DIGITAL SELF-DEFENCE

IN AN INSECURE WORLD

Safer Browsing & Digital Hygiene for Ordinary People

A Standing Tall companion booklet

StandingTall.co.za

© 2026 Shelley Childs / Standing Tall. All rights reserved.
Free to download, print, and share as-is for personal and educational use.
Not to be edited, rebranded, resold, or republished without permission.

Introduction: Why This Matters Now

The world is facing more cybercrime, more scams, more outages and more online fraud than ever before. It is easy to assume this is a problem for banks, big companies, or people with a lot of money — but that is not how it works in practice.

Ordinary people are targeted not because they are important or wealthy, but simply because they are available. A scammer does not need you to be rich; they need you to answer the phone, open the email, or click the link. That is the entire qualification to be a victim.

Here is the single most important idea in this whole booklet: most successful attacks exploit human behaviour rather than technology. Firewalls, antivirus software and bank security systems are usually strong. The weak point is almost always a person making a fast, emotional decision — which means the single best security tool you own is not a piece of software. It is you, thinking clearly, for just a few extra seconds before you act.

This booklet follows the two-part U3A talk on digital hygiene. Part One covers scams, passwords and the everyday tricks used against you. Part Two goes further into identity theft, online tracking, data safety and artificial intelligence. You do not need to be a technical person to use any of it — everything here is written for ordinary people living ordinary digital lives.

A Few Tech Worries You May Recognise

Before going further, it is worth naming the kinds of things that already worry most people, because you are probably not alone in any of these:

- Phone scams promising a prize you ‘just need to claim’ with a few personal details.
- Calls or messages claiming your bank details have been compromised, asking you to ‘confirm’ them.
- AI-generated fake voice calls that sound exactly like someone you know.
- A WhatsApp message from a stranger, or an unfamiliar number, asking urgently for help.
- Silent calls that hang up the moment you answer.
- Emails from senders you have never heard of.

Every one of these works the same way: it tries to create a strong feeling — fear, urgency, sympathy, curiosity — quickly enough that you act before you think. Recognising the pattern is most of the defence.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

Part One

Scams, Passwords, and the Everyday Tricks Used Against You



© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

WHY YOU MATTER TO CRIMINALS

It can feel strange to think of yourself as a target. You are not a bank, not a celebrity, not a business — so what could a criminal possibly want from you? The honest answer is: quite a lot.

Think about what you actually have. You have a visiting pattern — predictable routines a criminal can learn. You have assets — savings, a home, a car, a pension. You have a clean record — no fraud flags, which makes your identity more useful to steal than one already tainted by prior misuse. And, perhaps most importantly, you are available — reachable by phone, email and WhatsApp, often several times a day.

None of this means the world is a frightening place to be avoided. It means it is worth spending a few minutes understanding how you are seen from the other side, so that ordinary caution replaces either naive trust or constant anxiety.

Your Best Security Tool Is Yourself

Technology helps, but thinking protects. Before you do anything in response to an unexpected call, message or email, get into the habit of asking three simple questions:

Who are you?

What do you want?

Why should I trust you?

If you cannot answer all three comfortably, slow down. This applies particularly before you click a link, reply to a message, download an attachment, make a payment, or share any personal information. Every one of those five actions can be undone by five extra seconds of hesitation — but almost none of them can be undone once you have gone ahead.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

WHEN ATTACKS GO BEYOND YOU: DDOS AND NATIONAL INCIDENTS

Not every attack is aimed directly at an individual. A Distributed Denial of Service (DDoS) attack floods a service with fake traffic until real users cannot get through — rather like thousands of hoax phone calls jamming a switchboard so genuine callers can never get an answer. Banks, internet service providers, municipalities and ordinary businesses can all be affected.

Even when the underlying infrastructure survives an attack like this undamaged, something important is still disrupted: trust and access. You may find you cannot log into your bank, pay an account, or reach a service you rely on — not because your own security failed, but because the systems around you came under strain.

SOUTH AFRICAN CASE STUDY

Transnet Cyberattack (2021)

A major cyberattack disrupted container terminals and logistics operations across South Africa's ports.

Paper-based systems had to be used temporarily to keep freight moving. They also moved a lot more slowly.

