

Beyond the Human Firewall

The Psychology of Scams and
Community Defence Strategies

White Paper



Copyright © 2026 European Neighbourhood Watch Association

This publication is available as a PDF on the European Neighbourhood Watch Association website under a Creative Commons license that allows copying and distributing the publication, only in its entirety, as long as it is attributed to the European Neighbourhood Watch Association and used for noncommercial educational or public policy purposes.

Published by:

European Neighbourhood Watch Association – EUNWA

Via Terraglio 64

30174 Venice, Italy

www.eunwa.eu

For more information contact:

head-office@eunwa.eu

Date of publication: March 2026

Note on images: All photographs and images used in this document are distributed under Creative Commons (CC) licences, are in the public domain, or are reproduced with the express permission of the copyright holders. Specific author attribution is provided in the captions or in the photo credits list.

Beyond the Human Firewall

The Psychology of Scams and
Community Defence Strategies

This page intentionally left blank.

Table of Contents

Abstract	7
Acknowledgements	8
Preface	9
Introduction	10
Methodological note and scope	12
Chapter 1 - The human constant in technological evolution	13
Chapter 2 - The mind of the manipulator and the ecology of defence	16
Chapter 3 - The psychology of the target - why vulnerability is widely distributed	21
Chapter 4 - From theory to practice	26
Chapter 5 - Strategic considerations for National Boards	34
References	37
ANNEX A: Advanced Psych - Ops Classification	38
ANNEX B: Action Card	39
ANNEX C: Cognitive Defence Glossary	40
ANNEX D: Your "Security Companion" (The Designated Sceptic)	42
ANNEX E: Illustrative scenarios for stress inoculation	43
ANNEX F: The family safe word	44

Tables

Table 1. Analytical Mapping of Fraud Syntax and Cognitive Vulnerabilities	30
Table 2. Mapping Threats to Cognitive Vulnerabilities	38

Figures

Figure 2. The Confidence Loop. A recurring psychological process through which scams develop and persist: from the identification of emotional vulnerability, to meaning construction and emotional investment, followed by escalating commitment

and reinforced silence. The loop explains why scams rarely stop spontaneously and why external interruption is required to prevent repetition. 17

Figure 3. The Lake Wobegon Curve. The Lake Wobegon Effect describes the systematic tendency of individuals to believe they are more intelligent, competent, or discerning than the average. In the context of fraud, this illusion of superiority reduces vigilance and increases susceptibility, as confidence in one's own judgement discourages verification, external consultation, and critical doubt. 22

Figure 4. The Cognitive Switch. Under conditions of urgency, fear, or authority pressure, decision-making shifts from deliberative reasoning (System 2) to automatic emotional response (System 1). The "Cognitive Switch" is activated not by individual willpower, but by external interruption, such as time delay, verification, or consultation with a trusted third party, restoring access to rational judgement. 27

Abstract

Despite sustained investment in awareness campaigns, patrimonial losses related to fraud reported across Europe continue to rise. The rise in fraud despite awareness campaigns reveals a structural flaw: information alone cannot protect someone when their judgement is being systematically undermined.

Modern fraud is a form of psychological manipulation that exploits urgency and isolation to temporarily disable a person's ability to think clearly.

This White Paper proposes a strategic shift from awareness-based prevention to **cognitive defence**. Rather than cataloguing scam narratives, it examines the underlying psychological structures that make deception effective and resilient to change. By focusing on the syntax of fraud rather than its content, the paper reframes prevention as a question of managing cognitive vulnerability under stress.

Central to this approach is the concept of the **Cognitive Switch**: the moment at which external stimuli (social, environmental, or procedural) interrupt automatic emotional responses and restore deliberative control. From this perspective, effective prevention cannot rely solely on individual self-regulation but must be supported by community-based mechanisms capable of providing external verification and cognitive grounding.

Drawing on research in psychology, criminology, and behavioural science (Kahneman, 2011; Thaler & Sunstein, 2008), the paper outlines a set of **non-binding strategic levers** that National Neighbourhood Watch Associations may consider. These include mechanism-based recognition frameworks, social circuit breakers such as the Designated Sceptic, environmental nudging, and stress inoculation through controlled exposure. These options are presented as adaptable frameworks rather than prescriptive models, fully respecting national autonomy and contextual diversity.

