



Digital Red Flags

Your Shield as a South African Parent in 2025



A Vital Resource from Tanosec Cybersecurity



Table of Contents

1. Introduction
2. Why This Guide Is Your Lifeline
3. It's Not What It Used To Be
4. Decoding the Digital Footprint on Social Platforms
5. Gaming Platform Red Flags-When Play Becomes Peril
6. Emerging Threats and Technologies
7. Mental Health and Emotional Manipulation
8. Financial and Identity Theft Red Flags
9. Warning Signs in Digital Communication
10. Practical Monitoring and Detection Strategies
11. Response Strategies and Resources
12. Building Long-Term Digital Resilience
13. Conclusion: Empowering South African Parents and Care givers in the Digital Age

This guide was compiled using the most current information available as of July 2025, specifically tailored for South African parents and primary caregivers. The digital safety landscape changes rapidly, and we encourage you to stay informed about new developments and emerging threats through reputable sources and ongoing education.



The Digital Veld Our Children Roam

Baholo, re a le lumela ka tlotlo.

We at Tanosec understand. You're navigating a digital world that is constantly changing. For us, who often grew up with rotary phones and "Go-Go" bag phones, the screens our children hold are their entire universe. They're 'digital natives', zipping through apps and games we barely understand, but this doesn't mean they're automatically safe.

The truth, as difficult as it is to face, is that our children – your children, our future – are more connected, more exposed, and tragically, more vulnerable than any generation before them. That smartphone in their hand? It's a powerful gateway to global networks, virtual worlds, and unseen dangers. The lines between what's public and private, friend and stranger, real and artificial, have blurred into a digital fog.

The predators out there aren't using obvious, old-school tactics. They're cunning. They've evolved right alongside the technology. They use clever psychological manipulation, they infiltrate the social spaces in gaming, and they even use artificial intelligence to create convincing, trusted personas.

+ Why This Guide Is Your Lifeline

The reality of online child safety is stark, and it's worsening globally and right here in Mzansi. Investigations reveal shocking vulnerabilities in platforms used by millions of South African children daily. Our own law enforcement agencies are seeing a dramatic surge in online crimes against children, with predators becoming more sophisticated, more brazen, and tragically, more successful.

But here's the most unsettling truth: many parents significantly underestimate the risks. You might feel you understand your child's online world because you recognise the app names – TikTok, Roblox, WhatsApp. But do you truly understand how these platforms function as complex social environments, how easily a wolf can hide among the sheep? Studies consistently show a worrying gap between what parents think is happening and what is actually happening online.

This knowledge gap has devastating consequences. When our children encounter predators, cyberbullying, or exploitation, they often don't tell us. Why? Sometimes it's fear – fear of getting in trouble, fear of losing their device, fear of judgment.

They understand how platforms work, how to grab attention, and they turn the very features designed for connection into tools for exploitation.

And while all this is happening, many of you, the dedicated parents and guardians, feel like you're playing catch-up. The digital gap between generations is real. Your child often knows more about the inner workings of an app than you do, making it incredibly hard to offer truly meaningful safety guidance.

This guide is here to change that. It's your compass, your early warning system. We're providing you with the most current insights into the red flags you need to watch for, specifically tailored to the social media platforms and online gaming environments your children are on right now in 2025.

This isn't generic advice; it's actionable knowledge directly from the frontline of child safety, informed by law enforcement, experts, and research, specifically designed for your family in South Africa.

Other times, it's because the danger is subtle, insidious. Predators use gradual grooming techniques that normalise inappropriate behaviour over time, making your child believe they're "friends" or even "in love." The impact isn't just emotional. Identity theft targeting children is on the rise, a silent crime where criminals exploit a child's clean record for years before it's discovered. And the emotional scars of online exploitation can last a lifetime, affecting their schooling, future relationships, and mental well-being. This guide matters because knowledge truly is your power.

By understanding how modern threats operate, by learning to spot the warning signs before a situation spirals, and by maintaining open, trusting communication with your child, you can drastically reduce their risk. Our goal at Tanosec is to give you practical, actionable knowledge that reflects today's digital realities, empowering you to confidently guide your children through an increasingly complex online world. We're here to help you protect what matters most.



It's Not What It Used to Be

+ The New Reality in Our Digital Neighbourhood

The online world your children are navigating in 2025 is fundamentally different from even two years ago, and certainly light-years from our own youth. Investigations and local reports highlight concerning trends every South African parent needs to grasp:

Identity Theft and Financial Fraud

Children are increasingly targeted through social media and gaming. Seemingly harmless requests for personal details – a school name, a favourite sport, even a family pet's name – are scooped up by criminals. This isn't just about data; it's about creating "synthetic identities" or building profiles for future financial fraud, often years down the line.

Mental Health Exploitation

Beyond the obvious nastiness of cyberbullying, there's a disturbing surge in content specifically designed to exploit children's mental health vulnerabilities. Think self-harm "challenges," content promoting eating disorders, or algorithms that feed depressive content, trapping vulnerable young minds in dangerous echo chambers.

