knowbe4

September 2026

Crime or Career?

Youth voices on cybercrime across the Global South

What's Inside

Executive Summary **3**

1. Introduction and Background **4**

Contributors 4

2. Results **5**

2.1 Who Took Part 5

2.2 How Common is it For a Young Person to Get Involved in Cybercrime? 9

2.3 What Types Of Scams Do Young People See in Their Communities? 10

2.4 What Draws Young People In 11

2.5 Who Recruits, and Where? 12

2.6 How it is Framed 14

2.7 How Offenders Are Seen, and How Communities React 16

2.8 What Young People Say Would Help 18

2.9 How Worried Respondents Are 19

3. Discussion And Conclusion **20**

3.1 Two Engines, Not One 20

3.2 Where Crime is Admired, Fear Does Not Compete 21

3.3 It Does Not Look Like A Crime; it Looks Like a Job 22

3.4 Recruitment Runs On the Platforms Young People Already Use 22

3.5 What Young People Are Asking For 23

3.6 The Honest Limit 24

4. Recommendations **25**

5. Limitations **26**

6. Acknowledgements **27**

7. Methodology **28**

Survey Design 28

Sample and Recruitment 28

Data Collection, Consent and Anonymity 29

Analysis Approach 29

References 30

Executive Summary

In June 2026 the Global South CAN (Cyber Academies Network) surveyed 238 young people and youth-facing practitioners about cybercrime in their own communities: what draws a young person in, who approaches them, how the offer is framed, how offenders are regarded, and what would help. Of those, 119 responded from Latin America, 90 from South Africa, and 29 from The Hacking Games community across a mix of other regions. This report describes what they told us. It measures perception, not incidence. These are the beliefs young people hold about their own environment, and on their own account. Five findings stand out.

1. Economic pressure is the strongest reported driver in South Africa

Survival or supporting family was selected by 77% of South African and 61% of LATAM respondents, and lack of jobs by 74% and 61%. Curiosity or testing skills leads the LATAM list at 64%, against 40% in South Africa.

2. Recruitment does not look like crime

Nearly four in five South African respondents (78%) and 56% in LATAM said involvement is presented as a normal online job. Fake online job offers are the single most-reported crime type among respondents from South Africa (82%) and in the other-regions group (83%).

3. Where offenders are admired, deterrence has less to work with

Asked how a community reacts when a young person suddenly makes unexplained money online, 46% of South African respondents said the person is admired or treated as a role model, against 19% in LATAM. LATAM respondents were far more likely to reach for the word “criminal” (56% vs 32%). It is one of the sharpest attitudinal splits in the data, alongside “confident and bold” (41% South Africa against 8% LATAM).

4. Recruitment happens on mainstream platforms, not hidden ones

WhatsApp leads in both focal regions (72% LATAM, 71% South Africa). The regional differences are in the second tier: Telegram (61% LATAM vs 31% South Africa) and Discord (41% vs 23%) against TikTok (53% South Africa vs 29% LATAM).

5. What respondents ask for is opportunity and someone who invests in them

Jobs and income tops the list in every group (91% LATAM, 87% South Africa, 83% other), with skills training and cyber education close behind. Mentorship (54% vs 32%) and community support (53% vs 32%) are markedly more sought in South Africa.

The practical implication runs through the whole report: if the criminal pipeline recruits on opportunity, status and belonging, prevention has to compete on the same terms. It has to out-recruit, not only out-threaten. Where a young person is admired for what they are doing, a warning message is not a deterrent; it can even become a badge.

Findings from the Global South CAN survey, June 2026

N = 238 respondents · Latin America, South Africa and other regions in preparation for a talk delivered at the 7th International Cyber Offender Prevention Network (InterCOP) Conference, held from 15–16 July 2026 at INTERPOL Headquarters in Lyon. France.

1. Introduction and Background

Most of what the cybercrime-prevention field knows about young offenders comes from the Global North. Longitudinal pathway studies, offender interviews, diversion programmes with published evaluations: a lot of it is European, British, Nordic or North American. That evidence base is good, but it travels less well than we assume.

At the InterCOP conference in Lyon in July 2026, session after session converged on a similar profile of the young person entering cyber-dependent crime: curiosity about computers beginning around age ten, gaming and cheat markets as the on-ramp, and a need for recognition and belonging that the offending community supplies. Prof Eric Leukfeldt's work on Dutch pathways and Finland's national youth survey both point that way, and the age brackets keep coming down: Finland skewed towards 13–14, France 13–23, and some offenders in "the Com" reported as young as 11.

Dr Suleman Lazarus's fieldwork on West African "Hustle Kingdoms"; fraud academies that operate like schools, supplying the income, status, structure and career path the formal economy does not, reveals a second engine. Where the Northern literature finds curiosity and recognition, much of the South finds survival and aspiration. Those two engines call for different interventions, and a prevention model based on only one may misfire on the other.

This survey was designed to provide youth voices from the Global South as contributors. It asked four questions:

- What do young people believe draws their peers into cybercrime?
- Who approaches them, on which platforms, and how is the offer framed?
- How are people behind these crimes regarded in their communities?
- What would help

This is a perception survey with a self-selected sample, drawn largely from students in the Global South CAN, such as the Information Security and Risk Institute (IRSI) in LATAM, MiDO Cyber Academy and Absa Cyber Academy in South Africa and from The Hacking Games global community, and it is not representative of youth in either region. What it does provide, however, is a signal: young people's own accounts of how their environment responds to cybercrime.

Our Contributors

Author

Anna Collard | SVP & CISO Advisor

With the Help of KnowBe4 Africa Autumn Interns:

Relebohile Senatsi

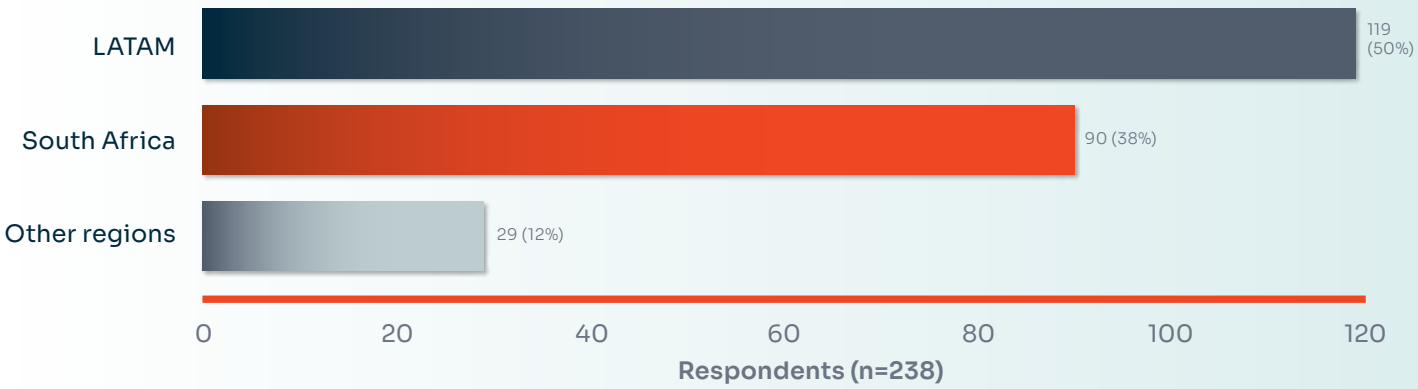
Lebohang Selela

Lwando Ntontela

2. Results

2.1 Who Took Part

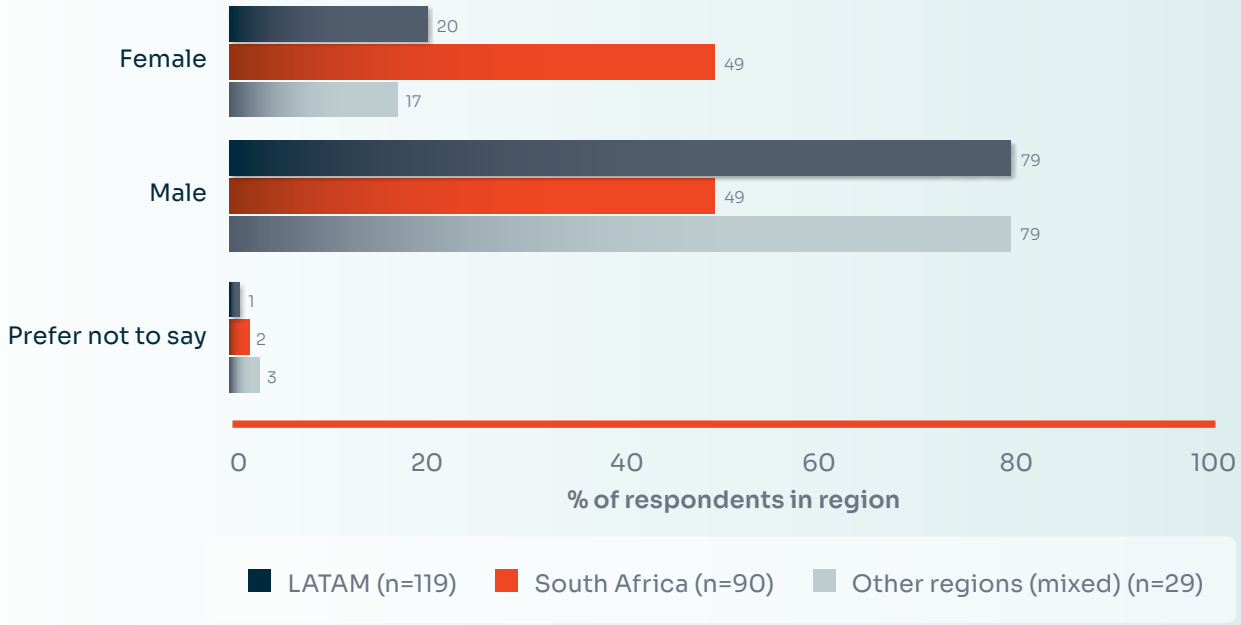
Fig 1. Regional Distribution of the 238 Respondents



Latin America supplied half the sample (119, 50%), South Africa 38% (90) and the mixed other-regions group 12% (29). The two focal regions together account for 88% of all responses. Any statement about the third group rests on 29 people and is presented for context only.

Respondents are young across all three groups: 18–34 year olds account for 94% of LATAM, 92% of South Africa and 97% of the other-regions group.