The incident is a clear reminder that cyberattacks on 'big' targets ripple down into ordinary economic activity — delayed goods, delayed payments, delayed services — for people who never interacted with the attackers at all.

SOUTH AFRICAN CASE STUDY

Department of Justice Ransomware Attack

Government systems and online services were disrupted, making access to information and official services difficult for weeks.

Cybersecurity is no longer a niche IT concern — it is now a matter of national resilience.

In both this case and the Transnet attack, the criminals' initial access was most likely gained because someone, somewhere, opened a single email they should not have.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

HUMANS AND THEIR BEHAVIOUR ARE THE TARGET

Scammers rarely attack technology directly — they attack you, using a small, well-worn set of emotional levers: urgency, fear, authority, loneliness and greed. Fake bank calls, courier scams and WhatsApp impersonation are among the most common versions of this in South Africa today.

The goal in almost every case is the same: to make you act before you think. A scammer who can keep you on the phone, keep you anxious, or keep you moving quickly is a scammer who is winning. The single most effective countermeasure is simply to slow down.

The Courier Scam

A typical version goes like this: you receive a message about a parcel that needs a small payment to be released. You look, you decide it is a small enough amount that it is not worth the hassle of investigating, and maybe you pay. It feels like 'not a big loss' — but it is worth asking what the scam operation actually gets out of it besides your money: a confirmed working phone number, a confirmed willingness to pay on request, and possibly your card or banking details, all of which can be resold or reused against you later. One of the things you should think about is why is there an amount due and why are you liable. Afterall, the sender usually pays the courier company. If appropriate they bill you. The tax or customs duty, if a professional freight forwarding company is involved is usually paid upfront by a freight company so why is an intermediary courier company asking you for money.

SOUTH AFRICAN CASE STUDY

Fake SARS Refunds

Victims receive emails or SMSes claiming they are owed a tax refund from SARS.

The links lead to fake websites designed purely to steal login credentials or banking details.

The messages typically create urgency, or fear of penalties, to stop you thinking clearly.

Protection: only access SARS through official channels that you type in yourself — never through a link someone else has sent you.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

PASSWORD SAFETY

Passwords remain one of the simplest places to dramatically improve your security. A few core habits do most of the work:

- Never reuse the same password across important accounts — if one site is breached, a reused password hands criminals the keys to everything else.
- Use passphrases rather than passwords. A phrase such as 'Doctor-mYself-baNish' is both easier to remember and harder to crack than a short jumble of characters, because length matters more than complexity.
- Use a password manager where you can. You do not need to buy anything special — Google, Edge, Firefox, Brave and DuckDuckGo all come with a built-in password manager you may already have without realising it.
- Take breach warnings seriously. If your browser (the companies listed above and others) or email provider such as Google, MWeb, etc, tells you that, say, thirty-two of your passwords have been found in a data breach, that is not routine background noise — it is a direct instruction to go and change them.

It is worth pausing on why 2FA (see next page) and passphrases matter together: a compromised password is rarely the result of someone guessing it. It is far more often the result of a data breach at a company you trusted, a phishing email that tricked you into typing it into a fake site, malware quietly recording your keystrokes, or simple *shoulder surfing in a public place.

** shoulder surfacing, someone behind you watching or recording what you are typing.*

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

PHONE SECURITY

Your phone is not just a phone. It typically contains your banking apps, proof of identity, your full contact list and, often, saved passwords — which makes it one of the single most valuable things you own from a criminal's point of view, whatever it cost you to buy.

Three habits protect it well: install apps only from official stores, never from links in messages; keep the device's software updated, since updates frequently patch security holes; and keep it locked with a PIN, password or biometric lock at all times, even at home. Have your phone automatically lock after a few minutes of non use.

Two-Factor Authentication (2FA)

Two-factor authentication adds a second security step beyond your password — typically a code sent to your phone, or generated by an app. Authenticator apps are generally safer than codes sent by SMS, because SMS can be intercepted through tricks like SIM swapping (covered later in this booklet).

If you protect only one account with 2FA, protect your email account first. Email is usually the account used to reset every other password you have, which makes it the key to everything else.