Sophisticated Grooming Techniques

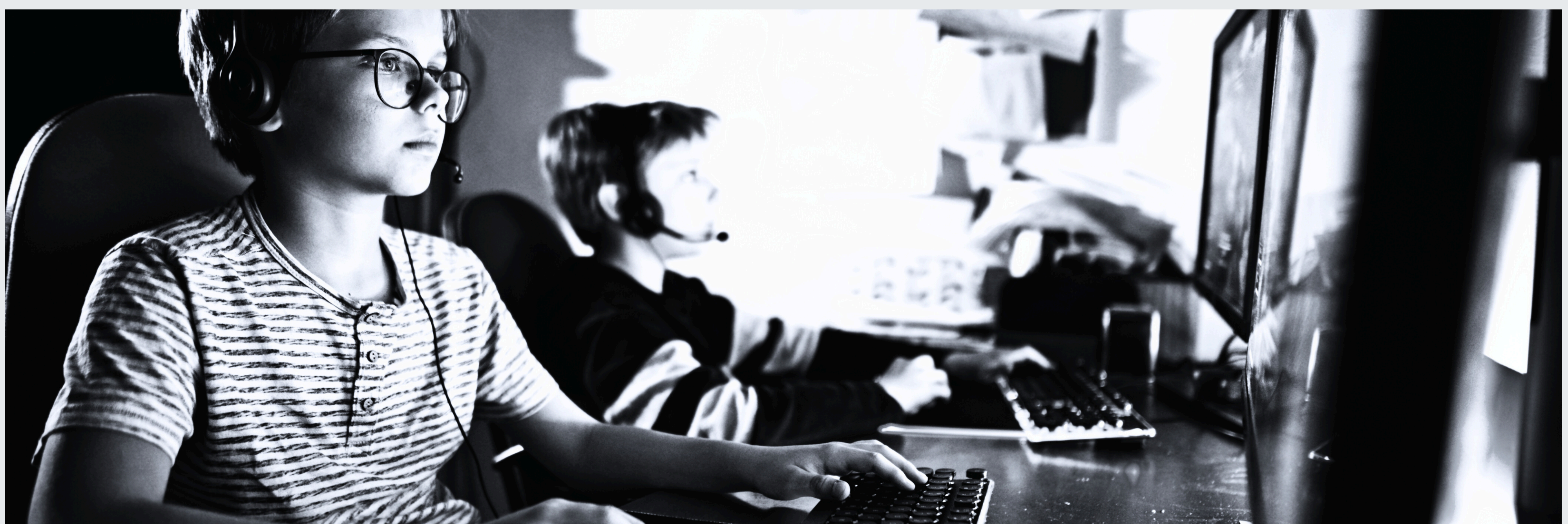
Predators have become masters of disguise. They bypass traditional safety measures by using encrypted chat features, voice notes, and even game-based communication (like in-game emotes or private lobbies) to build "relationships" with children over extended periods. This makes their advances appear normal and unthreatening to the child.

AI-Generated Deception

This is a truly chilling development. Artificial intelligence is now creating incredibly realistic fake profiles, manipulated images (deepfakes), and convincing personas. It's becoming almost impossible for children, and even adults, to tell if they're interacting with a real person or an AI construct designed to deceive them.

+ How platforms Have Morphed

- **Social Media Platforms:** Instagram, TikTok, Facebook (yes, some kids still use it), and others have introduced new features like disappearing content (Snapchat's influence), AI filters that can alter reality, and live streaming. While these can be fun, they also create new avenues for risk and exploitation, offering instant, unmoderated interaction.
- **Gaming Platforms:** Games like Roblox, Fortnite, Minecraft, and others have evolved beyond simple play. They are now vibrant social hubs with voice chat, video sharing, and cross-platform communication. This creates complex social environments where traditional safety rules or basic monitoring might not be enough.





Decoding the Digital Footprint on Social Platforms

As parents and guardians, you are the first line of defence. Understanding these red flags can help you spot trouble before it becomes a crisis. Look beyond the screen; pay attention to their behaviour.

+ Behavioural Changes

The Quiet Warnings.

These are often the first, subtle signs that something is amiss. Trust your gut.

Sudden Secrecy Around Device Use:

- They quickly close apps or switch screens when you approach.
- They become defensive or agitated if you ask about their phone or computer.
- New passwords suddenly appear on devices previously shared with the family.
- They start asking for privacy settings on apps you've never discussed, or they hide their profiles

Emotional Volatility Linked to Online Activity

- Extreme mood swings – unusually happy then suddenly withdrawn or angry – often after checking social media.
- Visible anxiety or agitation when separated from their devices, even for short periods.
- Noticeable depression, sadness, or withdrawal following online interactions.
- Sudden, intense excitement about meeting "friends" they've never mentioned before.

Changes in Sleep and Social Patterns

- Staying up unusually late to communicate with online contacts, disrupting their sleep cycle.
- Losing interest in real-world friendships, family activities, or hobbies they once loved.
- Receiving calls or messages at odd hours, like late at night or very early morning.
- Using devices in highly private or hidden spaces like bathrooms, closets, or under blankets.



