EMERGENCY PREPAREDNESS FOR SOUTH AFRICA

CIVIL UNREST & DIGITAL PREPAREDNESS

THINK AHEAD. STAY INFORMED. STAY HOME IF NEEDED. STAY SAFE ONLINE.

UNDERSTAND THE RISK

Civil unrest can happen quickly and escalate fast. Preparation is about awareness, decisions and discipline.

- Protests can turn violent.
- Looting can spread quickly.
- Services (power, transport, banks, networks) may be disrupted.
- Police and emergency services may be stretched.
- Misinformation can create panic and poor decisions.

WARNING SIGNS TO WATCH FOR

- Large gatherings or protests announced
- Increased rumours, tension or hate speech online
- Service delivery protests and shutdown threats
- Transport disruptions and road block warnings
- Panic buying or sudden stock shortages
- Visible police / military deployment in your area
- Court rulings or political events likely to trigger unrest
- Internet or social media restrictions or outages

STAYING HOME: YOUR BEST OPTION

- Avoid unnecessary travel.
- Stay informed, not anxiously online.
- Close and lock all doors and windows.
- Keep family and pets safe and calm.
- Have food, water, first aid and lighting ready.
- Keep a low profile and avoid confrontation.

When in doubt, stay home. Stay safe.

DIGITAL SECURITY – PROTECT YOURSELF ONLINE

Your devices hold your life. Protect your data. Protect your future.

SECURE YOUR ACCOUNTS

- Use strong, unique passwords.
- Enable 2FA (two-factor authentication) on all important accounts.
- Use a password manager or secure storage.
- Review account recovery options regularly.

Weak passwords open doors. Strong habits keep you safe.

LIMIT WHAT YOU SHARE

- Don't post your location, plans, travel or valuables.
- Avoid real-time updates during unrest.
- Be careful what you share about your family, work, or routine.
- Think before you post or forward.

Less information shared = less risk to you and your family.

PROTECT YOUR IDENTITY

- Guard your ID number, bank details and personal information.
- Shred documents with personal data.
- Be cautious when sharing online forms.
- Monitor your credit report when possible.

Your identity is valuable. Protect it like cash.

SECURE YOUR DEVICES

- Keep devices and apps updated.
- Use antivirus and firewalls.
- Lock devices with PIN, fingerprint or face ID.
- Encrypt important files and backups.

A secure device protects your data and your privacy.

STAY CONNECTED SAFELY

- Use trusted networks.
- Avoid public Wi-Fi for banking.
- Use a VPN when necessary.
- Back up important data offline and in the cloud.

Good connections are powerful. Stay secure.

IDENTITY RISK & MODERN EXPOSURE

Identity theft can happen anywhere – online or offline.

- Phishing scams via email, SMS, WhatsApp & social media
- Fake websites and payment links
- Shoulder-surfing and card skimming
- Data breaches and leaked personal information
- Scammers using fake news, urgency and emotion.

REDUCE YOUR RISK

- Don't click unknown links or open strange attachments.
- Verify requests directly with the organisation.
- Use virtual cards for online payments.
- Check privacy settings on social media.
- Remove old accounts and limit stored data.
- Monitor for suspicious activity and report it.

Scammers rely on information. Take it away.

DURING UNREST – WHAT TO DO

STAY INDOORS	STAY INFORMED	KEEP LIGHTS LOW	KEEP SECURE	SUPPORT EACH OTHER	BE READY
It's safest to stay home and avoid unnecessary movement.	Use trusted news sources. Avoid rumours and social media panic.	At night, use minimal lighting. Don't draw attention.	Lock all entry points, gates and garages.	Check on neighbours. Share information and look out for the vulnerable.	Keep essentials ready: water, food, first aid, cash, radio, power.

IF YOU MUST TRAVEL

- Know your route and avoid hotspots.
- Travel during safer times.
- Keep fuel in your tank.
- Stay aware – avoid headphones and distractions.
- If you feel unsafe, leave the area calmly and immediately.

IF CAUGHT IN UNREST

- Avoid crowds and remain calm.
- Don't film or take photos.
- Move away from the area if possible.
- Follow instructions from authorities.
- Get to a safe location.

COMMUNICATION PLAN

- Agree on check-in times and methods.
- Have backup ways to contact family.
- Keep important numbers written down.
- Use encrypted messaging apps where possible.

BUILD RESILIENCE OFFLINE

- Know your community.
- Build trusted relationships.
- Have cash available.
- Keep important documents safe and backed up.
- Practice your family plan.

