

Unlimited but Unprotected

The Security Gap of Unfiltered Internet Access in
Somalia

Somalia does not need less internet. Somalia
needs a safer internet.

Affordable. Accessible. Secure. Protected.



The Opening Challenge

**Somalia has succeeded in expanding access.
Have we built the security layer needed to
protect the people using it?**



The goal is not to control the internet. The goal is to reduce preventable harm while preserving openness, access and innovation.

Why This Conversation Matters Now

5.47M

Internet users

Somalia, Oct 2025

11.5M

Mobile connections

58.1% of population

3.51M

Social-media user identities

15.6

Median age

Half the population younger



A young, mobile-first society means online safety is not a future issue — it is a present public-interest issue.

Somalia's Digital Transformation: Access Is Growing

Digital transformation is already part of Somalia's economy and public-service agenda.

Connectivity

Mobile internet, fixed broadband and submarine-cable investments expand digital reach.

Public services

Digital ID, payment systems and e-government plans increase dependence on secure infrastructure.

Finance

Mobile money and digital payments make online trust and fraud prevention economically significant.

Institutional capacity

NCA plans include CSIRT, cybersecurity governance and regulatory modernization.

The opportunity is real. The security model must mature at the same time as access, payments, platforms and services.

Internet Penetration:

Internet users

5.47 million

Total population

19.8 million

$$5.47\text{M} \div 19.8\text{M} \times 100 = 27.6\%$$

International comparison: internet penetration



Important distinction: mobile connections, broadband-capable mobile connections, social-media identities and internet users are different indicators.

The Price of Internet: Low Cost Is an Opportunity

ITU 2025 data-only mobile-broadband basket: Somalia 5GB = US\$2.00 → US\$0.40/GB equivalent

Selected low-cost markets — standardized price per 1GB



Somalia ranking

#10

globally among the cheapest economies in a
StatRanker table computed from ITU 2025
basket data

Low cost expands opportunity. Low cost + high availability + weak safeguards expands exposure.

Affordable Internet Must Become Protected Internet

Affordable + Accessible

- ✓ More students online
- ✓ More businesses digital
- ✓ More mobile payments
- ✓ More public-service access



Unprotected + Unfiltered

- ⚠ Phishing and impersonation
- ⚠ Malware and fake apps
- ⚠ Gambling and harmful content
- ⚠ Fraudulent ads and social engineering

The policy issue is not access. The policy issue is access without proportional safeguards.

What “Unfiltered Internet” Actually Means

- | | | |
|---|----------------------------|--|
| 7 | Platform controls | Moderation, fraud detection, age tools |
| 6 | Endpoint protection | Phones, laptops, institutional devices |
| 5 | Content/category filtering | Policies by age, network or institution |
| 4 | Application control | App/protocol identification and policy |
| 3 | Secure Web Gateway | URL categories: malware, phishing, adult, gambling |
| 2 | IP/domain reputation | Threat-intelligence blocking |
| 1 | DNS security | Malware, phishing, C2 and scam domains |

Filtering is not one switch. It is a layered control model with different owners, limits and safeguards.

WHAT "UNFILTERED INTERNET" ACTUALLY MEANS

Protection operates in layers, not one switch

01

DNS security

Blocks known malware, phishing, scam and command-and-control domains before connection.

02

IP / domain reputation

Threat-intelligence feeds identify and block known malicious infrastructure.

03

Secure web gateway / URL filtering

Categorises destinations: malware, phishing, fraud, gambling, adult content, illegal markets.

04

Application control

Identifies and manages specific applications or protocols crossing the network.

05

Content / category filtering

Applies policy by organisation, network, age group, institution or user type.

06

Endpoint protection

Controls applied directly on phones, laptops, university and government devices.

07

Platform-level controls

Facebook, TikTok, YouTube, Instagram, Google and messaging apps run their own moderation — separate from ISP filtering.

ISP filtering ≠ platform moderation

The two operate at different layers, with different tools and different responsible parties.