Phishing and Fake Messages

Phishing is the general name for messages designed to trick you into clicking, replying or handing over information. A few habits catch the great majority of them: check web addresses (URLs) carefully before clicking anything, since fake addresses often look almost — but not quite — right; never trust an unexpected link or attachment, even one that appears to come from someone you know; and remember that urgency is very often the enemy of good judgment. A message that pressures you to act 'right now' deserves more suspicion, not less.

Three Kinds of Security

It helps to know that security generally falls into three broad categories, and that the strongest protection usually combines more than one:

- Something you know — a password or a PIN.
- Something you have — your phone, an authenticator app, or a physical security key.
- Something you are — a fingerprint, face recognition, or another biometric marker.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

A password alone (something you know) can be stolen. Adding a second category — your phone, or your fingerprint — means a criminal who has your password still cannot get in without also having physical access to you or your device.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

Part Two



© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

AI, DEEPFAKES AND MANIPULATION

Artificial intelligence can now imitate voices, images and written messages convincingly enough that seeing — or hearing — is no longer believing. A call that sounds exactly like your grandchild, in distress, is no longer proof that it is your grandchild. The only reliable response is to always verify unusual requests independently, through a channel you control — calling back on a known number, or checking with another family member — rather than trusting the channel the request arrived through.

SOUTH AFRICAN CASE STUDY

WhatsApp Family Impersonation

A scammer pretends to be a child or relative messaging from a 'new number'.

The victim is told there is an urgent emergency or payment problem that needs immediate action.

Emotional urgency is deliberately used to stop the victim from pausing to verify.

Protection: always verify using a separate contact method before sending any money — for example, emailing the family member directly through Gmail or iCloud Mail, or phoning their known number, rather than replying on the new number itself.

SOUTH AFRICAN CASE STUDY

Municipal & Utility Scams

Residents receive fake messages threatening imminent water or electricity disconnection.

Victims are pressured into making an immediate payment to avoid the supposed cutoff.

Fraudsters deliberately exploit the fear and confusion many people already feel around municipal billing.

Protection: verify directly with the municipality using official contact details you already have, and build the habit of never paying in response to a threat alone.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

TRACKERS AND 'FREE' ACCESS

Here is a simple way to picture how online tracking works. Imagine walking into a shopping centre wearing a numbered badge. Every shop you pass can see 'Badge 1234' and quietly notes what it observes: likes gardening, looked at dog food, read articles about retirement in a shop window, stops and reads a travel advert and then picks up a brochure, lives in Pretoria and shops in say Brooklyn. The shops may never learn your actual name — but between them, they build up a remarkably detailed picture of Badge 1234 all the same. That badge is, in essence, what your browser and phone carry with them everywhere online.

How Google Trackers Work

Say you see an advert on Google for washing lines and click through to the seller's site. That site gives you an identity — a badge — and that identity becomes embedded on your device – laptop, phone, tablet, desktop. For entirely legitimate purchases, this mostly keeps you conveniently anonymous as a person. But the same system means bad actors will do everything they can to turn that anonymous badge back into an identifiable person.

Online, that 'badge' is usually made up of one or more of the following: cookies, device fingerprints, advertising IDs, logged-in accounts, and your IP address. When a website loads, it may quietly also load content from Google, Meta, various advertising companies, analytics firms, video providers and others — all watching the same visit. This, in effect, is the contract you have already signed with Google, whether or not you remember signing or reading anything. Other companies work in more or less the same way.

Google itself provides a wide range of free tools to website owners — Google Analytics, Google Ads, YouTube embeds, Google Fonts, and the familiar 'I am not a robot' reCAPTCHA box. But rarely is anything free. Each one, while useful to the website owner, is also a channel through which Google can learn something about you: which page you visited, when you visited it, what browser you used, your rough location, how long you stayed, and which links you clicked. The overall goal on Google's side is to understand audiences well enough to make advertising more effective — not to do you personal harm, but you are, nonetheless, the raw material.

