, technology and operations so their digital assets are more effective, better governed and built to scale.

Author Details:
Nikolai Lombaard | Technical Director, ANTI.Social Collective (Pty) Ltd | +2773 409 7444 | nikolai@antisocialcreative.com