Decoding the Digital Footprint on Social Platforms

+ Content and Communication Red Flags

The Digital Trail

These are specific cues within their online interactions that should set off alarm bells.

Inappropriate Gift-Giving or Financial Offers:

- Modern predators often use digital "gifts" as grooming tools. Be wary of:
- Gaming currency, "skins," or premium accounts given by "friends" your child met online.
- Gift cards or online purchases made by unknown contacts.
- Offers to pay for subscriptions or premium features on apps/games.
- Requests for your child's banking details to "send them money" or "share a prize."

Advanced Manipulation Tactics:

- "They understand me better than you do": Adults who claim to uniquely understand your child's feelings, struggles, or interests, often creating a false sense of deep connection.
- "Let's keep this our little secret": Contacts who actively encourage keeping their relationship or conversations hidden from parents or other trusted adults. Creating artificial urgency: Phrases like "delete this message now," "don't tell anyone, this is just between us," or "I need you to do this immediately."
- Gradual introduction of inappropriate topics: Starting with innocent conversations and slowly, subtly, introducing sexually suggestive or otherwise inappropriate subjects.

Identity Verification Requests: A Trap for Personal Information

Be extremely alert to seemingly innocent requests that are actually designed to gather information for identity theft or further grooming:

- Requests for school names, exact addresses, or detailed family information (e.g., "what time do your parents get home?").
- Questions about family routines, work schedules, or travel plans.
- Pressure to share identification documents, even for seemingly legitimate reasons like "verifying age" or "winning a contest."
- Requests for photos in specific locations (like their bedroom, or outside their school) or with identifying information visible (e.g., school uniform, street signs).



+ Platform-Specific Warning Signs

Knowing the Battleground

Each platform has its quirks and vulnerabilities. Here's what to specifically watch for on popular South African platforms:

Instagram and TikTok

- Following accounts with suggestive usernames, profile pictures, or content.
- Creating secondary, "finsta" (fake Instagram), or "spam" accounts to hide activities from you.
- Participating in "challenges" that involve sharing personal information or engaging in risky behaviours.
- Receiving direct messages (DMs) from accounts with very few followers, suspicious profiles, or those that seem too old for them.

Snapchat

- Heavy reliance on disappearing message features to prevent message history from being saved.
- Sharing their precise location data with unknown contacts via the Snap Map.
- Receiving "snaps" (messages) from adult users who are not known to the family.
- Using the app's map feature to arrange to meet strangers in person.

Discord and Similar Chat Platforms (e.g., WhatsApp groups with strangers):

- Joining "servers" (groups) with adult-oriented themes, offensive content, or inappropriate chat.
- Participating in voice chats with unknown adults, where conversations are harder to monitor.
- Extensive use of private message features to communicate outside monitored public channels.
- Being invited to "exclusive" or "private" servers by new online contacts.

WHAT TO WATCH OUT FOR

Gaming Platform Red Flags-When Play Becomes Peril

+ The Gaming Threat Landscape in 2025

Not Just Fun and Games

Gaming platforms, especially popular ones in South Africa, have become a primary hunting ground for predators. Why? Because of their interactive social features and the inherent trust children place in their online gaming communities. Recent investigations have exposed serious concerns.

Roblox-Specific Concerns

Roblox has faced significant global scrutiny in 2025, with multiple lawsuits and investigations highlighting:

- Predators using the platform's chat features to identify, isolate, and groom children.
- Exploitation of the game's virtual economy to offer gifts (Robux, exclusive items) in exchange for personal information or favours.
- The creation of "private servers" or custom games designed as unmoderated spaces for inappropriate interactions.
- Voice chat features that bypass traditional text-based monitoring, making it much harder to track conversations.

Discord Gaming Integration

Discord's widespread integration with gaming has opened new vulnerabilities:

- Private servers: Where moderation is minimal or non-existent, creating a "closed community" for illicit activity.
- Voice chat: Conversations that leave no digital trail like text messages, making it harder to track.
- Screen sharing: Capabilities often used to show inappropriate content to children.
- Integration with other gaming platforms: This can expose children to wider networks of unknown users and potential predators.



+ Gaming-Specific Red Flags

More Than Just Leveling Up

Look out for these signs that suggest more than innocent gameplay.

Communication Pattern Changes

- Using gaming voice chat for conversations that are clearly unrelated to the game itself.
- Spending excessive, unexplained time in private gaming servers or small, exclusive groups.
- Receiving frequent or valuable in-game gifts (currency, rare items) from unknown players.
- Being invited to join "exclusive" gaming groups or servers by new, older, or unknown contacts.

Financial Red Flags in Gaming

- Unexplained premium purchases or sudden acquisitions of in-game currency.
- Offers from other players to purchase gaming items or accounts for real money outside the game's official store.
- Requests to share account information, passwords, or even credit card details for "transactions."
- Being asked to participate in "trading" schemes that involve real money transfers or off-platform transactions.