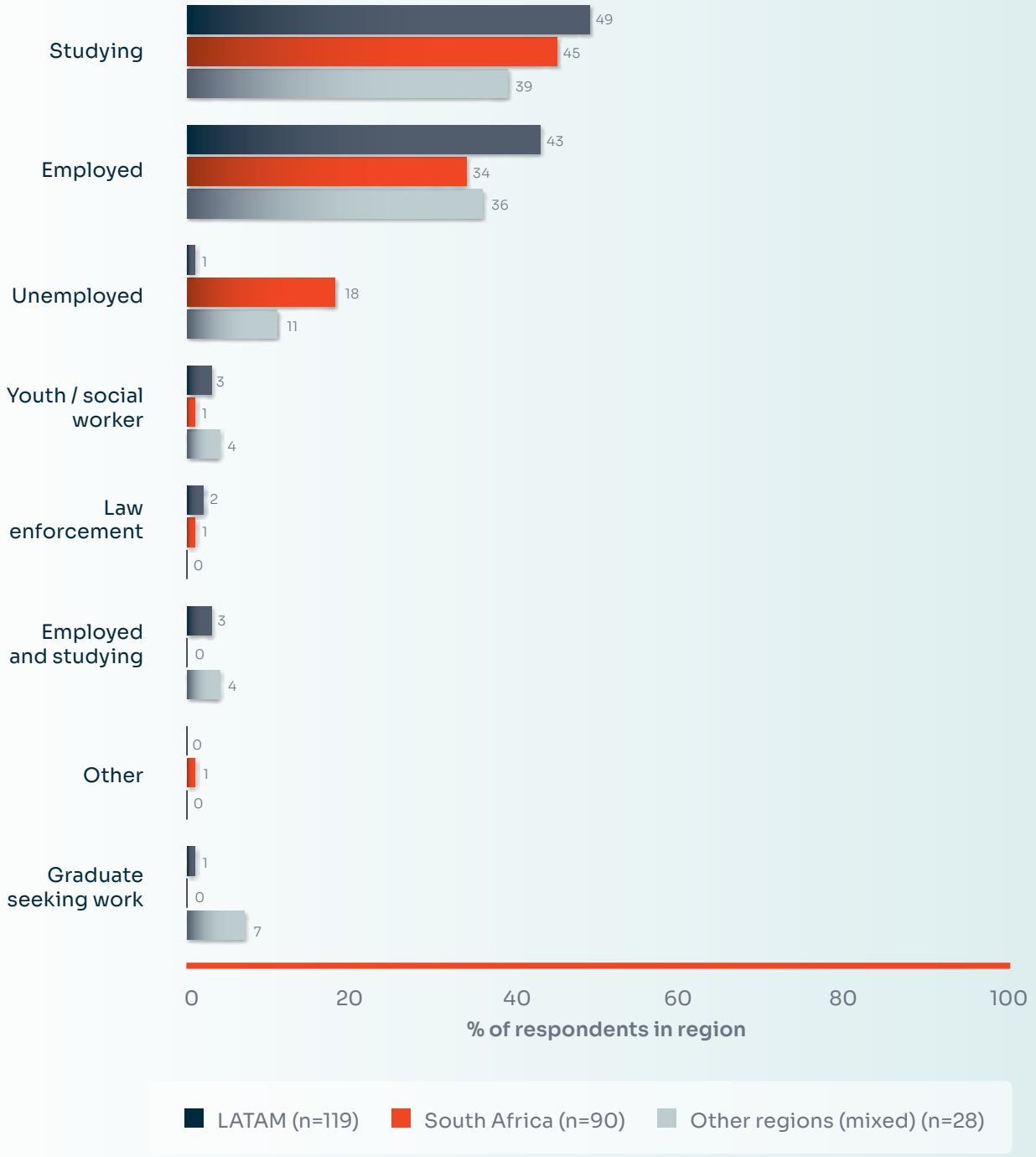
Fig 2. Gender Distribution Within Each Region, as a Percentage of Respondents In Region



South Africa is evenly split (49% female, 49% male, with 2% prefer not to say),. LATAM and the other-regions group are heavily male (79% each). Because two thirds of the total sample is male, findings should not be read as gender-balanced; this is listed as a limitation in section 5. It also matters substantively, because networks are known to recruit young women for social-engineering roles, and a male-weighted sample will under-see that.

Fig 3. Respondent Profile Within Each Region, Harmonised into Eight Categories

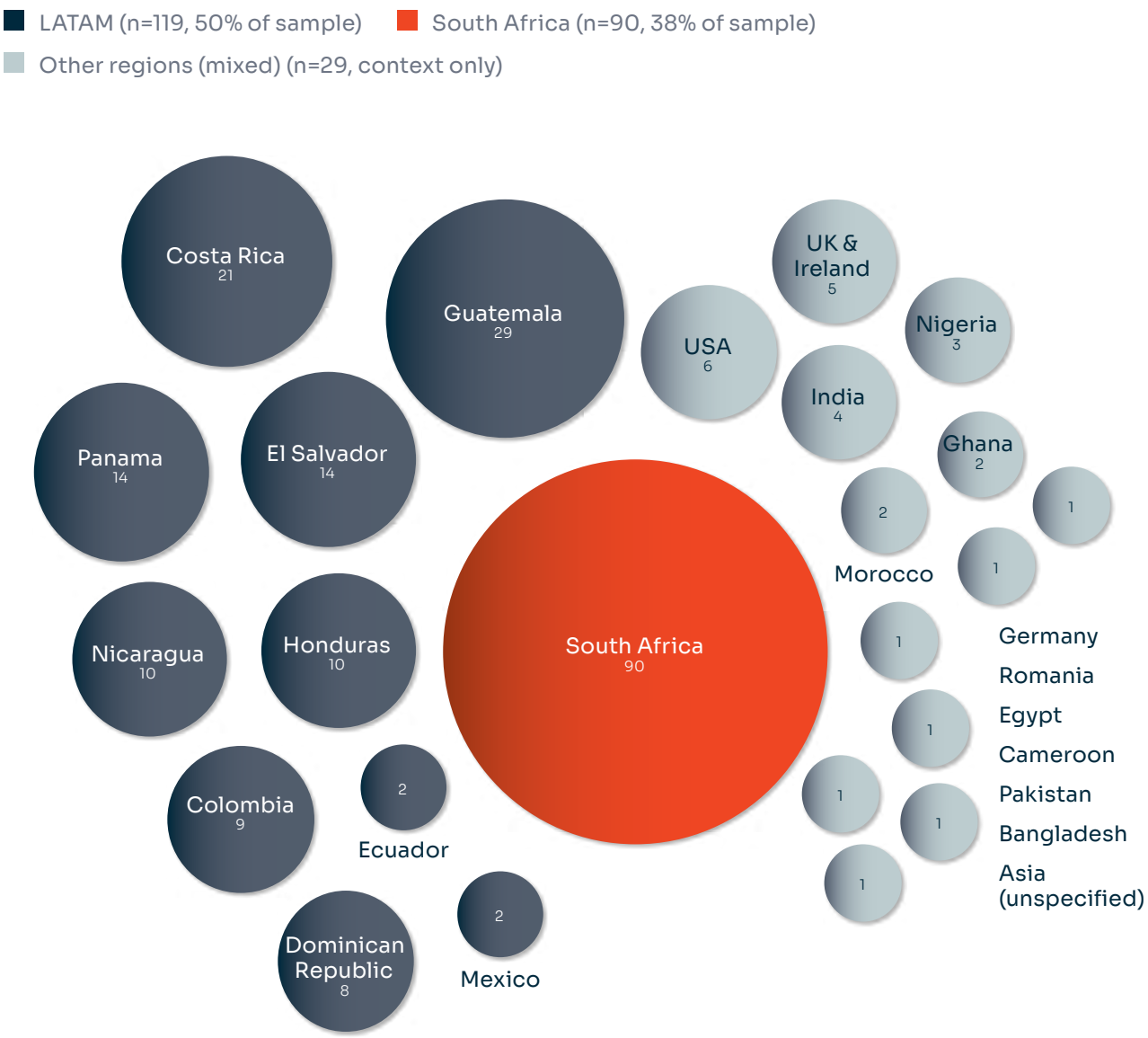
Bases: LATAM 119, South Africa 90, other regions 28. One South African respondent selected “disability” and two respondents did not choose an answer.



Students form the largest group everywhere (49% LATAM, 45% South Africa, 39% other regions), followed by employed young people. The clearest structural difference is unemployment: 18% of South African respondents describe themselves as unemployed and not studying, against 1% in LATAM. The sample also contains a small number of youth workers, social workers and police officers, whose answers are observations about young people rather than about themselves.