By framing Neighbourhood Watch networks as potential guardians of what this paper terms “cognitive space”, this White Paper contributes to the European debate on community-based security. It offers National Boards a shared analytical framework to support strategic deliberation, policy design, and cross-border dialogue on fraud prevention in an increasingly complex threat environment.

Acknowledgements

The publication of this White Paper marks a fundamental step for our European network. Its analytical and strategic robustness would not have been possible without the invaluable and careful review by **Mauro Bardi** (Lawyer and Victim Support Specialist) and **Andrea Poltronieri** (Psychologist and Victim Support Specialist).

Their profound legal and psychological expertise has allowed us to rigorously validate the theoretical framework of the document. Thanks to their contribution, we can deliver these guidelines to the National Boards with the utmost confidence, offering concrete, secure, and tested tools to strengthen the defence architecture of our communities. We extend our deepest gratitude to them.

Mauro Bardi (PhD) - Member of the Milan Bar specialising in legal and communication psychology, the sociology of deviance, and victimology. He works closely with the General Crime Victim Support Centre at Rete Dafne Mantova and across the wider Rete Dafne Italia network. He has authored numerous studies on public law, criminology, urban security, and victimology. Contact: info@maurobardi.com

Andrea Poltronieri - Clinical psychologist and psychotherapist, and faculty member at the "AETOS" School of Specialisation in Psychotherapy. He is a psychologist at Libra ETS, working within the General Crime Victim Support Centre at Rete Dafne Mantova, and manages regional and European projects focused on victim support. He has previously worked as a clinical psychologist within local health and social services in the Mantua area, partnering with public bodies and judicial authorities on psycho-forensic interventions.

Preface

It is not just about numbers

Behind every statistic cited in official reports, there is a human story that often remains unheard. There is the silence of an elderly person who stops leaving their home out of shame. There is the quiet devastation of life savings, built over decades for children or grandchildren, vanishing in the space of a single phone call. And perhaps most painfully, there is the lingering feeling of having been “stupid” for trusting something that, in the moment, felt entirely real.

Fraud does not end when the money is gone. In many cases, its most enduring damage is psychological. It fractures trust, not only in others, but in oneself. It isolates victims, pushing them into silence precisely when connection and support would be most protective. Shame often becomes one of the scammer’s most effective allies.

At EUNWA, we believe that security cannot be reduced to cameras, locks, or digital safeguards alone. Security is also made of **human relationships**, of proximity, and of shared responsibility. The crime of fraud possesses a highly peculiar nature: unlike predatory crimes that use physical force to violate our spaces, fraud bypasses physical defences by infiltrating our lives through deception. It relies on a markedly interactive dynamic that paradoxically requires our own cooperation. Criminals do not force a door; they manipulate the mind, surgically exploiting our human frailties—such as loneliness, the need to be heard, the sense of urgency, and our natural propensity to trust. Through these levers, they manage to make narratives that we would otherwise consider entirely implausible appear credible and unassailable.

This White Paper was written in response to that reality. It is not born from abstraction, but from the accumulated experience of communities across Europe; communities that have witnessed how deception erodes dignity long before it appears in crime statistics. Our intent is not to blame individuals for falling victim, but to recognise fraud for what it is: a professional, deliberate manipulation of human psychology.

We offer this document as an act of collective responsibility. Its purpose is to contribute to a culture in which victims are no longer left alone with their shame, and in which communities are empowered to protect not only material assets, but also personal dignity. Because resilience is not only a matter of prevention; it is also a matter of how societies respond when prevention fails.

No one should have to face deception, loss, and silence alone.

The EUNWA Team – March 2026

Introduction

From awareness to cognitive defence: a strategic challenge for European communities

Let us begin with a difficult but necessary question: **why do intelligent, educated, and cautious individuals still fall victim to scams?** For decades, crime prevention strategies across Europe have relied on a seemingly intuitive assumption: if citizens are informed, they will be safe.