+ Cross-Platform Risks

The Digital Leap

One of the most concerning tactics predators employ is platform jumping. They use gaming environments as initial contact points before pushing the interaction to less monitored platforms, making it harder for parents to track.

The Progression

- Starting conversations innocently enough in games like Roblox, Minecraft, or Fortnite.
- Suggesting communication moves to Discord for "better team coordination" or "private chat."
- Eventually trying to move to encrypted messaging apps (like Signal, Telegram) or even direct phone calls for "more privacy."
- Using multiple platforms to rapidly build a false sense of established relationship and trust.

Social Engineering Through Gaming

- Players who ask overly detailed personal questions about your child's real life during gameplay ("Where do you live?" "What school do you go to?").
- Gaming contacts who suggest moving conversations from the game's public chat to less monitored platforms (like WhatsApp, Instagram DMs, or direct phone calls).
- Users who try to create artificial intimacy by offering "exclusive" gaming experiences or "special" coaching.
- Players who offer to teach "advanced gaming techniques" but only in private settings or direct, one-on-one communication.



WHAT TO WATCH OUT FOR

Emerging Threats and Technologies

The Bleeding Edge of Danger

The digital world is constantly evolving, and so are the threats. As guardians, we need to stay one step ahead.

+ AI and Deepfake Concerns

When Seeing Isn't Believing

Artificial Profile Creation

- AI-generated profile pictures that look like real teenagers, making them appear trustworthy.
- Chatbots designed to mimic teenage communication patterns, making conversations feel natural.
- Synthetic personalities created by AI to perfectly appeal to your child's specific interests (e.g., a shared love for a niche K-Pop band or a specific gaming franchise).
- Automated systems that can maintain multiple deceptive relationships simultaneously, making these threats scalable.

+ Cryptocurrency and Digital Assets

New Ways to Exploit

New Financial Exploitation Methods

- Criminals using NFTs (Non-Fungible Tokens) and cryptocurrency to obscure money trails, making it harder to trace illicit transactions.
- Gaming platforms with cryptocurrency integration creating new opportunities for fraud and illicit exchanges.
- "Educational" content about crypto used as a pretext for financial exploitation schemes.
- Fake investment opportunities or "get rich quick" schemes targeted at children through gaming and social platforms, promising big returns for small initial "investments."

Manipulated Content

- Deepfake technology used to create highly convincing, compromising images or videos of your child, often from innocent photos they've posted online.
- AI-generated voice messages that sound like real people, even impersonating voices they know.
- Manipulated screenshots of conversations designed to create false evidence or confuse your child.
- Synthetic media used to normalise inappropriate behaviour, slowly desensitising your child.

+ Virtual and Augmented Reality Risks

Immersive Dangers

Immersive Environment Dangers

- VR platforms (like Meta Quest worlds) with limited moderation and reporting mechanisms, creating spaces where children can be targeted.
- Augmented reality (AR) filters in apps that can inadvertently reveal sensitive location information.
- Virtual spaces designed to normalise inappropriate behaviour, acting as "testing grounds" for grooming.
- Haptic feedback technology (devices that simulate touch) in VR that can simulate physical contact, adding a disturbing layer of realism to inappropriate interactions.



RED FLAGS

Mental Health and Emotional Manipulation The Hidden Scars

Beyond the direct threat of predators, the online world itself can be a minefield for our children's emotional well-being.

+ Algorithm-Driven Harm

The Unseen Influence

Social media algorithms are powerful, and they can inadvertently—or deliberately—expose children to deeply harmful content.

Content Recommendation Risks

- Self-harm and suicide-related content that creates dangerous "echo chambers," making children feel alone and reinforcing negative thoughts.
- Eating disorder content cleverly disguised as "health and fitness" advice, promoting dangerous habits.
- Conspiracy theories and radicalisation content subtly targeted at vulnerable youth who are seeking identity or belonging.
- Content specifically designed to exploit insecurities and promote unhealthy behaviours, chipping away at self-esteem.

Addiction-Like Patterns

- Platforms are designed to maximise engagement, leading to dependency-like behaviours, similar to addiction.
- Fear of missing out (FOMO) constantly exploited through algorithmic content delivery, making them feel compelled to stay online.
- Validation-seeking behaviours constantly reinforced through likes, comments, and shares, creating a constant need for external approval.
- Severe sleep disruption patterns caused by the attention-capturing design features of apps, impacting their physical and mental health.

+ Psychological Manipulation Tactics

Modern Grooming Approaches

Today's predators are not just "stranger danger." They are sophisticated manipulators, employing psychological techniques to control and exploit.

Love-bombing followed by withdrawal

- Showering your child with excessive attention and affection, then suddenly pulling back to create emotional dependency and a desire for that attention to return.

Gaslighting

- Making your child question their own perceptions, memories, and instincts, leading them to doubt what they know is right.

Isolation techniques

- Gradually encouraging your child to distance themselves from real-world friends, family, and support systems, making the predator their sole confidant.

Exploiting insecurities and mental health struggles

- Predators often scour social media for signs of vulnerability (e.g., posts about sadness, loneliness, body image issues) and then target these specific weaknesses to build rapport and control.