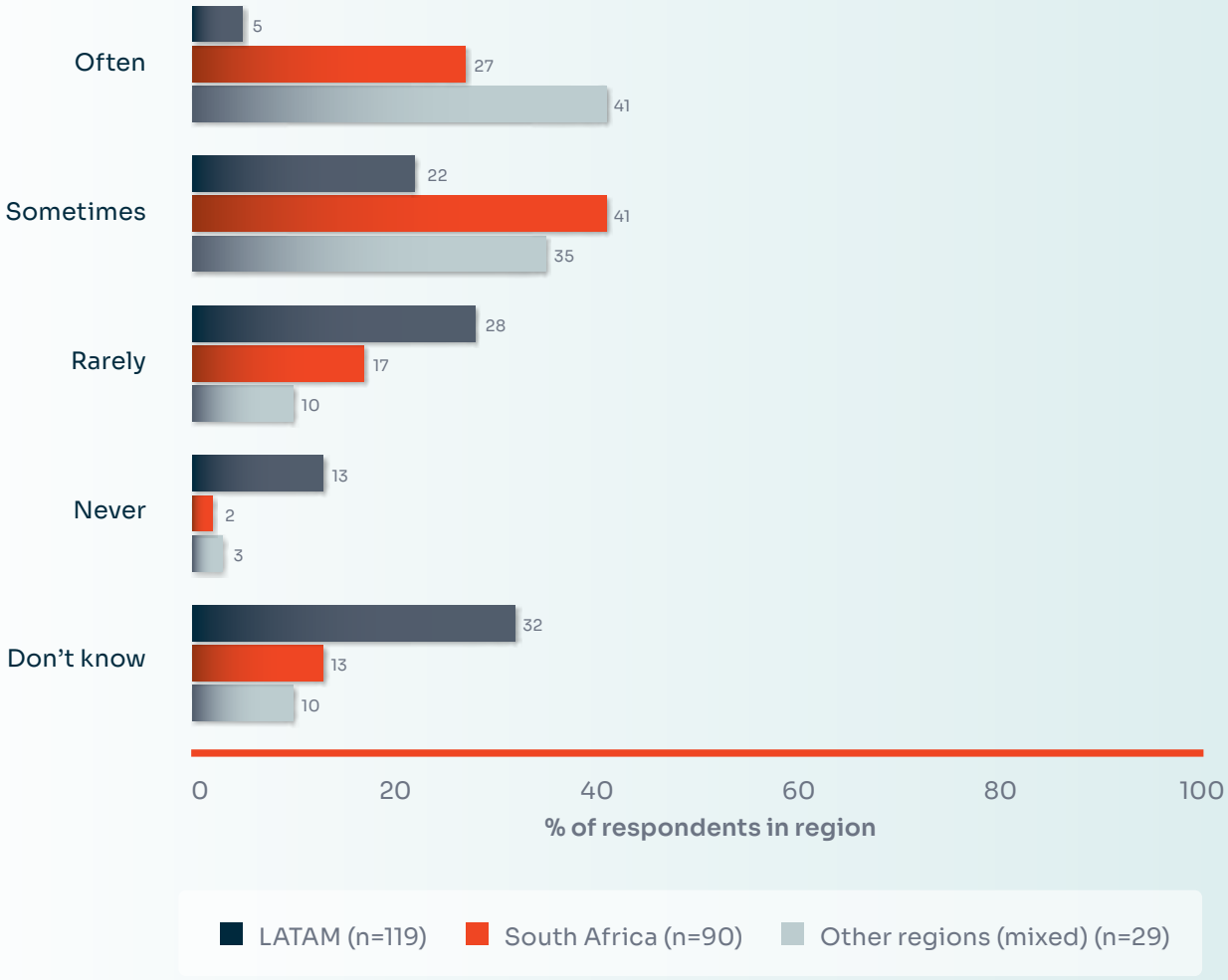
Fig 4: Where the Voices Came From

Respondents by country and region - Global South CAN survey, June 2026



2.2 How Common is it For a Young Person to Get Involved in Cybercrime?

Fig 5. How Often do Young People in Your Community get Involved in Cybercrime

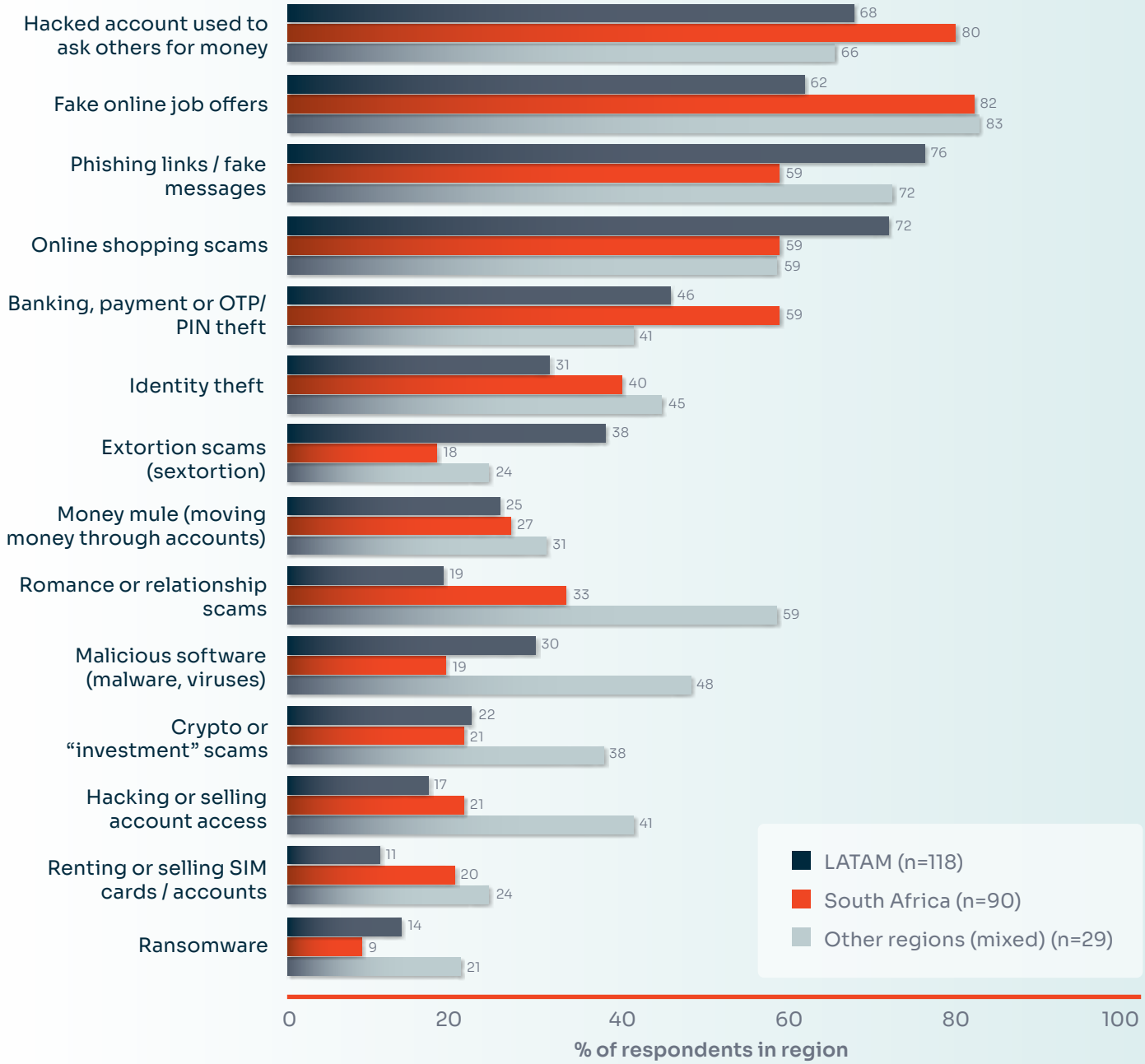


Two thirds of South African respondents said "often" or "sometimes" (68%), against 27% in LATAM, where the largest single answer was "I don't know" (32%) followed by "rarely" (28%). In the other-regions group 76% said often or sometimes. The open-ended answers corroborate the gap: roughly three in ten LATAM respondents volunteered that they had not seen or heard of anything, against fewer than one in ten in South Africa.

2.3 What Types of Scams do Young People See in Their Communities?

Fig 6. Types Of Online Crime Respondents Have Seen or Heard About Most in Their Community

Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%.
Bases: LATAM 118, South Africa 90, other regions 29.

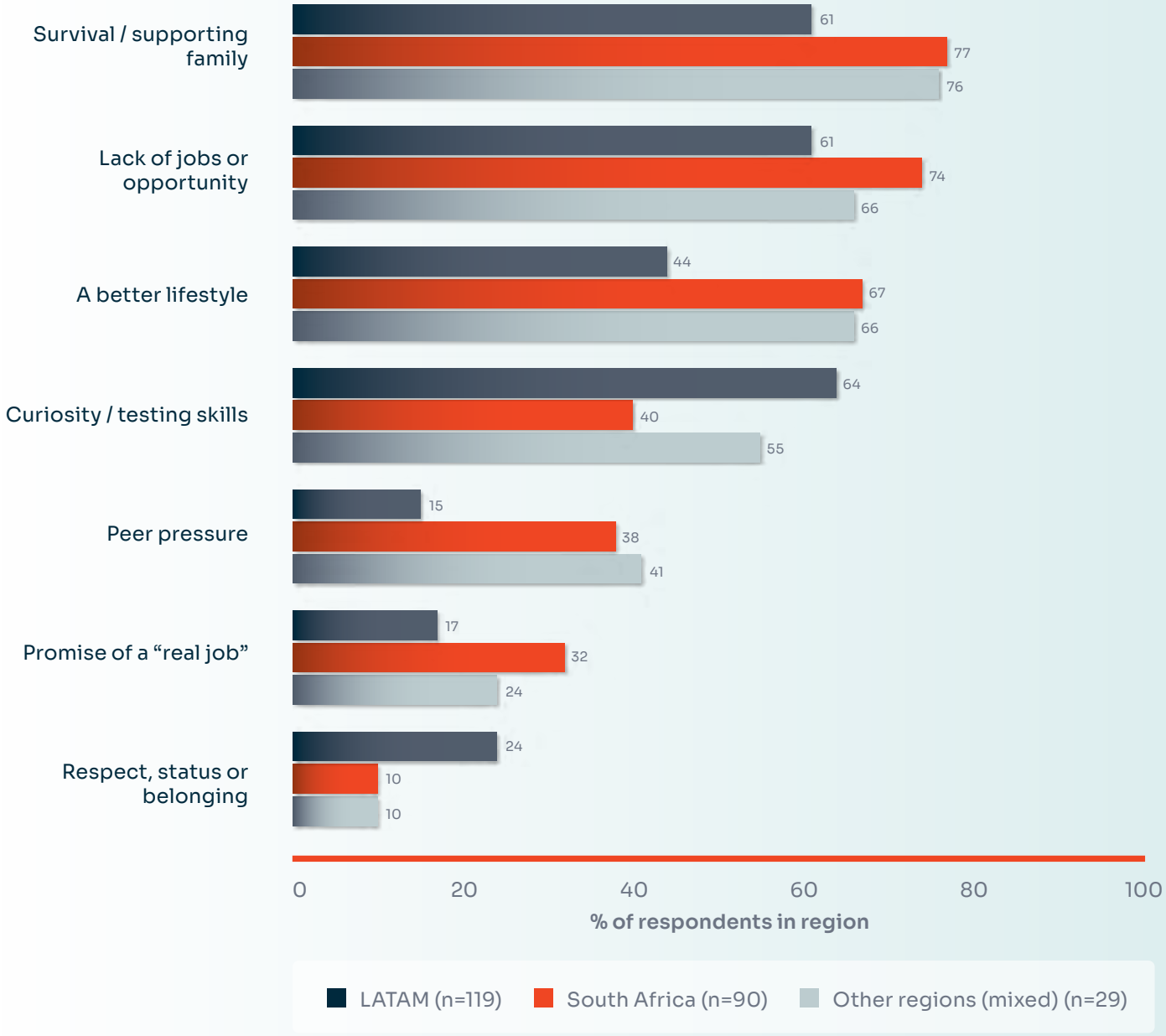


Fake online job offers are the most-reported crime type in South Africa (82%) and in the other-regions group (83%), and rank fourth in LATAM (62%), where phishing (76%) and online shopping scams (72%) come first. Hacked accounts used to solicit money from contacts are near the top everywhere (68% LATAM, 80% South Africa). Banking, payment and OTP/PIN theft is reported by 59% of South African respondents. Money-mule activity (25–31%) and SIM-card or account renting (11–24%) are reported at lower but non-trivial rates in all groups.

2.4 What Draws Young People in

Fig 7. What Respondents Believe Most Draws a Young Person Into Cybercrime (up to 3 choices with multiple choices allowed).

Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%.
Bases: LATAM 119, South Africa 90, other regions 29.