KEY REMINDERS

PREPARE · INFORM · PROTECT · RESPOND

"AWARENESS TODAY. PREPARATION TODAY. SAFETY TOMORROW."

USEFUL CONTACTS (SAVE OFFLINE)

- SAPS Emergency: 10111
- Fire & Rescue: 10177
- Ambulance: 10177
- Disaster Management: 080 911 4357
- Childline: 116
- Fraud Hotline (SAPS): 0800 20 50 26

STRONG FAMILIES.
STRONG COMMUNITIES.
A SAFER SOUTH AFRICA.

STAY AWARE. STAY PREPARED. STAY TOGETHER. THINK. PLAN. PROTECT.

19 CIVIL UNREST AND RIOTS

Nine Days That Shook South Africa

Mail & Guardian / ACCORD / Expert Panel Report — July 2021

It began quietly enough. On the evening of 9 July 2021, a handful of supporters of former President Jacob Zuma gathered near his homestead in Nkandla, KwaZulu-Natal. Zuma had just begun serving a 15-month prison sentence for contempt of court. By the following morning, burning tyres blocked the N3 highway. By the end of the week, South Africa was on fire.

What followed was the worst civil unrest this country had experienced since the end of apartheid. For nine days — from 9 to 17 July 2021 — KwaZulu-Natal and Gauteng descended into chaos. Shopping malls were stripped bare and set alight. Warehouses, factories and distribution centres were gutted. Trucks were hijacked and burned on the highways. The ports of Durban and Richards Bay ceased operations entirely.

The numbers tell a story that is almost impossible to comprehend:

- *354 people lost their lives*
- *3 000 stores were looted*
- *61 shopping malls were damaged or destroyed*
- *11 warehouses and 8 factories were extensively damaged*
- *40 000 businesses and 50 000 informal traders were affected*
- *150 000 jobs were immediately placed at risk*
- *50 billion was wiped from the South African economy*
- *25 000 army troops were eventually deployed to restore order*

In KwaZulu-Natal alone, R20 billion worth of stock was lost. In Durban, R1.5 billion of stock disappeared in a matter of days. Shoprite alone reported that 200 of its stores had been looted, vandalised or burned across the two provinces.

The impact extended far beyond the immediate destruction. Supply chains collapsed. Food shortages spread through the affected provinces. Pharmacies were looted — including those holding COVID-19 vaccines, at the height of South Africa's third wave. Banking branches closed across KZN and Gauteng. Ordinary families who had done nothing wrong could not buy food, could not access cash and could not move safely through their own neighbourhoods.

President Cyril Ramaphosa called it an attempted insurrection. The Expert Panel appointed to investigate described the period as an "orgy of destruction and looting" and found that the violence was well-orchestrated and deliberately planned — designed to make the country ungovernable.
But here is the most sobering finding of all. In the communities worst affected, families that had prepared — that had food in the house, cash at home, fuel in the tank and a plan for staying safe — survived those nine days with far less trauma than those who had not. The shops were empty. The ATMs were offline. The roads were dangerous. For the unprepared family, those nine days were a genuine crisis of survival.

For the prepared family, they were simply nine very difficult days spent safely at home.
"The glue that held communities together was shaken. Citizens felt abandoned by the State."

— Report of the Expert Panel into the July 2021 Civil Unrest, November 2021

South Africa has a long and complex history of civil unrest. From service delivery protests that block roads and burn tyres, to large-scale riots that engulf entire cities — as we witnessed during the July 2021 unrest — civil unrest is one of the most distinctly South African emergency scenarios that this guide must address.

What makes civil unrest particularly dangerous is its unpredictability. It can escalate from a localised protest to a city-wide crisis within hours. Supply chains collapse almost immediately. Shops are looted and closed. Roads become impassable or dangerous. Police and emergency services are overwhelmed. And ordinary families who were completely unprepared find themselves trapped — unable to buy food, unable to travel and unable to get help.

The good news is that the preparation you have already done throughout this guide — your food and water storage, your communication alternatives, your evacuation plan and your community network — is exactly what you need to survive a period of civil unrest.

19.1 UNDERSTANDING THE PHASES OF CIVIL UNREST

19.1.1 PHASE 1 — WARNING SIGNS

Unrest rarely erupts without warning. The signs are usually visible days or even weeks before violence breaks out — growing social media tension, protest announcements, political speeches that inflame public anger, service delivery grievances that have gone unaddressed. Pay attention to local news, community WhatsApp groups and neighbourhood watch communications. If tensions are rising in your area, begin quietly activating your emergency preparations without waiting for things to deteriorate further.