Financial and Identity Theft Red Flags - Protecting Their Future

Beyond emotional harm, online interactions can directly threaten your child's financial future and identity.

+ Sophisticated Financial Exploitation

The Digital Swindle

Social Engineering for Financial Gain

- Requests for "help" with online purchases, gift card codes, or setting up accounts.
- Offers to "share" streaming service or gaming platform accounts, often as a way to gain login credentials.
- Fake emergencies that require immediate financial assistance ("My account is frozen, can you send me money?").
- "Investment opportunities" or "money-making schemes" targeted at minors, promising quick cash for a small initial outlay.

Identity Information Harvesting:

Criminals are now using gaming and social platforms as vast data-gathering operations for identity theft. Look out for:

- Seemingly innocent questions about "security questions" answers like pets' names, favourite teachers, childhood street names, or family traditions.
- Requests for photos that might contain identifying information in the background (house numbers, unique landmarks).
- Gaming contests or surveys that demand personal information (full name, ID number, address) as "entry requirements."
- Social media challenges that encourage sharing personal milestones or detailed family information.

+ Digital Footprint Exploitation

The Long Game

Predators and criminals often play the long game, spending months building comprehensive profiles of potential victims.

Long-term Information Gathering

- Analysing social media posts to determine family routines, work schedules, and even perceived financial status.
- Using location data from photos and check-ins to map daily activities and predict movements.
- Gathering information about extended family members to create convincing impersonation scenarios.
- Building detailed profiles that can be used for future exploitation, sophisticated scams, or long-term identity theft.



WHAT TO LOOK OUT FOR

Warning Signs in Digital Communication Deciphering the Hidden Meanings

+ Sophisticated Financial Exploitation

Social Engineering for Financial Gain

- Requests for "help" with online purchases or account creation
- Offers to share streaming service or gaming platform accounts
- Fake emergencies requiring immediate financial assistance
- Investment opportunities or money-making schemes targeted at minors

+ Digital Footprint Exploitation

The Long Game

Long-term Information Gathering

Predators and criminals often spend months building profiles of potential victims:

- Analyzing social media posts to determine family routines and financial status
- Using location data from photos and check-ins to map daily activities
- Gathering information about family members to create convincing impersonation scenarios
- Building comprehensive profiles for future exploitation or identity theft.

Identity Information Harvesting

Criminals now use gaming and social platforms to gather information for identity theft:

- Seemingly innocent questions about pets' names, favorite teachers, or family traditions (often used as security questions)
- Requests for photos that might contain identifying information in the background
- Gaming contests or surveys that request personal information as "entry requirements"
- Social media challenges that encourage sharing personal milestones or family information



IF YOUR'RE A VICTIM

Warning Signs in Digital Communication

The way your child communicates online, especially with new contacts, can reveal crucial red flags.

+ Advanced Communication Red Flags

Coded and Secret Language

Modern online predators are cunning; they use methods that bypass simple keyword detection.

Coded Language and Secret Communication

- Using gaming terminology or slang to disguise inappropriate conversations ("Wanna trade X for Y?" could mean something sexual).
- Emoji combinations that have specific, often sexual, meanings in predatory contexts (e.g., eggplant and peach emojis).
- References to meeting in "safe" online spaces away from parental oversight or moderation ("Let's go to my private server, it's just for us").
- Use of seemingly innocent phrases that have double meanings, understood only by the predator and groomed child.

Grooming Through Gaming and Social Media

- Gradual introduction of adult topics: Starting with innocuous game chat and slowly, imperceptibly, shifting towards sexually suggestive conversations or content.
- Using shared interests: Exploiting a child's passion for a specific game, streamer, or online content to build a false sense of intimacy and trust.
- Creating artificial emergencies or problems: The predator might invent a crisis that "only your child can help with," demanding secret communication or actions.
- Exploiting the desire to appear mature: Introducing "adult conversations" or "grown-up content" to appeal to a child's desire to seem older or more sophisticated.

1. Abbreviations Used to Hide From Parents

- **POS** – Parent Over Shoulder
- **PIR** – Parent In Room
- **KPC** – Keeping Parents Clueless
- **99** – Parent has stopped watching / end of conversation
- **WTTP** – Want To Trade Pictures?
- **LMIRL** – Let's Meet In Real Life
- **P911** – Parent Alert (911 = danger)
- **CD9** – Code 9, parents around

2. Drug & Alcohol Slang Kids Might Use (Sometimes Overlaps With Grooming)

- **420 / 710** – Marijuana / Oil (710 upside down = OIL)
- **X, Molly, E** – Ecstasy/MDMA
- **Candy / Smarties / Skittles** – Drugs (often pills)
- **CU** – See you (but can also mean "cocaine user")

There are a number of slang terms, coded language, and abbreviations predators or kids might use online to hide the real meaning of conversations. These evolve quickly, so any list is never 100% complete. Learn these terms but focus on context (not every 🍆 is sexual, but combined with 💦 and 😊, it likely is).