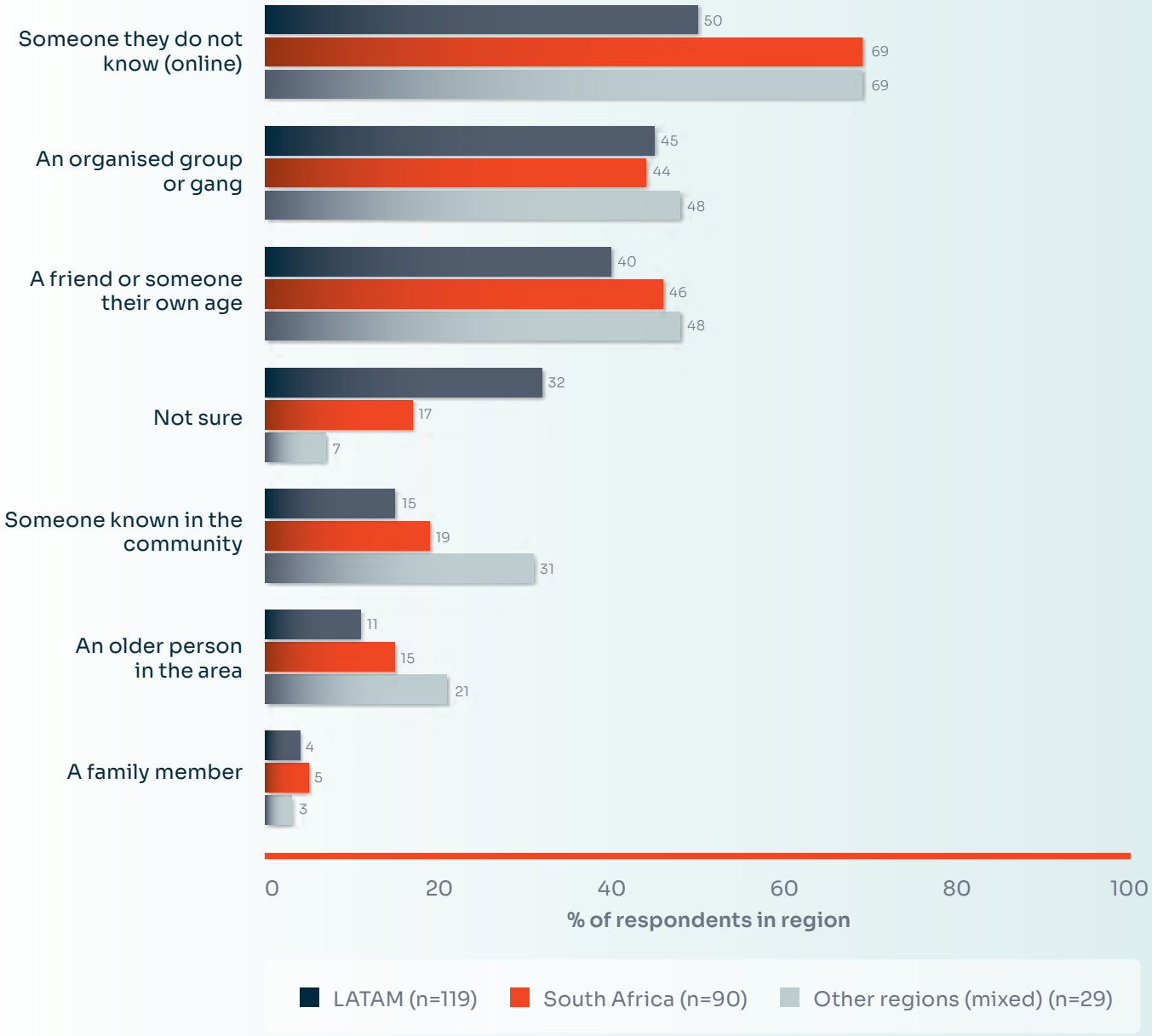


The two regions agree that economics dominates: survival or supporting family (77% South Africa, 61% LATAM) and lack of jobs or opportunity (74% and 61%) are the top two in South Africa and the joint-second pair in LATAM, just behind curiosity. They diverge on curiosity or testing skills, which is the single most-selected driver in LATAM (64%) but only 40% in South Africa, while a better lifestyle runs the other way (67% South Africa, 44% LATAM). Peer pressure is more than twice as prominent in South Africa (38% vs 15%); respect, status or belonging is more prominent in LATAM (24% vs 10%).

2.5 Who Recruits, and Where?

Fig 8. Who Respondents Believe Usually Approaches Young People About Getting Involved.

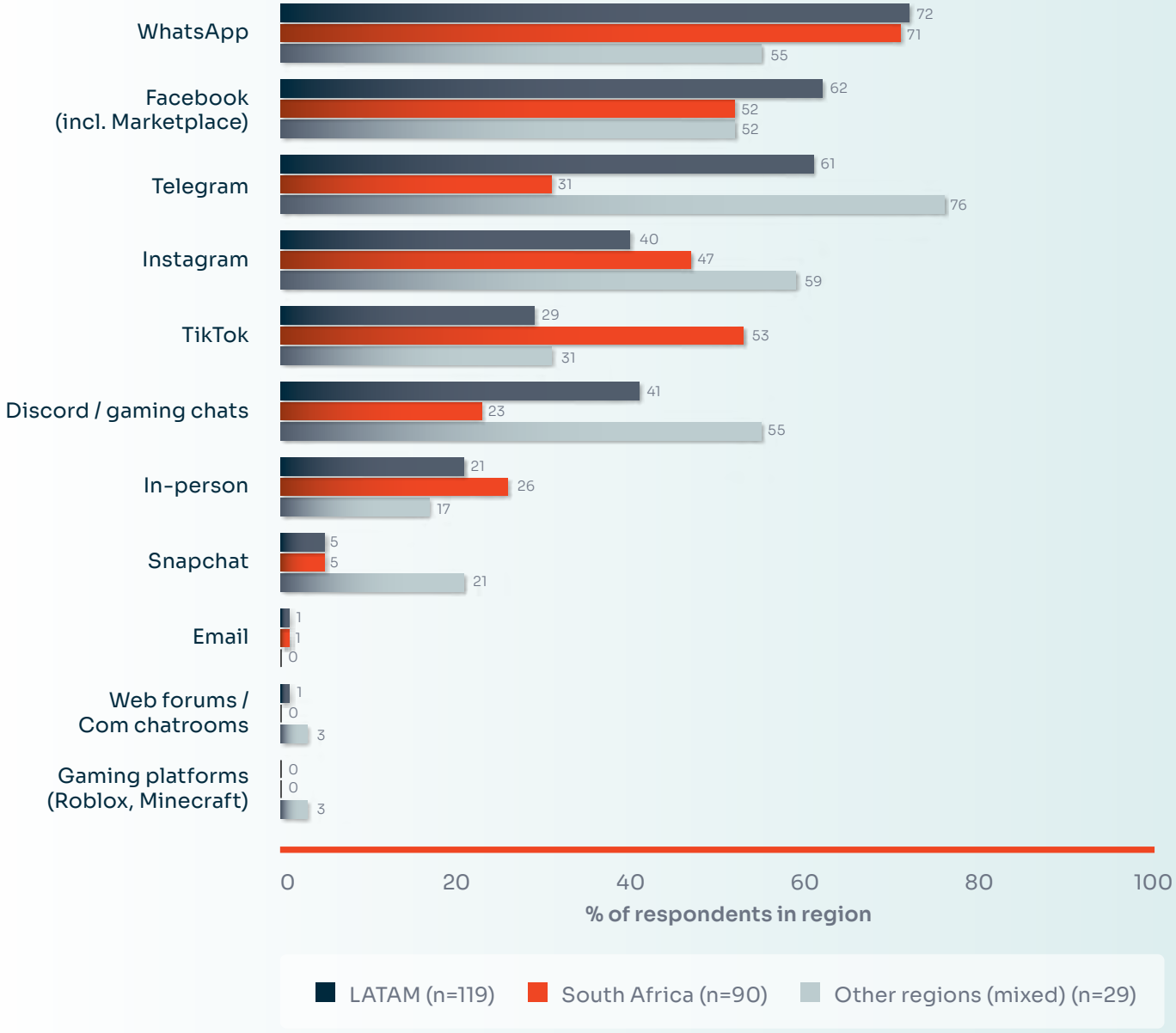
Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%.
Bases: LATAM 119, South Africa 90, other regions 29.



A stranger online is the most-selected recruiter in every group (69% South Africa, 50% LATAM). Organised groups or gangs (44–48%) and friends of the same age (40–48%) follow close behind, and family members are rare (3–5%). The other notable difference is uncertainty rather than a named actor: 32% of LATAM respondents said they were not sure who approaches young people, against 17% in South Africa.

Fig 9. Platforms on Which Respondents Believe This Usually Happens.

Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%. Bases: LATAM 119, South Africa 90, other regions 29. Three further options (gaming platforms, email, web forums or Com chatrooms) were each named by one or two respondents.