19.1.2 PHASE 2 — LOCALISED DISRUPTION

Road blockages with burning tyres, isolated incidents of looting, sporadic violence in specific areas. This is the time to fill your fuel tank, withdraw cash, top up your food and water supplies and make sure your family knows the emergency plan. Do not leave this until Phase 3.

19.1.3 PHASE 3 — WIDESPREAD UNREST

Violence has spread across a wider area. Roads are dangerous or impassable. Shops are closed or looted. Emergency services are overwhelmed. At this stage your priority is to stay home, stay safe and rely on your preparations.

19.1.4 PHASE 4 — STABILISATION

Security forces restore order and the immediate danger begins to recede. Even at this stage caution is warranted — sporadic incidents can continue and supply chains take time to recover.

19.2 IMPORTANT RULES

19.2.1 THE GOLDEN RULE — STAY HOME

The single most important principle during civil unrest is this: *stay home*. The vast majority of people who are injured or killed during civil unrest are those who went out unnecessarily, to watch what was happening, to try to reach a family member, to get supplies they should have already had, or simply because they underestimated the danger. Curiosity and complacency kill.

19.2.2 BEFORE UNREST REACHES YOUR AREA

- **Fill your fuel tank** and if possible, fill your reserve fuel containers.
- **Withdraw cash in small denominations**. ATMs are among the first things that become inaccessible during unrest.
- **Top up your food and water supplies**. Shops close within hours of unrest beginning and may remain closed for days or weeks.
- **Charge all devices** — phones, power banks, radios and torches.
- **Communicate with your family**. Make sure every member knows the plan and has emergency contacts memorised.
- **Activate your community network**. Contact trusted neighbours and establish a communication protocol.
- **Secure your property**. Close and lock all gates, doors and windows. Bring valuable items inside or behind secured gates.
- **Prepare your self-defence measures** as discussed in the Safety and Security chapter.

19.2.3 DURING ACTIVE UNREST

- **Stay informed without exposing yourself.** Monitor local news, community WhatsApp groups and social media carefully. Follow official SAPS and municipal accounts for updates.
- **Keep a low profile.** Do not draw attention to your home or your preparations. Do not post on social media about what supplies you have. Discretion is a form of security.
- **Do not engage with crowds or confrontations.** If unrest reaches your street, do not go outside to confront anyone or to protect property at the cost of your personal safety. No physical possession is worth your life.
- **Coordinate with trusted neighbours.** A street that is organised and communicating is significantly safer than a street of isolated households. Share information and watch out for each other.

19.2.4 IF YOU ARE CAUGHT OUTSIDE DURING UNREST

- **Do not drive towards the unrest** - Turn around immediately and find an alternative route home or to a place of safety.
- **Avoid main roads and shopping centres** — these are the most common flashpoints during unrest.
- If your vehicle is surrounded by a crowd, **remain calm**. Keep your doors locked and windows up. Do not make sudden movements or aggressive gestures.
- If you cannot get home safely, **go to the nearest place of safety** — a police station, a hospital, a church or the home of a trusted person.
- **If you are on foot**, move calmly and purposefully away from the unrest. Do not run. Find shelter as quickly as possible.

19.2.5 AFTER THE UNREST

- **Do not rush outside** the moment things seem quiet. Situations can reignite quickly.
- **Assess your supplies and determine what you need to replenish**. Expect shortages and higher prices in the weeks following significant unrest.
- **Document any damage to your property** thoroughly with photographs for insurance purposes.
- **Support your community**. After unrest, communities need to rebuild trust and solidarity.
- **Debrief with your family**. Talk through what happened, what worked and what gaps you identified. Update your emergency plan accordingly.