3. Sexual / Grooming Slang

- **CU46** – See You For Sex
- **1174** – “Meet me at a party” (sexual invite)
- **8/ate** – Oral sex
- **GNOC** – Get Naked On Camera
- **GYPO** – Get Your Pants Off
- **MIRL** – Meet In Real Life (**dangerous red flag**)
- **WTM** – Want To Meet?
- **NIFOC** – Naked In Front Of Computer
- **MPFB** – My Personal F*** Buddy

4. Innocent-Looking Emojis With Hidden Meanings

- 🍆 - Penis
- 🍑 - Butt
- 🍊 - Vagina
- 💦 - Sexual Fluids
- 👁️ - Interested / Watching
- 🚗💨 - Sneaking out / Going Somewhere Secretly
- 🔑 or **P** - Code for Drug, - “plug” (dealer)
- 🌈 - Can be LGBTQ+ but also used for drug culture context



+ Technology-Enabled Deception

When Impersonation Goes Digital

Advanced Impersonation Techniques

- Using information gathered from social media to impersonate known individuals (friends, relatives, teachers) to gain trust.
- Creating fake emergency scenarios involving family members or close friends to elicit information or actions.
- Using voice-changing technology in gaming voice chats to sound like a peer or a different gender.
- Sophisticated catfishing, where AI-enhanced photos and fabricated personas are used to create entirely fake, highly convincing identities.

BUILDING YOUR DEFENCE

Practical Monitoring and Detection Strategies – Your Tools for Protection

As parents & guardians, we have a vital role to play in monitoring our children's online lives, not as spies, but as protective guardians.

+ Effective Monitoring Without Invasion

Finding the Balance

It's about transparency and trust, not just surveillance.

Technology-Based Solutions

- Using parental control software that focuses on behaviour patterns and communication anomalies rather than simply blocking content. Look for solutions that provide insights into who they're talking to and when, rather than just what websites they visit.
- Setting up network-level monitoring (e.g., on your home router) that can detect unusual communication patterns or attempts to access restricted sites.
- Implementing time-based restrictions on devices that align with healthy digital habits, ensuring they get enough sleep and offline time.
- Using family safety tools that provide transparency and conversation starters, rather than enabling absolute secrecy.

Communication-Based Strategies

- Regular, casual check-ins about their online experiences. Focus on their feelings ("How did that game make you feel?") rather than just their activities ("What did you do online?").
- Creating a safe space where your children feel they can report any uncomfortable online interaction without fear of judgement or losing privileges. Reassure them, "No matter what, you can tell me anything, and we will face it together."
- Establishing family technology agreements (a shared "Digital Family Pact") that set clear expectations, boundaries, and consequences for online behaviour.
- Teaching children directly to recognise manipulation tactics and to trust their instincts if something feels "off" online.



+ Red Flag Detection Systems

Becoming a Digital Detective

Beyond software, your own observational skills are powerful.

Behavioural Pattern Recognition

- Notice subtle changes in their communication style or vocabulary, possibly influenced by new online contacts.
- Increased secrecy around topics they used to be open about (e.g., "who are you chatting with?").
- New interests or knowledge that seems age-inappropriate or concerning.
- Changes in their risk tolerance or decision-making patterns online.

Digital Forensics for Parents

- Learning to safely and transparently check browser history, app usage times, and privacy settings with your child, without compromising trust.
- Understanding how to document concerning online interactions (screenshots, saving messages) for potential reporting to authorities or platforms. This evidence is crucial.
- Knowing how to preserve evidence of cyberbullying or predatory behaviour without deleting crucial information.
- Understanding the legal implications of monitoring your child's digital activity in South Africa, ensuring you act within the bounds of the law while prioritising their safety.

BUILDING YOUR DEFENCE

Response Strategies and Resources When You Need to Act

Despite our best efforts, red flags might emerge. Knowing how to respond immediately and effectively is paramount.

+ Immediate Response Protocols

Becoming a Digital Detective

When You Detect Red Flags, here are step-by-step response plans for different scenarios:

For Suspected Predatory Contact

- 1.Document everything: Screenshot all communications, profiles, and anything suspicious. Do not delete anything. This is crucial evidence.
- 2.Avoid direct confrontation: Do NOT confront the predator yourself through your child's accounts. This can alert them and make them disappear or retaliate.
- 3.Contact local law enforcement immediately: If you suspect criminal activity, contact your local South African Police Service (SAPS) station or their Cyber Crime Unit. They have specific procedures for these cases.
- 4.Report to the platform: Use the platform's reporting mechanisms to report the individual.
- 5.Seek professional counseling: Your child might be traumatised. Find support from a qualified counsellor or child psychologist.

For Cyberbullying or Harassment:

- 1.Screenshot and save all evidence: Document every instance of harassment, including dates and times.
- 2.Block and report: Block the offending accounts on all platforms and report them to the respective platform administrators.
- 3.Contact school officials: If the harassment involves classmates or occurs during school hours, inform the school immediately.
- 4.Monitor emotional response: Closely observe your child's emotional state and seek counselling if needed.
- 5.Consider temporary restrictions: Temporarily limit or restrict social media use while actively addressing the situation.