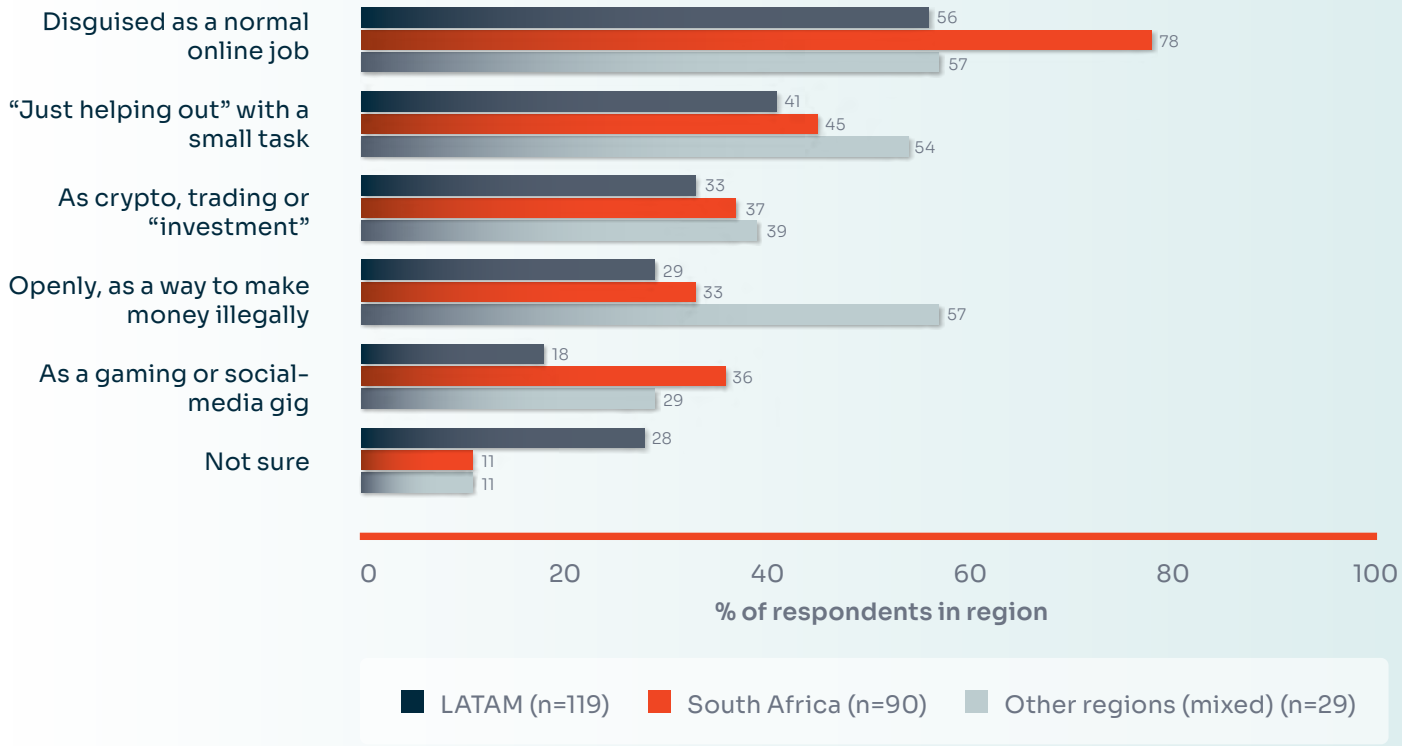


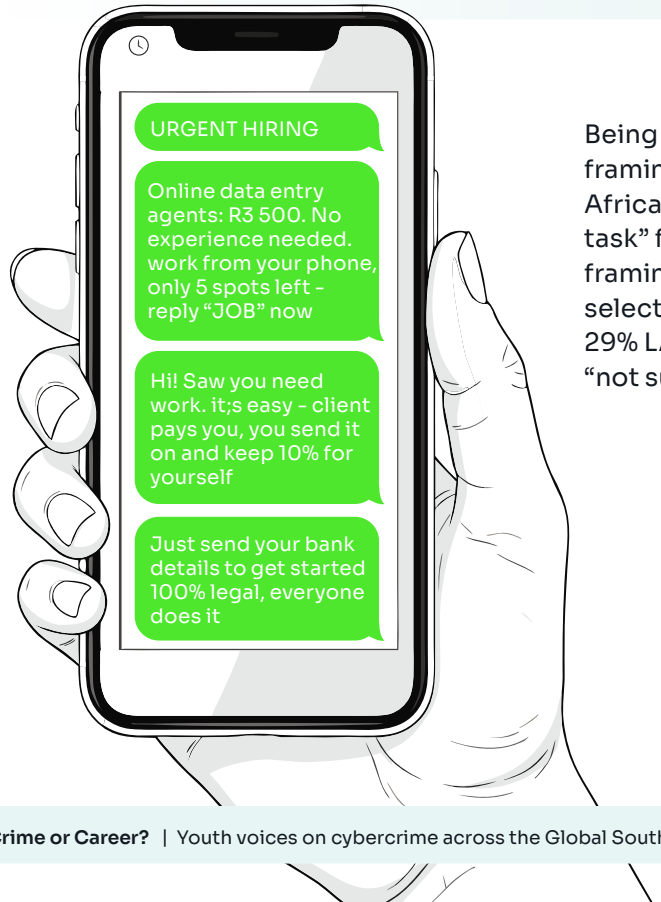
WhatsApp leads both focal regions almost identically (72% LATAM, 71% South Africa). Second place differs: Facebook including Marketplace in LATAM (62%), TikTok in South Africa (53%, with Facebook just behind at 52%). The regional differences sit in that second tier: Telegram (61% LATAM vs 31% South Africa) and Discord or gaming chats (41% vs 23%) against TikTok (53% South Africa vs 29% LATAM). In-person approaches are still named by a fifth to a quarter of respondents in both regions (21% and 26%). Every platform at the top of this chart is a mainstream, legal service.

2.6 How it is Framed

Fig 10. How Respondents Believe the Opportunity is Usually Presented to a Young Person

Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%.
Bases: LATAM 119, South Africa 90, other regions 29.





Being disguised as a normal online job is the most-selected framing in both focal regions, but markedly stronger in South Africa (78%) than in LATAM (56%). "Just helping out with a small task" follows (45% and 41%), then crypto, trading or investment framings (37% and 33%). Open presentation as illegal money is selected by under a third in both focal regions (33% South Africa, 29% LATAM), well below the job framing in each. Note the LATAM "not sure" rate of 28%, against 11% in South Africa.

Fig 11. The Escalation Ladder

How respondents in both regions described getting pulled in - step by step

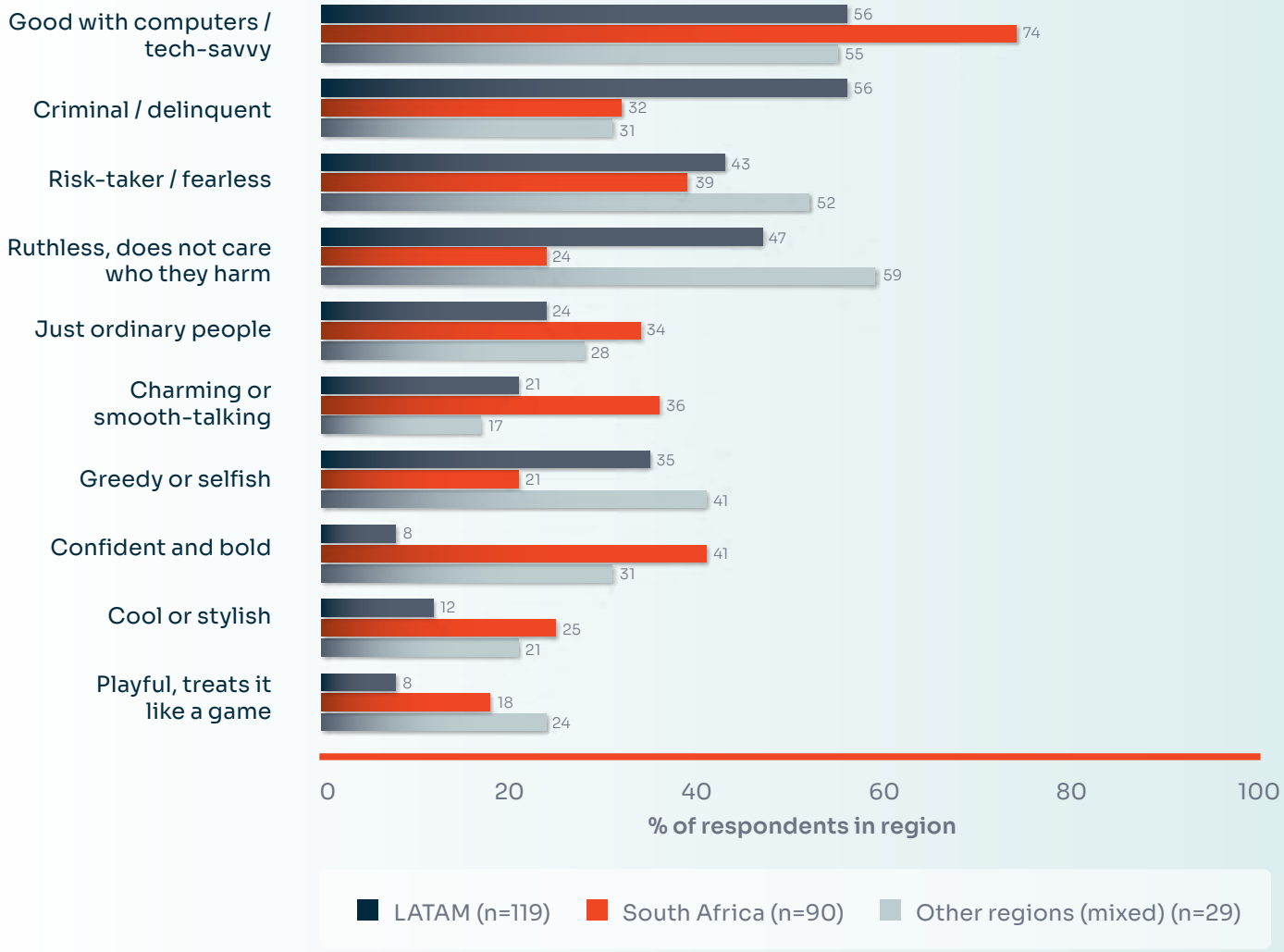
"They are offered small tasks with rewards, convinced these are legal things that won't harm them, and then the level of the rewards keeps going up."

- Survey Respondent, El Salvador

2.7 How Offenders Are Seen, and How Communities React

Fig 12. Words Respondents Say People Their Age Would Use to Describe Someone Who Commits Online Crime

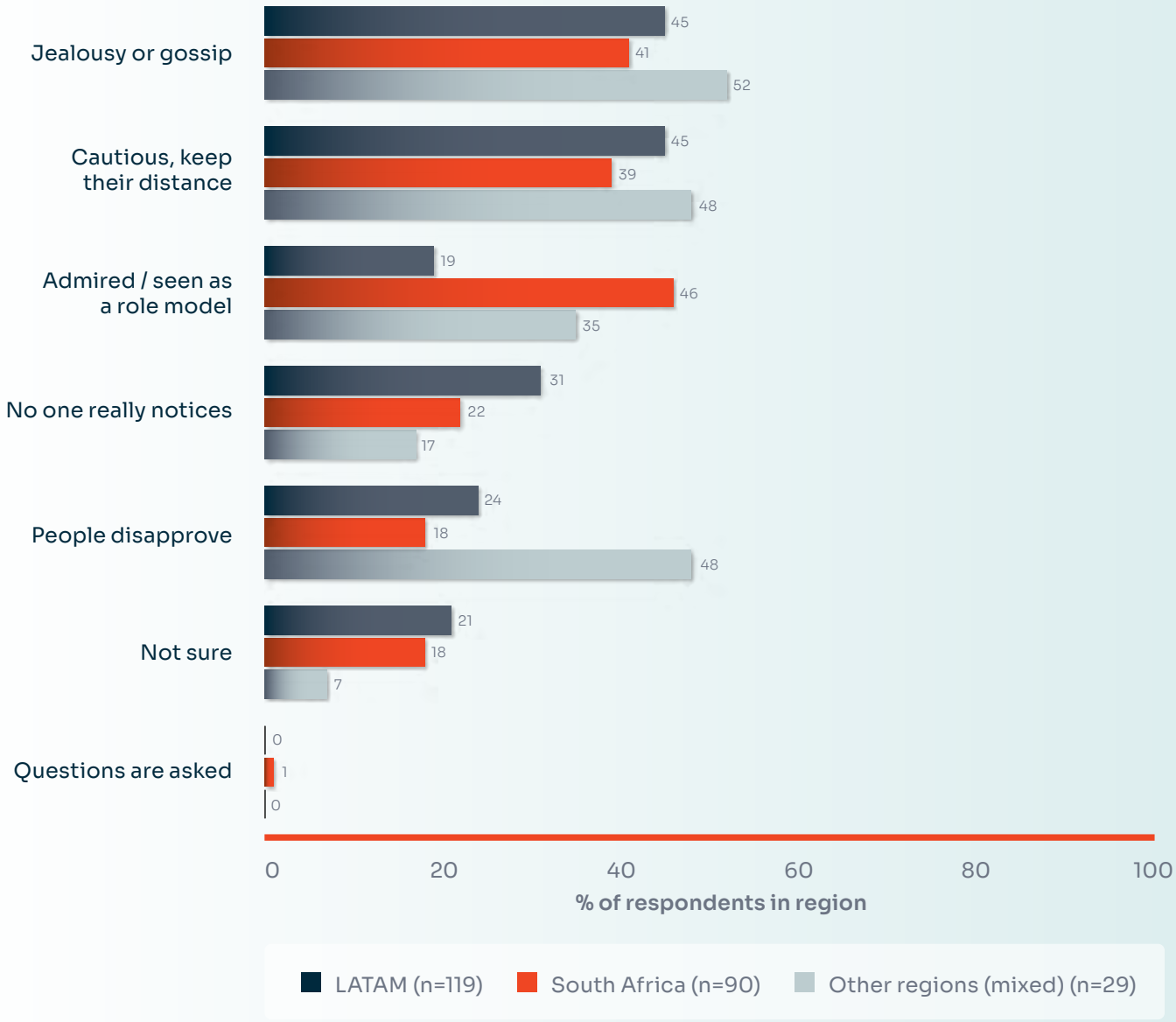
Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%.
Bases: LATAM 119, South Africa 90, other regions 29.