Risk Landscape: Ordinary Users, Real Threats

Online scams & fraud

Fake shops, investment scams, romance, jobs, scholarships, mobile-payment fraud

Phishing & credentials

Fake login pages, account takeover, impersonation, payment redirection

Gambling exposure

Sports betting sites, ads, mobile access, youth exposure

Harmful content

Adult content, graphic violence, exploitative communities, cyberbullying

Malware

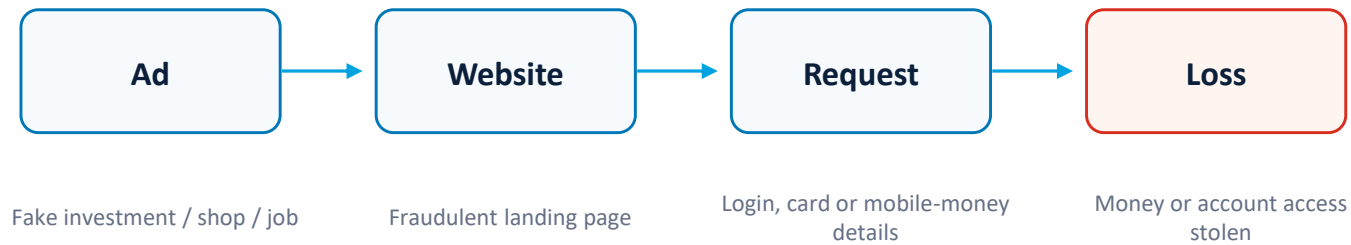
Malicious APKs, trojans, stealers, ransomware, fake downloads

Social-media abuse

Fake accounts, fraudulent ads, harassment, manipulative links

The exposure environment is created by websites, apps, ads, messaging links, social platforms and malicious infrastructure — not by “the internet” as a single object.

Scenario 1: Social-Media Scam Funnel



Where controls can interrupt the scam

Platform ad review

Domain reputation

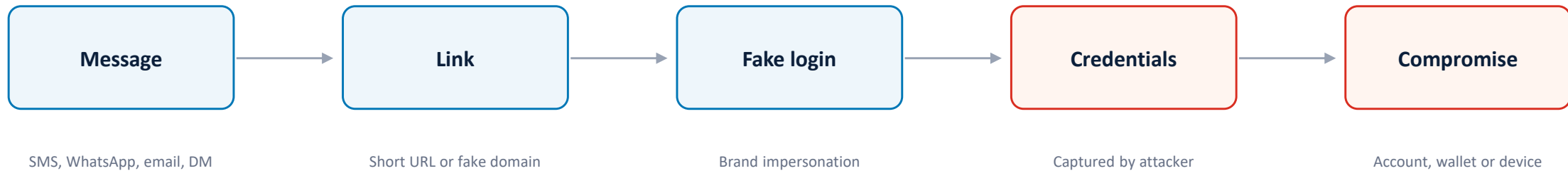
Protective DNS

Browser warnings

MFA + user awareness

Abuse reporting

Scenario 2: Phishing and Malware Attack Chain



Security controls that can stop or reduce impact

DNS filtering

Blocks known malicious domains before connection

Threat intelligence

Detects reputation, lookalike and C2 infrastructure

MFA

Limits damage when passwords are stolen

Endpoint protection

Detects malware and malicious APKs

User awareness

Reduces link-click and credential submission

Reporting

Feeds removal and enforcement

Social-Media Risks: High Reach, Limited ISP Visibility



Common social-media exposure

- Fraudulent advertisements and fake shops
- Impersonation and fake accounts
- Manipulative links and account takeover
- Cyberbullying and harassment
- Dangerous trends and harmful recommendations

ISPs can often see domains and network patterns, but not every individual encrypted post, video or private message inside a platform.

Youth and Harmful-Content Exposure

15.6

Median age

Somalia, Oct 2025

53.0%

Age 0–17

0–4 + 5–12 + 13–17

64.1%

Social-media share of internet user base

user identities / users

37.7%

TikTok adult ad reach

Adults 18+

Adult material

Graphic violence

Harmful challenges

Exploitative content

Cyberbullying

Dangerous communities

Manipulative recommendations

Child online protection is a governance, education, platform, network and family issue — not only a blocking issue.

Not Everything Is “Internet Blocking”

Cybersecurity filtering

Known malware, phishing, scam and C2 infrastructure

Example: DNS blocks a phishing domain

Illegal-content restriction

Content prohibited under applicable law and lawful process

Example: legally authorized blocking request

Child / institutional filtering

Policies for schools, families, universities and public networks

Example: family-safe or campus profile

Platform moderation

Community standards, fraud detection, age tools and ad enforcement

Example: platform removes scam account

Separating these concepts is essential for credibility, proportionality and public trust.

Can Somalia Simply Filter Social Media at ISP Level?