How Facebook and Instagram Make Money

Meta — the company behind Facebook and Instagram — learns from almost everything you do on its platforms: the posts you read, the videos you watch, the pages you follow, the advertisements you click, the people you interact with, and simply how long you spend looking at any particular piece of content.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

If you stop scrolling and stare at a gardening video for twenty seconds, Meta learns that gardening interests you. It then sells that insight, in aggregate, as an advertising opportunity: a garden centre can ask Meta to 'show my advert to retired South Africans interested in gardening' — and Meta can do exactly that, because it has been quietly building that profile of you all along. Show my sales advert just to people in Pretoria. In order to specifically target a group of people the advertisers doing so need to know who you are.

WhatsApp, Encryption and Metadata

WhatsApp is worth understanding on its own, because it is genuinely different in one important way: messages are end-to-end encrypted, meaning WhatsApp cannot normally read the actual contents of your chats, and Meta says it cannot see the content of ordinary encrypted conversations. But — and this matters — the metadata around those messages can still be very valuable: who is contacting whom, how often, from which country, on what type of device, which groups someone has joined, and which business accounts they have been in touch with.

It helps to see the difference concretely. Imagine the message 'Let's meet for coffee tomorrow.' The content of that message may be private and encrypted. But the metadata around it might show: sent at 10:04am, to John, from Shelley, using an Android phone, located in Pretoria, and that these two people have been in contact three times this week. None of that required reading a single word of the message itself — and yet it tells a detailed story on its own.

Children, Gaming and Online Risks

Online games are, in effect, social networks with strangers present. Sometimes genuine, but also fake in-game rewards, and account theft, are common, and both can lead a child toward handing over information or access they should not. What protects children best is not fear, but regular, ongoing conversation with people who care and can positively influence children against all the negative influences — the same principle that runs through this entire booklet, simply applied a generation earlier.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

FREE AI: HOW IT ACTUALLY PAYS FOR ITSELF

The same underlying question — 'if it's free, how does it make money?' — applies just as much to AI tools as to social media. There are, broadly, four answers.

1. Training and Improvement

User interactions help developers learn which answers are useful, which are wrong, which questions come up often, and which features people actually want. Free users effectively help test and improve the system simply by using it.

2. Upselling Paid Subscriptions

Many AI companies run on a 'freemium' model: free access comes with limits — slower responses, fewer features. Some users later choose to pay for faster service, more usage, better models or extra tools. In effect, paying customers subsidise the free tier.

3. Business Customers

The real money in AI generally comes from organisations — companies, universities, governments and software developers — who pay significantly more than individual users ever do. Often this is for real and significant research and development that has a positive impact in health, technology, behaviour modelling or similar.

4. Data and Product Research

AI companies also study usage patterns — which features are popular, which industries are adopting AI, and what problems users are trying to solve — to guide future products and investment decisions.

Digital Self-Defence, in Two Questions

Every time you use a free online service — AI or otherwise — it is worth asking yourself two simple questions: how does this company make money, and what information am I giving in exchange for the service? Once you can answer both, you are in a position to judge for yourself whether the exchange is a reasonable one, or a risk you would rather not take.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

PUBLIC WI-FI AND VPNS

Public Wi-Fi networks are convenient, but they come with real trade-offs. Avoid doing sensitive banking on public Wi-Fi where possible, and be aware that fake hotspot networks — set up specifically to intercept traffic — are common in busy public places. A simple, low-tech alternative worth knowing about is a mini mobile router — a small personal hotspot device that gives you your own private connection instead of relying on a shared public network at all.

A VPN can improve your privacy on such networks, but it is not a magic shield against every risk, and it is worth considering the legality of VPN use in whichever country you are in. Also think about the reason why you want a VPN. Good and bad reasons.

If you are paying for a VPN so that you can watch something paid for by the German population you must consider whether, even though you pay the VPN company, you are not stealing. Legitimate uses pay to watch the rugby game. The organization they pay has in turn paid to the controlling body – say IPL cricket organisers, for the right to transmit the game.





© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

DATA SAFETY: ANTIVIRUS AND BACKUPS

Good data safety rests on two separate habits: keeping malicious software out, and making sure you can recover if something still goes wrong.

Antivirus and Security Software



Windows Defender, and the built-in protections from Google and Apple, provide a reasonable baseline on most devices. Dedicated products such as Bitdefender or Malwarebytes can add further protection, and phones and tablets deserve the same attention as computers — they are not automatically safe simply because they are smaller.