Technical competence is the common ground: “good with computers / tech-savvy” is the top or near-top description everywhere (74% South Africa, 56% LATAM). Beyond that the two regions diverge. LATAM respondents call cybercriminals “criminal / delinquent” 56%, “ruthless” 47%, “greedy” 35% where the South African figures are 32%, 24% and 21%. South African respondents more often choose traits that read as social capital: “confident and bold” 41% (LATAM 8%), “charming or smooth-talking” 36% (21%), “cool or stylish” 25% (12%).

Fig 13. How Respondents Believe Their Community Reacts When a Young Person Suddenly Makes Money Online In Unclear Ways.

Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%.
Bases: LATAM 119, South Africa 90, other regions 29.

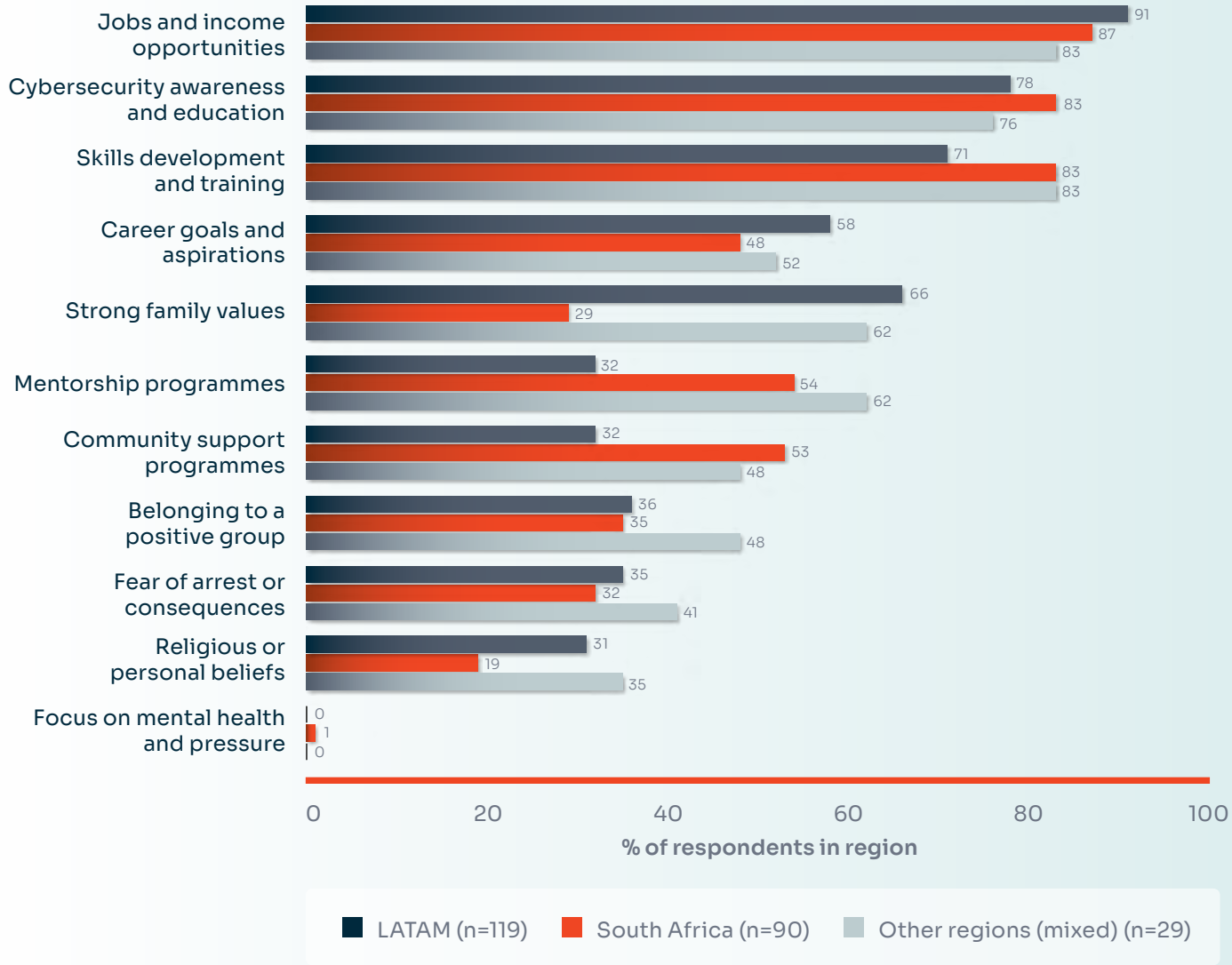


In LATAM the most common reactions are gossip (45%) and caution (45%). In South Africa the most-selected reaction is admiration: 46% said such a person is admired or seen as a role model, ahead of gossip (41%) and caution (39%), against 19% admiration in LATAM. Explicit disapproval is low in both (18% South Africa, 24% LATAM), and 21% of LATAM and 18% of South African respondents were unsure. Taken with Figure 12, the same pattern appears twice in the data from two differently worded questions.

2.8 What Young People Say Would Help

Fig 14. What Respondents Believe Would Help Young People Resist or Refuse Cybercrime.

Multi-select item: respondents could choose more than one option, so percentages do not sum to 100%. Bases: LATAM 119, South Africa 89, other regions 29. One South African respondent added “focus on mental health and pressure”.

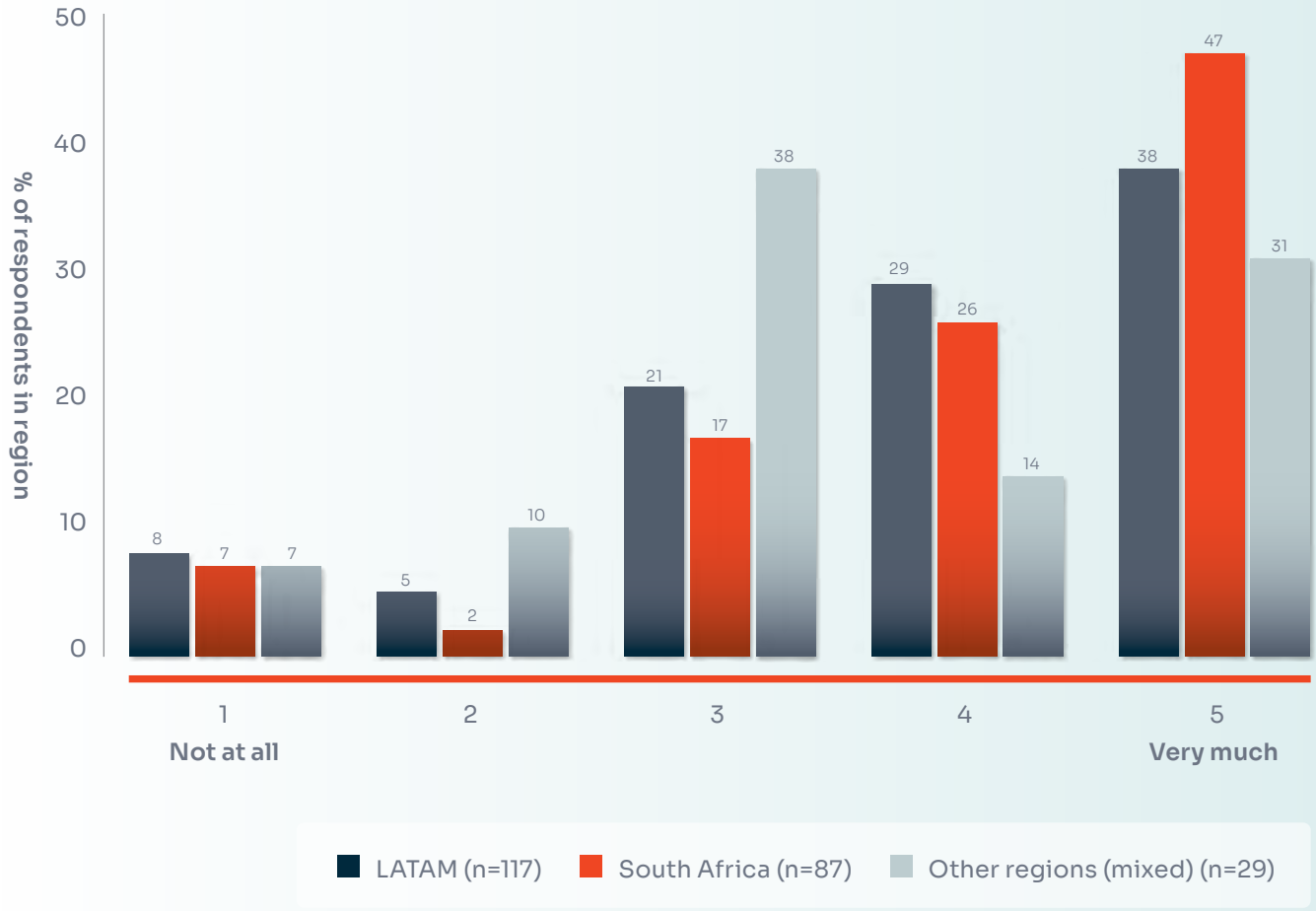


Jobs and income opportunities tops the list in both focal regions (91% LATAM, 87% South Africa) and ties with skills development and training in the other-regions group (83% each), with cyber awareness and education close behind everywhere (71–83%). The widest regional gap is strong family values (66% LATAM against 29% South Africa). The relational factors run the other way: mentorship (54% South Africa vs 32% LATAM) and community support programmes (53% vs 32%). Fear of arrest or consequences is chosen by roughly a third in both focal regions (35% LATAM, 32% South Africa), below jobs, skills and cyber education in every group.

2.9 How Worried Respondents Are

Fig 15. Personal Concern About The Respondent or a Family Member Becoming a Victim of Cybercrime in the Next 24 Months (1 = not at all, 5 = very much).

Bases: LATAM 117, South Africa 87, other regions 29.



Concern is high in both focal regions and highest in South Africa (mean 4.05, against 3.84 in LATAM and 3.52 in the mixed group). In both focal regions the single most common answer is the top of the scale — 47% of South African and 38% of LATAM respondents chose 5 of 5. The distributions are not symmetrical: a small group at the other end answered 1 (six in South Africa, nine in LATAM), so the means understate the spread. The mixed group clusters at the midpoint.

