

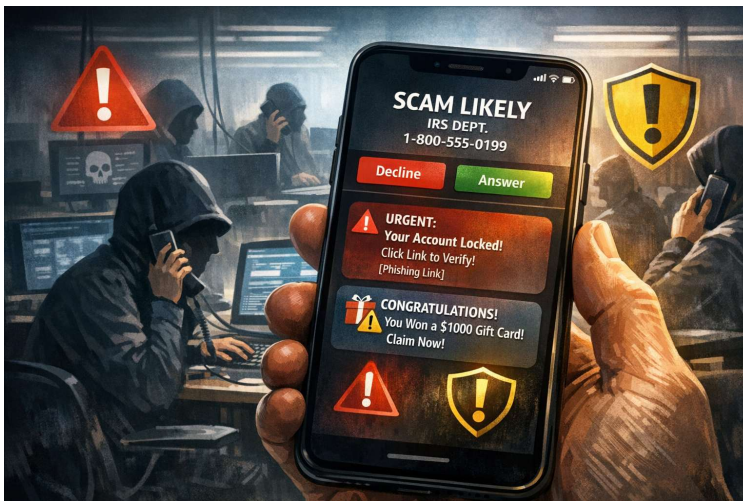
NEWSLETTER JUNE 2026

Hi all,

Stay One Step Ahead of Cell Phone Scams

Cell phone scams are becoming more convincing, but a few smart habits can make a big difference. The safest rule is simple: never share personal information, never click unexpected links, and always verify suspicious messages or calls through an official channel. Fraudsters often rely on urgency, fear, and emotional pressure to catch people off guard, so staying calm is one of your best defences.

Here are the most practical ways to protect your device, your accounts, and your money.



Be Careful with Calls and Messages

Hang up on pressure tactics. If a caller or automated message tries to rush you into deciding, end the call immediately. Legitimate organisations will not force you to act in panic.

Ignore one-ring calls. Some scammers use very short calls to tempt you into calling back expensive premium-rate or international numbers.

- **Verify independently.** If someone claims to be from your bank or service provider, hang up and contact them using a trusted number, such as the one on your bank card or official website.
- **Do not click suspicious links.** Avoid tapping links in unexpected text messages or opening attachments that appear to be delivery notices, billing alerts, or account warnings.
- **Watch for “friend in need” scams.** Be cautious if you receive a message from an unfamiliar number claiming to be a family member who has lost their phone and urgently needs money.



Secure Your Device and Accounts

- **Use strong access controls.** Protect your phone with a six-digit PIN, biometric login, or a strong pattern lock.
- **Lock your SIM card.** Ask your mobile network provider how to activate a SIM lock PIN to reduce the risk of identity theft and SIM-swap fraud.
- **Turn on multi-factor authentication.** Add this extra layer of protection to your banking, email, and social media accounts whenever possible.
- **Download apps only from official stores.** Stick to trusted app platforms to lower the risk of malicious software.
- **Avoid public Wi-Fi for sensitive activity.** When checking banking or personal accounts in public, use mobile data or a trusted virtual private network instead.

Monitor and Report Suspicious Activity

In short, the best defence against cell phone scams is to pause before you respond. Stay alert, verify every unexpected request, protect your device with strong security settings, and report anything suspicious quickly. A few careful steps can help you avoid costly mistakes and keep your personal information safe.

The Tech Guard

Don't Wait for the Crash: Why Backing Up Your Data is non-negotiable

Imagine waking up tomorrow morning, opening your laptop or phone, and finding absolutely nothing. Your family photos, tax documents, unfinished work projects, and scanned receipts are gone. For thousands of people every day, this nightmare becomes a reality.



Data loss is not a matter of "if," but "when." Whether it is a sudden hardware failure, a misplaced device, or a malicious ransomware attack, your digital life is constantly at risk. Relying on a single device to store your irreplaceable information is a dangerous gamble.



Investing a few minutes today into creating a secure data backup is the only way to guarantee your peace of mind for tomorrow.

The Hidden Costs of Digital Negligence

- **Financial loss:** Replacing lost business data or paying ransomware hackers costs thousands.
- **Wasted time:** Recreating lost documents and spreadsheets takes days of stressful labour.
- **Emotional distress:** Permanent loss of sentimental photos and videos cannot be undone.
- **Identity risks:** Lost local files often contain sensitive personal data.

The Gold Standard: The 3-2-1 Backup Strategy

Experts universally recommend the 3-2-1 rule to keep your data completely safe from any disaster.

- **3 copies of data:** Keep one primary version and two backups.
- **2 different media types:** Store data on two distinct device types, like an internal drive and an external hard drive.
- **1 offsite location:** Keep at least one backup away from your home, such as in cloud storage.

Action Steps for This Week

1. **Audit your data:** Identify your most critical files, photos, and financial documents.
2. **Pick a cloud provider:** Sign up for a reputable, automated cloud backup service.
3. **Buy external hardware:** Purchase a portable external hard drive for local backups.
4. **Automate the process:** Set your devices to back up automatically every night.

To help tailor future newsletters, tell me about your current setup:

- What **operating system** do you use most? (Windows, macOS, iOS, Android)
- Do you prefer **physical external drives** or **cloud storage**?
- Have you ever **lost important data** in the past?

I can provide a step-by-step setup guide for your specific devices.

Please stay safe and phone me if you need help or advice.

Regards

Gerhard Prinsloo
072 157 2479