19.3 A WORD ON THE SPIRITUAL DIMENSION OF UNREST

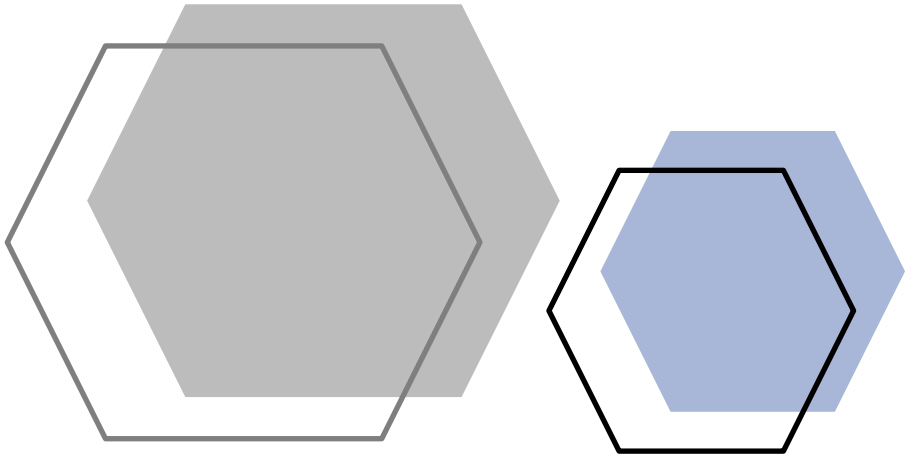
Civil unrest is deeply unsettling not only physically but spiritually and emotionally. Watching the society around your fracture, seeing fellow citizens destroy property and harm one another, feeling the fragility of the systems we depend on — these experiences shake something deep in the human spirit.

In those moments, return to the foundation laid in Chapter 1. Trust in God is not passive resignation — it is an active anchor that will keep you calm, purposeful and clear-headed when everything around you are chaotic.

Psalm 46:1-2 *reminds us: "God is our refuge and strength, an ever-present help in trouble. Therefore, we will not fear, though the earth give way and the mountains fall into the heart of the sea."*

19.4 SUMMARY

- **Pay attention to warning signs —** unrest rarely happens without advance indicators
- **Act early —** fill fuel, withdraw cash and top up supplies before the situation deteriorates
- **Stay home —** the golden rule of civil unrest survival
- **Keep a low profile —** do not advertise your preparations or engage with crowds
- **Coordinate with neighbours —** an organised street is a safer street
- **After the unrest —** replenish supplies, document damage and debrief with your family



20 CYBER SECURITY AND DIGITAL PREPAREDNESS

CASE STUDY — Your Personal Information Was Already Stolen. You Just Did Not Know It.

Times Live / Business Insider South Africa / SABRIC — August 2020

On 19 August 2020, South Africans woke up to news that stopped many of them cold. Experian — one of the country's largest credit bureaus, holding the personal financial records of virtually every adult South African — had handed the private details of ***24 million people and nearly 800 000 businesses*** *to a fraudster.*

Not hacked. Not broken into. Simply handed over.

The fraudster had done something remarkably straightforward. He picked up the phone, pretended to represent a legitimate client and persuaded Experian to release its consumer data in what appeared to be a routine business transaction. By the time anyone realised what had happened, the names, ID numbers, contact details, addresses and financial histories of more than half the South African adult population were in the hands of a criminal.

Experian's CEO Ferdie Pieterse explained it on Radio 702: "A perpetrator, using very smart social engineering techniques, put himself forward as a known customer of Experian and then contracted with us in the normal course of business and in that way illegally obtained the records of 23.4 million individuals."

The South African Banking Risk Information Centre — SABRIC — issued an immediate warning to the public. Their message was sobering:

"The compromise of personal information can create opportunities for criminals to impersonate you. Criminals can use this information to trick you into disclosing your confidential banking details."

Standard Bank confirmed that its clients' demographic information had been leaked and urged customers to change their passwords immediately. Banks across the country scrambled to identify which of their customers were affected.

Here is the most unsettling part of this story. ***If you were a South African adult in 2020, the chances are extremely high that your personal information was in that data.*** *You did not have to be an Experian customer. You did not have to have done anything wrong. Simply by having a bank account, a store card, a cell phone contract or any form of credit, your information had been shared with Experian as part of the normal operation of South Africa's financial system — and it was now in a criminal's hands.*

Most South Africans never received a phone call, an email or any notification that their information had been compromised. They went about their daily lives completely unaware that somewhere, a criminal now knew their full name, their ID number, where they lived and their financial history.

This is exactly how modern cyber-crime works. It does not announce itself. It does not break down your door. It slips through a gap you did not even know existed — and by the time you discover it, the damage may already be done.

The numbers that should concern every South African household:

- *South Africa suffers more than **150 data breach notifications every single month** — up from 56 per month just two years earlier (Information Regulator, 2024)*
- *South Africa recorded **34.5 million compromised accounts** in the first quarter of 2024 alone — making us the second most affected country in Africa for cyber incidents*
- *Digital banking fraud has surged by **45 percent**, with financial losses rising by **47 percent***
- *The average cost of a single data breach in South Africa reached **R53 million** in 2024*
- *South Africa loses an estimated **R2.2 billion** to cyber-crime every year*
- *In 2024, Cell C suffered a breach exposing the ID numbers, banking details and SIM card information of **7.7 million customers** — creating direct risk of SIM swapping and banking fraud for every one of them*

"I don't think South Africans take cyber security seriously, to be honest. The hackers have found very fertile ground in South Africa." — Advocate Pansy Tlakula, Chairperson of the Information Regulator, 2024

In previous chapters we discussed the importance of storing copies of your critical documents digitally — on a flash drive, in cloud storage or on your phone. This is excellent advice and I stand by it completely. However, the digital world comes with its own set of vulnerabilities that every South African family needs to understand and prepare for.