3. Discussion and Conclusion

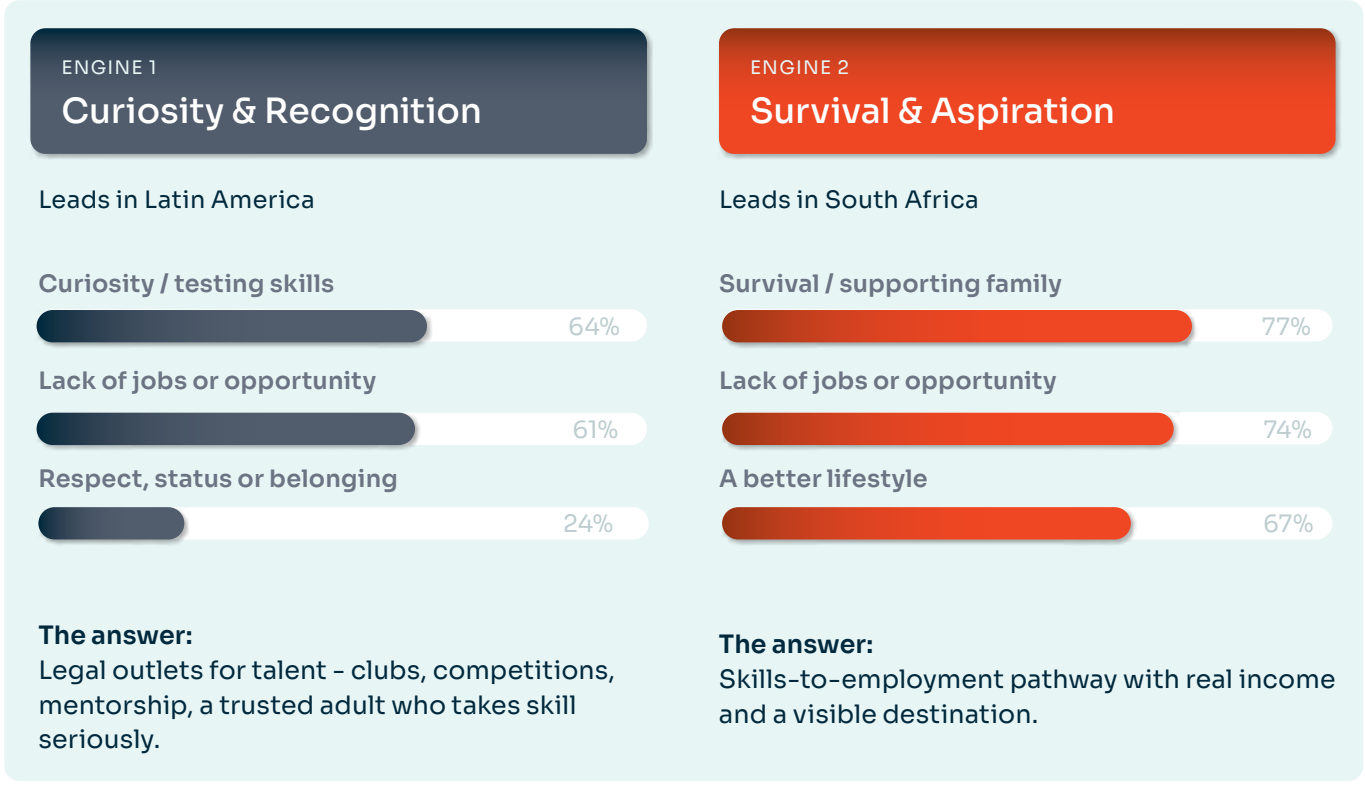
3.1 Two Engines, Not One

The Northern research on youth cybercrime has converged on a recognisable pathway: early curiosity about computers, gaming and cheat markets as the on-ramp, and a need for recognition that the offending community meets (Leukfeldt & Bekkers, 2026; Loggen et al., 2024). Our data does not contradict that account, curiosity is the single most-selected driver in Latin America, at 64%, but it does show that curiosity is not the whole engine, and in South Africa it is not even the main one.

In South Africa, survival and supporting family (77%) and lack of jobs (74%) sit above every other driver, and 18% of respondents describe themselves as unemployed and out of study. That is the pattern Dr Lazarus documents in West Africa, where the "Hustle Kingdoms" operate as schools precisely because they supply what the formal economy does not: income, structure, status and a career path (Lazarus & Soares, 2024; Lazarus et al., 2025). Where the pathway is economic, the intervention has to be economic too. A curiosity-shaped programme (redirect the talent, offer a legal outlet for the skill) will help the LATAM respondent who was testing what they could get away with, but may not touch the South African respondent who is trying to pay rent.

The practical reading is that the two engines require different tools, and that both are present in both regions in different proportions. Prevention designed for one and exported to the other may under-perform.

Fig 16. Different Drivers: Curiosity vs Survival



3.2 Where Crime Is Admired, Fear Does Not Compete

The sharpest finding in the dataset is not about money; it is about status. Asked how their community reacts when a young person suddenly makes unexplained money online, 46% of South African respondents said that person is admired or treated as a role model, against 19% in Latin America. Asked what words their peers would use, South African respondents chose “confident and bold” five times more often than LATAM respondents (41% vs 8%), while LATAM respondents were nearly twice as likely to say “criminal” (56% vs 32%). Two differently worded questions, the same split.

This matters because it sets a ceiling on what deterrence messaging can achieve. Fear works against a behaviour a young person already regards as shameful. Where the behaviour confers standing, a warning is not a cost, it is attention, and attention is the currency. The InterCOP evidence made this concrete from two directions. Dutch researchers who pushed a warning into an offender group found the group treated it as a badge. And a former offender, sharing a stage with a former FBI profiler, said plainly that no warning would have moved him; what might have helped instead was a trusted adult who took his talent seriously. Our own respondents put fear of arrest at around a third in both focal regions, well below jobs, skills and education everywhere. You cannot warn a young person out of a recognition deficit, and you cannot deter your way past aspiration. The legitimate path has to offer the status instead.

46% of South African respondents say a young person making unexplained money online is admired or seen as a role model

vs

19% in Latin America. Where crime is admired, fear doesn’t compete.

3.3 It Does Not Look Like a Crime; it Looks Like a Job

Nearly four in five South African respondents say involvement is presented as a normal online job, and fake online job offers are the most-seen crime type in both South Africa (82%) and the other-regions group (83%). They are not asked to commit a crime. They are offered work; data entry, an “agent” role, marketing, “just helping out with a small task”.

Two consequences follow. First, the point of contact is a labour-market moment, not a criminal one, so the intervention belongs where young people look for work: job boards, campus notice boards, WhatsApp job groups, learnership programmes. Second, awareness content built around the word “crime” will miss the moment entirely. The useful message is not “do not commit cybercrime”; it is “here is what a fake job offer looks like, and here is what happens to the person who takes it”. This is also where the young person moving funds through their own account is the one exposed to prosecution, a criminal record and long-term banking consequences, while the network’s core members stay hidden, and Bekkers et al. (2023) found young people systematically underestimate exactly those consequences.

Respondents in both focal regions, answering an open question independently, described the same graduated ladder: a first small task, paid; reassurance that it is legal and harms nobody; then tasks and rewards that escalate. One respondent in El Salvador described being “offered small tasks with rewards, convinced these are legal things that won’t harm them, and then the level of the rewards keeps going up”; two South African respondents described the same escalation in almost the same terms.

78%

of South African respondents say cybercrime involvement is presented as a normal online job

Openly framed as illegal money: under a third. Almost nobody is asked to commit a crime.

3.4 Recruitment Runs on the Platforms Young People Already Use

Nothing at the top of Figure 9 is a hidden channel. WhatsApp leads both regions at around 72%, with Facebook, Telegram and Discord strong in Latin America, and TikTok second only to WhatsApp in South Africa. A fifth to a quarter of respondents in both regions still name in-person approaches, which is a useful corrective to a purely online model of recruitment.

That distribution puts prevention squarely in the product-governance layer. If the first contact happens on a mainstream service, then platform design - how job offers are surfaced, how quickly a recruitment account can reach a minor, what a reported account costs its owner - is prevention infrastructure, and platforms and AI providers need to be part of this. The regional differences also mean a single platform strategy will not travel: a Telegram-and-Discord campaign built for Latin America maps poorly onto a South African cohort that is on TikTok.

3.5 What Young People Are Asking for

The protective-factor item is the most actionable in the survey, and its ranking is remarkably stable across three very different groups: jobs and income first (83–91%), then skills training and cyber education (71–83%). The widest regional gap is strong family values (66% LATAM against 29% South Africa); the relational factors run the other way, with mentorship and community support chosen by over half of South African respondents and by under a third in Latin America.

Europol's description of the underground economy as a reputation market, such as badges, seller tiers, trust ledgers and the Italian investigators who profiled a group of minors and found nothing pathological, only belonging, a parent's attention and peer mirroring, describe a pipeline that competes on recognition. Our respondents are asking for the legitimate version of exactly that, and their free-text answers say it more plainly than any framework.

A respondent in Panama: "the trick is for job offers to be more competitive than crime."

One in the Western Cape: "give us digital literacy, because if you don't, desperation will keep teaching us to scam faster than your laws can catch up." And one in Gauteng, on what world leaders should do: invest in education and opportunity rather than punishment, so that young people become "defenders of technology rather than offenders."

91%

of Latin American respondents say jobs and income opportunities would most help young people refuse cybercrime

The top answer in every region.
Fear of arrest: chosen by around a third.

