Personal Data & Digital Safety Guide

Understanding Online Risks, Protecting Your Identity & Practicing Safe Web Habits

1. Why Digital Safety Matters

Most South Africans now access the internet through **mobile phones**, but many still use **laptops and PCs** for work, job applications, online learning, and finances.
This makes strong digital safety habits essential across *all* devices.

Cybercrime in South Africa is rising every year. Common risks include:

- Identity theft
- Banking fraud
- SIM-swap attacks
- Phishing links
- Fake investment scams
- Device hacking
- Data leaks

Staying informed and practicing safe habits protects your money, your career, and your personal identity.

2. Common Online Risks

2.1 Phishing

Messages pretending to be from banks, SARS, or companies asking you to click a link or provide details.
Can happen on:

- WhatsApp
- SMS
- Email
- Social media

Signs of phishing:

- Urgent language (“Your account will be closed!”)
- Unofficial email addresses
- Incorrect spelling or grammar
- Requests for passwords or OTPs

2.2 SIM-Swap Fraud

Criminals clone your SIM card by doing a sim-swap to receive your bank OTPs.

Warning signs:

- Suddenly no network signal
- Phones calls or SMSes from unknown “customer support”
- SIM stops working for no reason

2.3 Fake Job, Loan & Investment Scams

Common tactics:

- “Pay a fee to secure an interview.”
- Telegram/WhatsApp “trading gurus.”
- Fake recruitment offers requesting copies of ID, bank statements, or photos.

2.4 Unsafe Public Wi-Fi

Using free Wi-Fi can expose:

- Banking logins
- Email passwords
- Social media accounts

Hackers can intercept data on shared networks.

2.5 Malware & Spyware

Downloaded through:

- Fake apps
- Torrented movies/software
- Unsafe websites
- USB drives (especially at work)

These can steal:

- Passwords
- Banking details
- Stored documents

3. Protecting Your Personal Identity

3.1 Strengthen Your Passwords

Use long, unique passwords with:

- Capital letters
- Numbers
- Symbols

Avoid using:

- Date of birth
- Child’s name

- Partner’s name
- “12345” or “password”

Use a **password manager** where possible.

3.2 Activate Multi-Factor Authentication (MFA)

Turn on OTP or app-based authentication for:

- Email
- Banking
- Social media
- Work accounts

This prevents criminals from accessing accounts even if they guess your password.

3.3 Be Careful What You Share Online

Avoid posting:

- ID photos
- Bank cards
- Boarding passes
- Address
- Workplace details

Criminals can collect small pieces of info and build your identity.

4. Safe-Web Habits for Everyday Users

4.1 Verify Links Before Clicking

Always check:

- Website spelling
- The lock symbol (HTTPS)
- If the message is from an official source

If unsure: **DO NOT CLICK.**

4.2 Avoid Downloading Unknown Files

Only download from:

- Official app stores
- Verified company websites
- Trusted email senders

Never download:

- “Cracked” software
- Free movies or programs
- Attachments from strangers

4.3 Update Your Devices Regularly

Updates patch security holes.

Mobile:

- Keep your Android/iOS updated
- Update banking apps
- Remove unused apps

Laptop/PC:

- Update Windows/macOS
- Update browsers and antivirus

4.4 Use Antivirus Software (PC & Mobile)

Good software protects you from:

- Malware
- Ransomware
- Keyloggers
- Unsafe websites

Recommended (free or paid):

- Bitdefender
- Kaspersky
- ESET
- Windows Defender (PC built-in)

4.5 Be Cautious With USB Drives

Especially for mine-sector workers using shared computers.

Risks:

- Malware
- Worms spreading across networks

Tips:

- Scan USBs before opening
- Avoid unknown flash drives
- Don’t plug personal drives into work computers

5. Mobile Device Safety

Most South Africans bank using mobile phones — which makes them a prime target.

5.1 Lock Your Phone

Use:

- PIN
- Fingerprint
- Face unlock

Avoid simple codes like 1111 or 0000.

5.2 App Permissions

Some apps request access to:

- Contacts
- Photos
- Camera
- Location
- Microphone

If unnecessary, deny permissions.

5.3 Protect Your SIM Card

Activate:

- SIM PIN
- Network provider's fraud alerts

5.4 Avoid Using Banking Apps on Public Wi-Fi

Rather use:

- Mobile data
- A personal hotspot
- A trusted home/work network

5.5 Beware of Fake Apps

Happens often to Android users.

Only download from:

- **Google Play Store**
- **Apple App Store**

Never download apps from:

- Random websites
- Telegram links
- WhatsApp "APK" files

6. Laptop & PC Safety

6.1 Keep Antivirus & Firewall On

Never disable your firewall.
Run regular virus scans.

6.2 Use Verified Software Only

Avoid installing:

- Cracked programs (fake copies of programs or Apps not verified on the Google play store or Apple Appstore)
- Free key generators
- Unknown software from torrents

These often contain malware.

6.3 Browser Safety

Use secure browsers:

- Chrome
- Firefox
- Edge

Add extensions like:

- AdBlock
- Password managers
- Malware-blocking tools

6.4 Secure Your Wi-Fi Router

Change the default password.
Enable WPA2 or WPA3 encryption.

7. Safe Online Banking

7.1 Tips for Secure Banking

- Never share your OTP
- Never approve unknown app login requests
- Use banking apps instead of browser banking
- Check your account activity weekly

7.2 Warning Signs of Fraud

- Unexplained debits
- Unknown devices linked to your banking profile
- Sudden lack of mobile network signal (possible SIM swap attack)

7.3 What To Do If You Suspect Fraud

Immediately:

1. Contact your bank

2. Freeze your cards or account
3. Change your passwords
4. Report the incident to SAPS
5. Inform your mobile network

8. Workplace Digital Safety (Mine & Industrial Workers)

Mine- and construction-sector workers often use:

- Shared office computers
- Public Wi-Fi
- USB drives
- Company email accounts

Safety Tips

- Always log out of systems
- Never save banking passwords on shared computers
- Do not plug personal devices into work machines
- Confirm emails from HR before opening attachments
- Report anything suspicious to IT or your supervisor immediately

9. Summary of Best Practices

✓ Use strong, unique passwords
✓ Enable multi-factor authentication
✓ Keep apps and devices updated
✓ Avoid clicking unknown links
✓ Protect your SIM card
✓ Use antivirus on PC and phone
✓ Avoid public Wi-Fi for banking
✓ Be careful with USB devices
✓ Think before you share personal information online