Not completely.

Modern services predominantly use encrypted HTTPS and platform-controlled architectures.

ISP often can identify

- ✓ Domain names
- ✓ IP addresses
- ✓ Known malicious destinations
- ✓ Some app/network characteristics

ISP generally cannot inspect

- × Individual Facebook posts
- × TikTok videos
- × WhatsApp messages
- × Instagram posts
- × YouTube recommendations

Effective protection requires Government + Regulator + ISPs + Platforms + Universities + Cybersecurity teams + Families + Users.

INTERNATIONAL CASE STUDY

Japan — carrier filtering, not platform bans

Legal foundation

2008 Act on Development of an Internet Environment for Young People (revised 2018): mobile carriers must provide default content filtering for under-18 contracts; guardians may opt out.

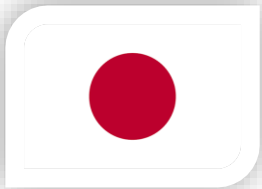
Platform accountability

2025 Information Distribution Platform Act designates large platforms (Google, LINE, Yahoo, Meta, TikTok, X) for expedited takedown and transparency duties.

What it avoids

No nationwide social-media ban for minors; no mandatory identity-based age verification; filtering is default-on but user/guardian adjustable.

ISPs also voluntarily filter known child-sexual-abuse-material domains through the Internet Content Safety Association — a cybersecurity filtering function, distinct from the youth-content filtering above.



INTERNATIONAL CASE STUDY

United Arab Emirates — codified categories, active enforcement

Regulatory structure

TDRA's Internet Access Management policy defines a published list of prohibited-content categories; licensed ISPs (Etisalat, du) must block per TDRA direction using DNS, IP, URL and deep-packet-inspection filtering.

Reported enforcement scale

TDRA reported blocking 7,289 websites in Q2 2025 across 17 categories — drugs and gambling each 30.24%, fraud/impersonation/phishing 26.48%.

Child digital safety

Federal Decree-Law No. 26 of 2025 requires platforms to verify age and protect under-13 users' data, or face blocking.

Cybersecurity filtering (malware, phishing infrastructure) and broader public-morality content categories are governed under the same TDRA process — a reminder that codifying and separating these categories clearly, as this talk recommends, is not automatic even in mature regulatory systems.



INTERNATIONAL CASE STUDY

Saudi Arabia — a dedicated national cybersecurity authority

Legal foundation

Anti-Cyber Crime Law, enacted 2007 and revised 2015 — the cornerstone cybercrime statute addressing unauthorised access, fraud and data interference.

Institutional structure

National Cybersecurity Authority (NCA), established 2017, issues Essential Cybersecurity Controls (ECC-1: 2018; updated ECC-2: 2024) for government and critical-infrastructure entities.

Sector regulation

Communications, Space & Technology Commission (CST, formerly CITC) runs a dedicated Cybersecurity Regulatory Framework (2020) for the ICT and telecom sector.

The structural takeaway is institutional separation of duties: one authority (NCA) sets cross-government cybersecurity standards, while the sector regulator (CST) governs telecom-specific cybersecurity obligations — a division of labour Somalia's own NCA is now beginning to take on in a single body.



SOMALIA'S INSTITUTIONAL MOMENTUM

The foundations are already being built

2017	2023	AUG 2025	NOV 2025	JAN 2026	MAR 2026
Communications Act establishes the National Communications Authority (NCA)	Data Protection Law enters into force; Data Protection Agency (DPA) created	Cybercrime bill approved by authorities	E-visa system breach exposes personal data of an estimated 35,000 applicants	Parliament approves Somalia's Cybersecurity Law	SOMCIRT (national incident-response centre) launched; NCA runs public-sector cyber training

This talk is not arguing for a framework Somalia lacks entirely — it is arguing for finishing, coordinating and resourcing a framework that has already begun. The task now is turning these legal and institutional building blocks into operating capability.



International Comparison: Different Models, Different Lessons

Area	Somalia	Japan	UAE	Saudi Arabia
Internet penetration	27.6%	87.0%	99.0%	99.0%
Regulatory approach	Developing framework	Youth safety + private sector	Regulator-defined access policy	Central filtering + cybercrime law
Cyber-threat filtering	Baseline to assess	Carrier/institution options	Licensee implementation	Regulator/provider filtering
Child protection	Needs stronger framework	Legal basis + filtering promotion	Category controls	Legal/category restrictions
ISP role	Minimum standards needed	Filtering options for minors	Licensee obligations	Provider implementation
Digital literacy	Priority gap	Education and awareness	Policy-oriented	Policy-oriented
Reporting mechanisms	Need structured channels	Consumer/family tools	Blocking/unblocking requests	Blocking/unblocking service

The lesson is not “which country is best.” The lesson is that Somalia needs a proportional model suited to its infrastructure, law, capacity and society.