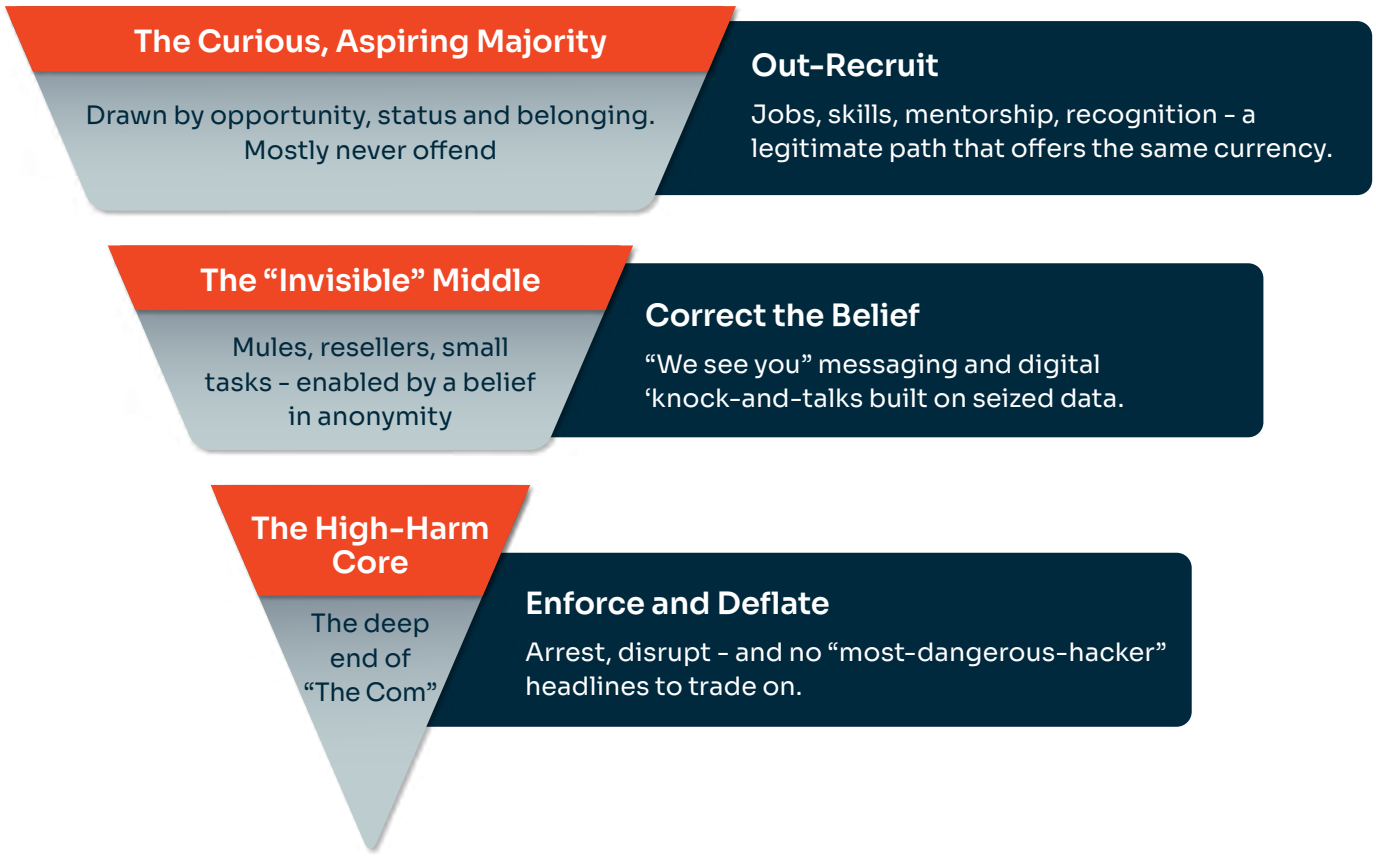
3.6 The Honest Limit

Belonging and opportunity explain, and can interrupt, the top of the funnel. They do not reach the deep end. The persistent, high-harm end of "the Com", online subcultures Unit 221B and the FBI describe, built on notoriety, serial offending and an absence of remorse is a different population, and a prevention argument that claims to cover the whole funnel will be wrong. For that group the levers are narrow: arrest, disruption, and denying them the reputation they trade on.

Every "most dangerous hacker" headline is free advertising that raises both their credibility and what victims will pay, and it makes them more admirable to the young people at the top of the funnel.

Between the two ends sits a large middle: lower-level participants who believe they are invisible. Europol's use of seized forum data to contact exposed users directly, such as a digital "knock-and-talk" is a great model for that tier, because it attacks the perceived anonymity the whole underground economy depends on. So prevention out-recruits at the top, targeted messaging corrects belief in the middle, and enforcement works at the bottom. The three have to work together.

Fig 17. Cybercrime Recruitment Funnel



4. Recommendations

The strategic conclusion is that prevention has to compete with the criminal pipeline on the pipeline's own terms. It has to out-recruit, not only out-threaten. Four things follow directly from the data.

1. Intervene at the Job-Offer Moment, Not the Crime Moment

Because involvement is presented as work (78% South Africa, 56% LATAM) and fake job offers are the most-seen crime type, awareness content should teach young people to read a job offer, and belongs where they look for work: WhatsApp job groups, campus boards, learnership and internship channels. Not in generic cybercrime messaging.

2. Lead With Opportunity, Not Deterrence

Jobs and income was the top protective factor in both focal regions and joint-top in the mixed group (83–91%); fear of arrest was chosen by around a third. Prevention budgets should follow that ranking: skills-to-employment pathways with a visible destination, tied to the cyber and technology sectors that are recruiting.

3. Compete On Status And Belonging Where Crime is Admired

In South Africa, 46% say offenders are admired, and mentorship and community support are sought by over half of respondents. Fund the programmes that supply recognition legitimately, example models already exists in Brazil's Hackers do Bem, CYSED in Nigeria, The Hacking Games, and the CyberHelpline and MiDO Academy pilot in South Africa. Resource them as prevention infrastructure rather than outreach.

4. Bring Platforms in as Partners, Region by Region.

Recruitment runs on WhatsApp, Facebook, Instagram, Telegram, Discord and TikTok, in different mixes by region. Platform and AI providers sit in the prevention path, and campaign design has to match the local platform mix rather than assume one.

5. Limitations

- This is a convenience, self-selected sample recruited through the Global CAN partner networks, largely young people already exposed to cybersecurity training. It is not representative of youth in either region, and no statistical inference is made from it.
- Group sizes are uneven and modest: LATAM 119, South Africa 90, other regions 29. The other-regions group mixes Global North and Global South respondents and is reported for context only.
- Two thirds of respondents are male (161 of 238). South Africa is evenly split; LATAM and the other-regions group are 79% male. Recruitment patterns specific to young women are likely under-observed.
- Responses are perceptions and self-report, not verified incidence. They describe what young people believe about their environment — the right input for prevention design, the wrong input for threat measurement.
- The two survey instruments differed slightly in wording between English and Spanish; responses were harmonised into common categories and checked against the Spanish source. Full methodological notes are available on request.

6. Acknowledgements

Thank you to our interns Relebohile Senatsi, Lebohang Selela and Lwando Ntontela, who are all graduates of the MiDO Cyber Academy, an initiative that provides pathways out of poverty through cybersecurity education for underserved youth in South Africa. There is meaning in their contribution, both in shaping and disseminating the survey and in helping to write this report.

Thank you also to Adriana Gomez from IRSI for sharing the survey with her LATAM student network, Nicole Cader from the Absa Academy, and Emily Peel from The Hacking Games.

A special mention of The International Cyber Offender Prevention Network (InterCOP) which is made up of international law enforcement agencies that share expertise and jointly develop, implement and evaluate Cyber Offender Prevention (COP) interventions and prevention campaigns.

7. Methodology

Survey design

The questionnaire contained 18 questions: single-select demographic and screening questions, eight multi-select ("select all that apply") items on crime types, drivers, recruiters, platforms, framing, perceptions, community reaction and protective factors, two free-text items, and one 1–5 concern scale. Two regional versions were fielded, in English and in Spanish. The versions are substantively parallel but not identical: some response options are worded slightly differently in translation, and the two versions were reconciled item by item against the original Spanish export. Latin American responses in the consolidated data are English translations of the Spanish originals.

Sample and recruitment

Respondents were recruited through the Global South CAN partner networks — mainly the Information Security and Risk Institute (IRSI) in Latin America, and the MiDO Cyber Academy and Absa Cyber Academy in South Africa. The sample is a convenience sample of young people who are in part already exposed to cybersecurity training, not a population sample.

The third group is drawn from The Hacking Games global community. It comprises Africa outside South Africa (9), Europe and the UK (7), Asia (7) and the USA (6) — roughly half of it Global North. Throughout this report it is called "Other regions (mixed)" and is shown in every figure as a de-emphasised third series, for context only. With n = 29 it supports no comparative claim, and none is made.

Table 1. Sample composition

Characteristic	LATAM	South Africa	Other regions (mixed)	Total
Respondents (n)	119	90	29	238
Age 18–24	66 (56%)	40 (44%)	20 (69%)	126
Age 25–34	46 (39%)	43 (48%)	8 (28%)	97
Age 35+	7 (6%)	7 (8%)	1 (3%)	15
Female	24 (20%)	44 (49%)	5 (17%)	73
Male	94 (79%)	44 (49%)	23 (79%)	161
Prefer not to say	1 (1%)	2 (2%)	1 (3%)	4

Source: Global South CAN survey master data, June 2026 (N = 238). Column totals reconcile to the group sizes; percentages are of the group.

Data collection, consent and anonymity

Data were collected in June 2026 through an online survey platform (Google Forms). The first item screened for age, restricting participation to respondents aged 18 and over. Participation was voluntary and no question required an answer, which is why item-level bases vary (reported on every figure). Respondents could enter a prize draw for a R500 or €50 gift voucher; prize-draw entries were collected on a separate, unlinked form so that contact details could not be traced to responses.

Analysis approach

Analysis is descriptive. For multi-select items, results are reported as the percentage of respondents in a region who answered that item and selected a given option; because respondents could choose several options, columns sum to more than 100%. Each figure states the base for each group. Wording differences between the English and Spanish instruments were harmonised into common categories and checked against the Spanish source. No inferential tests are reported, as a self-selected sample does not support them.

References

Bekkers, L., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Money mules and cybercrime involvement mechanisms: Exploring the experiences and perceptions of young people in the Netherlands. Deviant Behavior, 44(9), 1368–1385. https://doi.org/10.1080/01639625.2023.2196365

Federal Bureau of Investigation, Internet Crime Complaint Center. (2025, July 23). The Com: Theft, extortion, and violence are a rising threat to youth online (Alert No. I-072325-3-PSA). https://www.ic3.gov/PSA/2025/PSA250723-3

Lazarus, S., & Soares, A. B. (2024). From business centres to hustle kingdoms: Historical perspectives on innovative models of deviant education. International Annals of Criminology, 62(3–4), 449–468. https://www.cambridge.org/core/journals/international-annals-of-criminology/article/from-business-centres-to-hustle-kingdoms-historical-perspectives-on-innovative-models-of-deviant-education/B103B4F174764BCA6F5949A24ADD8FBA

Lazarus, S., Soares, A. B., & Button, M. (2025). Pathways, pressure, and profit: Adaptive innovation and strain in a convicted cybercrime academy called Hustle Kingdom. Deviant Behavior. Advance online publication. https://www.tandfonline.com/doi/full/10.1080/01639625.2025.2551790

Leukfeldt, E. R., & Bekkers, L. M. J. (2026). From curiosity to crime: Exploring pathways into criminal hacking. Computers in Human Behavior, 181, Article 108996. https://doi.org/10.1016/j.chb.2026.108996

Loggen, J., Moneva, A., & Leukfeldt, E. R. (2024). Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. Victims & Offenders. Advance online publication. https://doi.org/10.1080/15564886.2024.2370295

National Bureau of Investigation. (2026). Young people online: An educator's guide to cybercrime prevention and responsible online behaviour. Police of Finland.

Poliisi. (2026, March 24). Cybercrime is increasingly a part of young people's everyday lives — The Finnish police publishes a guide to support discussing cyber topics [News release]. https://poliisi.fi/en/-/cybercrime-is-increasingly-a-part-of-young-people-s-everyday-lives-the-finnish-police-publishes-a-guide-to-support-discussing-cyber-topics

Conference material referenced in section 3 is described from the research lead's own notes taken at InterCOP, INTERPOL headquarters, Lyon, 15–16 July 2026. Sessions presented under confidentiality or law-enforcement handling are deliberately omitted, and no speaker is cited as a published source. Where a conference point also exists in the peer-reviewed literature, the publication is cited instead.

About KnowBe4

KnowBe4 empowers the modern workforce to make smarter security decisions every day. Trusted by more than 70,000 organizations worldwide, KnowBe4 is the pioneer of digital workforce security, securing both AI agents and humans. The KnowBe4 Platform provides attack simulation and training, collaboration security, and agent security powered by AIDA (Artificial Intelligence Defense Agents) and a proprietary Risk Score. The platform leverages 15-years of behavioral data to combat advanced threats including social engineering, prompt injection, and shadow AI. By securing humans and agents, KnowBe4 leads the industry in workforce trust and defense.

More information at www.KnowBe4.com.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2026 KnowBe4 All Rights Reserved.