A personal disaster does not always arrive in the form of a flood, a power failure or a political crisis. Sometimes it arrives as a text message from your “bank” asking you to verify your details. Sometimes it is a phone call from someone claiming to be from SARS. Cyber-crime is one of the fastest growing threats in South Africa. According to the South African Banking Risk Information Centre, South Africa loses billions of rands annually to cyber-crime — making it one of the most targeted countries in the world relative to its size.

20.1 UNDERSTANDING THE THREAT

20.1.1.1 PHISHING

This is when a criminal sends you a fraudulent email, SMS or WhatsApp message that appears to come from a legitimate source — your bank, SARS, a courier company or even a government department. The message typically creates a sense of urgency and asks you to click a link or provide personal information. During a crisis, when people are anxious and distracted, phishing attacks increase dramatically.

20.1.1.2 SIM SWAPPING

A criminal uses your personal information to convince your mobile network to transfer your phone number to a new SIM card in their possession. Once they control your number, they can intercept one-time passwords and access your banking accounts. This can happen within hours and cause devastating financial loss.

20.1.1.3 IDENTITY THEFT

Your ID number, date of birth, home address and banking details are all that a criminal needs to open accounts, take out loans or commit fraud in your name.

20.1.1.4 DEVICE THEFT

In South Africa, phone and laptop theft is common. If your device is not properly secured, a thief gains access to your banking apps, emails, cloud storage and personal documents.

20.1.2 PROTECTING YOUR DIGITAL LIFE

20.1.2.1 USE STRONG UNIQUE PASSWORDS

A strong password is at least twelve characters long and contains a mix of upper- and lower-case letters, numbers and symbols. Never use the same password for more than one account. Consider using a reputable password manager application.

20.1.2.2 ENABLE TWO-FACTOR AUTHENTICATION

Most banking apps, email providers and social media platforms offer two-factor authentication. Enable this on every account that offers it.

20.1.2.3 BE SUSPICIOUS OF URGENCY

Legitimate banks and government departments will never ask you to click a link in an SMS or email to verify your details urgently. If you receive such a message, call the institution directly using the number on their official website or the back of your bank card.

20.1.2.4 PROTECT YOUR SIM CARD

Contact your mobile network provider and ask them to add a SIM swap block to your account. This takes less than five minutes and is one of the most important precautions you can take.

20.1.2.5 LOCK YOUR DEVICES

Every phone, tablet and laptop should have a strong PIN, password, fingerprint or face recognition lock enabled. Set the device to lock automatically after thirty seconds of inactivity.

20.1.2.6 BACK UP YOUR DATA REGULARLY

Keep encrypted backups of important files on both a physical device such as an external hard drive or flash drive and a secure cloud storage service. Store the physical backup in a different location to your device.

20.1.2.7 BE CAREFUL WHAT YOU SHARE ON SOCIAL MEDIA

What you post publicly tells criminals a great deal about you — when you are away from home, what valuables you own, where your children go to school. Review your privacy settings regularly.

20.1.3 WHAT TO DO IF YOU ARE COMPROMISED

- **Contact your bank** on their official number the moment you suspect fraud. Ask them to freeze your accounts immediately.
- **Contact your mobile network** if you suspect a SIM swap has occurred.
- **Change your passwords** on all affected accounts from a secure device.
- **Report the incident to SAPS** and to the South African Banking Risk Information Centre at sabric.co.za .
- **Check your credit report** through TransUnion or Experian to identify any fraudulent accounts opened in your name.
- **Inform your family** so they are not caught off guard by fraudsters impersonating you.

20.2 SUMMARY

- **Cyber-crime is a real and growing threat** — treat it as seriously as physical security.
- **Use strong unique passwords** — and a password manager to keep them organised.
- **Enable two-factor authentication** — on every account that offers it.
- **Request a SIM swap block** — from your mobile network provider today.
- **Lock your devices** — and back up your data regularly.
- **Act immediately if compromised** — speed is critical in limiting damage.