Somalia Safer Internet Security Architecture

National / Regulatory

Online-safety framework • cybercrime enforcement • child protection • ISP minimum cybersecurity standards

ISP / Telecom

Protective DNS • reputation filtering • anti-phishing • botnet/C2 blocking • DDoS • abuse reporting

Platform

Scam accounts • fraudulent ads • impersonation • harmful content • child-safety referrals

Institution

Schools, universities, agencies and businesses: secure DNS • firewalls • SWG • endpoint protection • logging

User

MFA • parental controls • SafeSearch • privacy settings • scam recognition • reporting

The architecture combines governance, network controls, platform cooperation, institutional security and user empowerment.

Practical Technology Options: What They Can and Cannot Do

Protective DNS

Can: Blocks known malicious domains; low-cost first layer

Cannot: Cannot see every encrypted app action

Secure Web Gateway

Can: URL/category policy, malware/phishing control

Cannot: Needs policy design and operational capacity

NGFW / IDS / IPS

Can: Network visibility, intrusion detection, policy enforcement

Cannot: Cannot replace endpoint and platform controls

Endpoint protection / MDM

Can: Protects devices and manages institutional assets

Cannot: Requires device ownership or user consent

SafeSearch / Restricted Mode

Can: Useful for schools/families; reduces inappropriate search/video exposure

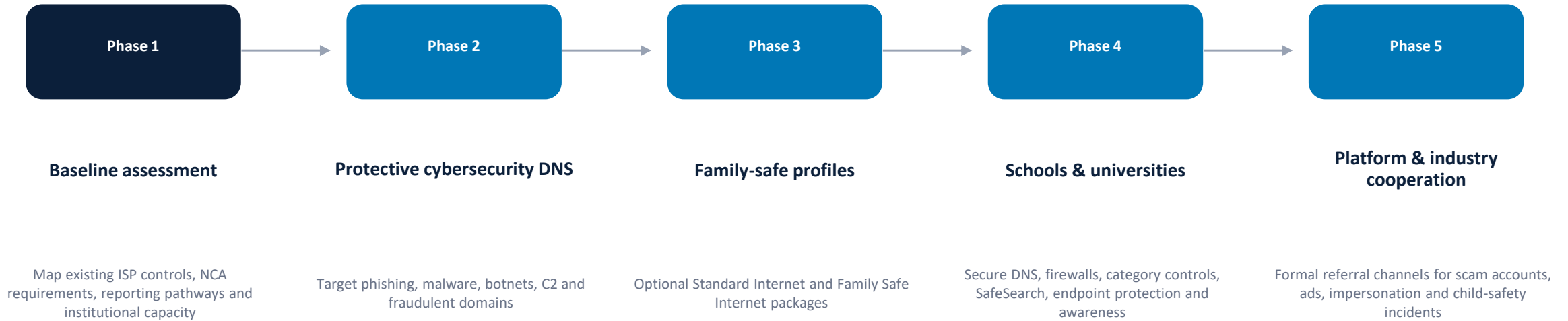
Cannot: Not complete; can be bypassed without controls

Platform cooperation

Can: Removes scam accounts, ads and harmful content at source

Cannot: Requires escalation channels and evidence quality

Implementation Model:



The safest path is incremental: secure the clearly malicious first, then expand voluntary and institutional protections with safeguards.

Security Without Overreach

Transparency

Legal authority

Due process

Proportionality

Accountability

Clear categories

Independent review

Appeals

Error correction

Privacy

Freedom of expression

What to avoid

Arbitrary blocking • unclear categories • no appeal path • poor documentation • overbroad technical rules

What to build

Defined legal process • technical precision • public reporting • auditability • trusted correction mechanisms

The goal should not be to build a closed internet. The goal should be to build a safer internet.



Somalia does not need less internet.

Somalia needs a safer internet.

Affordable. Accessible. Secure. Protected.

As Somalia expands digital access, can cybersecurity and online protection grow at the same speed?