Cloud and Other Backups

There are no guarantees in backups — only better and worse habits. Back up photos, contacts and important documents automatically where you can, and occasionally test that a restore in fact works: a backup you have never tested is only a hope, not a plan. It is worth genuinely assessing the risk profile of cloud backup for your own situation. The cloud is usually based in a building in some foreign country. Possibly foreign countries not enamoured with South Africa.

Considering physical alternatives too — an external SSD drive or a simple memory stick can be a useful second copy alongside anything stored online. Use it for your value documents. Like your tax and bank papers, copies of birth, marriage and death certificates and the most precious photos.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

A CAUTIONARY TALE: THE LAPTOP YOU THOUGHT WAS SAFE

This story is shared as an anonymised example — the lesson here is about habits, not about blaming any individual. Picture someone who has security software installed, genuinely believing they are protected — and yet warnings from that very software are quietly ignored over time, compromised passwords are never changed, and small unsafe habits are allowed to accumulate. When things go wrong, who is at fault. You are.

Two fair questions to ask of any security software are: what can and do these packages actually offer, and are all the different brands really equal? The uncomfortable answer in this story is that having security software installed is not the same as being secure — the software was doing its job. The warnings were simply not acted on. And no, not all brands are equal. They change over time. It is up to you to research the issue. Speak to other users. Read online articles, speak to distributers. Look for forums.

Laptop Health Checklist

- Update your software regularly.
- Keep your antivirus current — an out-of-date antivirus gives a false sense of security.
- Remove programs you no longer use.
- Back up your important files.

It helps to think of this the same way you think of maintaining a car: nobody expects a car to run forever without servicing, and a computer or phone is no different — it needs regular, unglamorous maintenance to keep doing its job safely.

Security Tools Need Human Help

Antivirus software warns you; it does not replace good decisions. Updates, strong passwords and careful browsing all still matter, however good your security software is. A useful comparison is a smoke alarm: it will warn you if there is a fire, but it will not put the fire out, evacuate the house, or stop you from leaving a candle burning in the first place. The warning is only useful if you act on it.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

THE BEST SECURITY IS A HABIT, NOT A PRODUCT

Perfect security does not exist, for anyone, at any budget. What does exist is a set of good habits that dramatically reduce your risk — and, encouragingly, the safest people online are very often simply the least impulsive and realistic, not the most technical.

SOUTH AFRICAN CASE STUDY

Load Shedding Opportunists

Scammers deliberately exploit the frustration many South Africans feel during power outages.

Fake inverter, solar or generator deals appear on social media, often at suspiciously attractive prices.

Victims pay a deposit for products that simply never arrive.

Protection: verify any such business independently before paying anything, and avoid rushed EFT payments made under time pressure — a genuine deal will still be there tomorrow.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

BRINGING IT ALL TOGETHER: THE GOLDEN RULES

The Six Golden Rules

- Slow down emotional reactions.
- Never trust someone else's sense of urgency — it is usually manufactured, not real. Ask yourself why.
- Verify independently, through a channel you chose yourself.
- Avoid suspect links.
- Use unique passwords, or better still, passphrases.
- Back up what matters.

A Simple Three-Step System

If even six rules feels like a lot to hold in mind in the moment, it can be boiled down further, to just three steps that cover almost every situation in this booklet:

- Slow down.
- Verify.
- Think before clicking.

None of this is about living in fear of the internet. It is about the same kind of ordinary, sensible caution you already apply when crossing a busy road or handing over your house keys — not paralysing, just enough to keep you, and the people you care about, genuinely safe. Go well, and go online with confidence rather than fear.

© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.

About This Booklet

Digital Self-Defence in an Insecure World is published on StandingTall.co.za.

© 2026 Shelley Childs / Standing Tall. All rights reserved.

This booklet is free to download, print, and share as-is, in full, for personal and educational use.

It may not be edited, rebranded, resold, or republished — in whole or in part — without written permission from the author.

For permissions or enquiries, get in touch via StandingTall.co.za



© 2026 Shelley Childs / Standing Tall. All rights reserved — not for editing, rebranding, or resale.