+ Immediate Response Protocols

Becoming a Digital Detective

For Financial or Identity Theft Concerns

1. Immediately change passwords: Change passwords on all affected online accounts (email, social media, banking, gaming). Use strong, unique passwords.
2. Monitor financial accounts and credit reports: Regularly check your and your child's bank accounts, and if possible, place fraud alerts with credit bureaus.
3. Report to relevant authorities: Report identity theft to SAPS and to the Southern African Fraud Prevention Service (SAFPS).
4. Document suspicious activity: Keep detailed records of all suspicious activity with timestamps and screenshots.
5. Place fraud alerts: Consider placing fraud alerts on all family financial accounts.

+ Professional Resources and Support

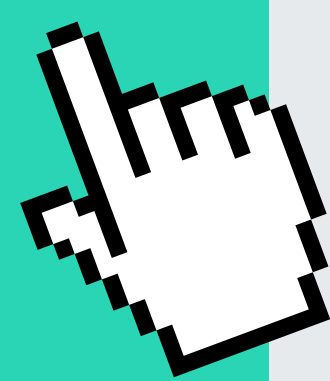
You Are Not Alone

Knowing when and where to get professional help is vital.

- Your child shows signs of trauma or severe emotional distress related to online experiences.
- You discover clear evidence of criminal activity targeting your child.
- Your child has shared personal information or explicit images with unknown individuals.
- Online interactions have led to real-world safety concerns.
- Your child expresses suicidal thoughts or self-harm intentions related to online experiences.

Reporting Mechanisms in South Africa

- **Platform-specific reporting procedures:** Familiarise yourself with how to report users on TikTok, Instagram, Roblox, etc. Understand their limitations.
- **SAPS Cyber Crime Unit:** For serious criminal activity, contact your local police or the dedicated SAPS Cyber Crime Unit.
- **School reporting:** For issues involving classmates, school-related harassment, or incidents impacting the school environment.
- **Child protection services:** The Department of Social Development in your province can provide assistance for suspected abuse or exploitation.
- **Internet safety organisations:** Local and international organisations offer support and resources. (e.g., Childline South Africa, Safer Internet Centre South Africa, or even contacting the international resources listed by Thorn or NCMEC, who have experience with global cases).





Building Long-Term Digital Resilience Empowering Our Children

Protecting our children online isn't a one-time fix; it's an ongoing journey. Our goal is to equip them with the resilience to navigate the digital world safely and independently.

+ Education and Prevention

Their Inner Shield

Education and Prevention: Their Inner Shield

Age-Appropriate Digital Literacy: Teach your children to recognise and respond to online threats. This includes:

- Understanding the permanence of digital communications and content ("Once it's online, it's out there forever").
- Recognising manipulation tactics and social engineering attempts.
- Learning to critically verify the identity of online contacts ("Are they really who they say they are?").
- Understanding the commercial motivations behind "free" online services (data collection, targeted ads).
- Developing critical thinking skills about online information and interactions ("Is this really true? What's the source?").

+ Staying Current with Emerging Threats

The Ever-Evolving Landscape

The digital threat landscape in South Africa and globally changes at lightning speed. Your commitment to continuous learning is crucial.

Continuous Learning for Parents

- Follow reputable cybersecurity and child safety organisations (like Tanosec) and local NGOs.
- Participate in school and community digital safety programs, often offered by local police or social services.
- Make an effort to understand new platforms and technologies before your children encounter them.
- Maintain relationships with other parents to share information and concerns, creating a community of vigilance.
- Regularly update your knowledge about current online trends and risks.

Creating a Family Digital Safety Culture

- Establish regular, open family discussions about online experiences. Make it a safe, non-judgmental space.
- Create an environment where children feel genuinely safe reporting any uncomfortable online interactions, knowing they won't be blamed.
- Model healthy digital behaviour and boundaries yourself. Put your phone away at dinner. Don't constantly scroll.
- Stay informed about new platforms and technologies your children are using. Ask them to show you!
- Balance safety with age-appropriate independence and privacy. As they grow, trust them with more responsibility, but keep the lines of communication open.

Adapting Strategies as Children Grow

- Adjust monitoring and communication strategies as your children mature. What works for a primary school child won't work for a teenager.
- Recognise when to transition from strict protection to a focus on education and empowerment, giving them the tools to make good choices.
- Maintain trust while ensuring safety across different developmental stages.
- Prepare children for independent digital decision-making as they approach adulthood, so they can navigate online challenges confidently on their own.



CONCLUSION

Empowering South African Parents & care givers in the Digital Age

The online safety landscape in 2025 presents both unprecedented challenges and opportunities for us, the parents and caregivers of South Africa. While the threats to our children have become more sophisticated, our understanding of these risks and the tools available to address them have also evolved.

The key to protecting our children online lies not just in monitoring and restriction, but in education, proactive communication, and building strong, trusting relationships that encourage our children to share their online experiences with us. By staying informed about current threats, maintaining open dialogue with our children, and wisely using appropriate technology tools, we can help them navigate the digital world safely.

Remember, perfect safety is impossible, but informed awareness and proactive engagement can significantly reduce risks. The goal is not to eliminate all online risks—which would also remove many of the incredible benefits of digital connectivity—but to help our children develop the skills and judgement they need to recognise and respond appropriately to dangerous situations.

As the digital landscape continues to evolve, so too must our approaches to keeping our children safe. This guide provides a strong foundation, but staying engaged with your child's digital life and remaining informed about new developments will always be essential components of effective online safety for your family.

The investment you make in understanding these threats and building strong communication with your children about their online experiences will pay dividends not just in their immediate safety, but in their long-term ability to navigate an increasingly complex digital world as independent, informed, and resilient individuals.

Stay Safe, Stay Informed



Additional Resources and Contact Information

When you face an online safety concern, knowing who to call is critical. Here's a list of essential contacts and resources, specifically for parents and caregivers in South Africa:

+ Immediate & Emergency Contacts

SAPS (South African Police Service)

- **National Emergency:** 10111 (For immediate emergencies or to report a crime in progress.)
- **Crime Stop (Tip-off Line):** 08600 10111 (For reporting criminal activities anonymously.)
- **SAPS Cyber Crime Unit:** While there isn't one single national contact number for the unit, reporting through your local police station is the first step. They will then escalate to the relevant cybercrime specialists.

Childline South Africa:

- **Toll-Free Helpline:** 08000 55 555 (Available 24 hours, 7 days a week, free from all networks. Provides counselling and assistance for matters related to abuse, bullying, substance abuse, human trafficking, and general advice for children.)
- **National Office:** (+27)-(0)31-201 2059 (General Enquiries)
- **Website:** www.childlinesa.org.za

Department of Social Development

- **Customer Care Helpline:** 012 312 7727
- Gender-Based Violence (GBV) Command Centre (includes support for child abuse):
- Toll-Free: 0800 428 428 (0800 GBV GBV)
- SMS: 32312
- Please Call Me: *120*7867# (free from any cell phone)
- The DSD is responsible for child protection services. Contact them if you suspect child abuse or neglect.

+ Financial & Identity Theft Concerns

Southern African Fraud Prevention Service (SAFPS)

- Helpline: 0860 101 248 (For reporting suspected fraud, especially identity theft.)
- Email: SAFPS@safps.org.za
- Website: www.safps.org.za

+ Mental Health & Support Services

TEARS Foundation

- Helpline (USSD): *134*7355# (Free, for victims of domestic violence, sexual assault, and child sexual abuse.)
- Tel: 010 590 5920
- Website: www.tears.co.za

The Teddy Bear Foundation

- Tel: 011 484 4554 (Office hours only)
- Specialised medico-legal clinic for children who have been abused or neglected, offering medical exams, forensic assessments, and therapeutic counselling.



+ General Online Safety & Education

Tanosec Cybersecurity

- Website: www.tanosec.co.za (Visit us for more guides, blog posts, info)
- Email: info@tanosec.co.za (For general enquiries and support.)
- Phone: +27 62 1234 244 if based in Bloemfontein
- Stay connected with our community and get updates on emerging threats relevant to South Africa.

UNICEF South Africa

- Website: www.unicef.org/southafrica (Offers online safety tips, resources, and reports on children's online behaviour in SA.)
- Safe Online Global: safeonline.global/unicef-south-africa (UNICEF's global initiative with information relevant to South Africa.)

+ General Online Safety & Education

The Cybersecurity Hub

- Website: www.cybersecurityhub.gov.za
- Email: info@cybersecurityhub.gov.za
- *South Africa's National Computer Security Incident Response Team (CSIRT), provides awareness and coordinates responses to cybersecurity threats*

THORN (Global Resource)

- Website: www.stopssextortion.com or www.thorn.org

While international, THORN provides invaluable resources, tools (like "Take It Down" for image removal), and support for sextortion victims globally.

BUILDING YOUR DEFENCE

About Tanosec Cybersecurity



At Tanosec, we believe that navigating the digital world should not be a source of fear, but a realm of opportunity and connection, especially for our children. Located in the heart of South Africa, we are more than just a cybersecurity company; we are a community-driven initiative passionately committed to making the digital landscape safer for everyone, from individuals and families to small businesses and larger enterprises.

Our mission is simple yet profound: To empower South Africans with the knowledge, tools, and confidence to thrive securely in the digital age. We strive to:

- **Educate:** Provide clear, actionable, and up-to-date information on online threats and best practices.
- **Protect:** Offer cybersecurity solutions that safeguard personal data, devices, and digital identities.
- **Empower:** Equip individuals, families, and organisations with the resilience to identify, prevent, and respond to cyber risks.
- **Support:** Be a trusted resource, offering guidance and assistance when digital challenges arise.



- Website: <https://tanosec.co.za>
- Email: info@tanosec.co.za
- Phone: +27 68 629 5030
- Follow us on socials for regular cybersecurity updates and tips or visit our website for more free resources.