Millions of leaflets have been distributed, warning about fake police officers, romance scams, investment frauds, or fraudulent phone calls. Yet, despite this sustained effort, reported losses across Europe continue to increase year after year. This pattern suggests a structural limitation in awareness-led prevention models: **they often treat the narrative of the scam as the problem, rather than the psychological mechanism that makes the narrative effective.**

We are currently living through a technological paradox. While devices, platforms, and financial systems are increasingly protected by sophisticated digital firewalls, the human mind remains guarded by the same cognitive architecture it has relied upon for tens of thousands of years. Modern offenders, empowered by Artificial Intelligence and Open-Source Intelligence (OSINT), have not fundamentally changed the nature of fraud; they have scaled and industrialised many of its mechanisms. They often exploit not ignorance alone, **but common human dispositions such as trust, fear, urgency, hope, and the need for connection** (Cialdini, 2001). In this context, fraud should not be understood solely as a failure of individual vigilance, but as a form of psychological engineering.

Techniques such as pretexting, sensory overload, and authority manipulation are specifically designed to overload emotional processing systems and temporarily impair rational judgement. Under these conditions, even well-informed individuals may become cognitively compromised. Knowledge alone, therefore, may be insufficient as a defence under conditions of emotional pressure.

This White Paper proposes a strategic shift: **from awareness-based prevention to cognitively informed defence.** Instead of focusing exclusively on scam typologies and evolving narratives, it examines the underlying psychological mechanisms that make deception effective and predictable. By understanding how the human mind may fail under emotional pressure—a dynamic widely popularised as the Amygdala Hijack (Goleman, 1995)—we can begin to design defensive strategies that do not rely solely on individual willpower at the moment of crisis. As firsthand accounts from victims testify, manipulative pressure often employs a verbal flow so rapid and relentless that it induces a genuine state of "trance" or mental subjugation. For this reason, breaking

the deception primarily means training oneself to actively interrupt the caller, preventing this induced hypnosis from taking hold.

Central to this approach is the recognition that fraud constitutes a profoundly asymmetric threat, a divide that has recently been further and dramatically exacerbated by two determining factors: the ever-increasing effectiveness of technological tools in creating false appearances, and the growing vulnerability of potential victims. On one side stands the professional scammer, equipped with scripted psychological techniques, technological anonymity, and unlimited patience. On the other stands the individual citizen, often isolated and emotionally engaged, who may be poorly equipped to resist manipulative pressure alone under conditions of emotional arousal and cognitive overload. This asymmetry is reversed only when the individual is embedded within a social structure capable of providing external verification and emotional grounding.

It is precisely here that **Neighbourhood Watch networks represent a unique strategic asset**. Operating at the “last mile” of security, where digital deception translates into real-world harm, these community-based structures possess forms of proximity, trust, and informal authority that formal systems and digital safeguards may struggle to replicate in the same way. Properly understood, Neighbourhood Watch is not merely a tool for observing physical space, but a potential community-level guardian of what this paper terms “cognitive space”.

By reframing fraud prevention as a question of collective cognitive resilience rather than individual attentiveness, this White Paper invites National Associations to reconsider how social cohesion, non-judgemental verification, and community proximity can be mobilised as defensive resources. Ultimately, the “Human Firewall” described in these pages is not built of software or surveillance, but of structured trust, shared responsibility, and the simple yet powerful act of asking: “*Does this make sense?*”

Methodological note and scope

This White Paper adopts an interdisciplinary analytical framework drawing on psychology, criminology, behavioural science, and legal history. Its primary objective is not experimental validation, but strategic sense-making: identifying recurrent psychological mechanisms underlying fraud and exploring how community-based structures may mitigate predictable cognitive vulnerabilities under stress.

Operational diversity and application

This White Paper is designed with the understanding that National Associations of Neighbourhood Watch operate within diverse cultural, political, and legal landscapes. Consequently, the strategic options, frameworks, and illustrative examples outlined herein are conceived purely as a non-binding, modular toolkit. They are intended to complement, rather than replace, institutional responses by law enforcement, financial institutions, and regulatory bodies, offering adaptable resources that can be tailored to specific local needs, structural capacities, and strategic priorities.

Conceptual terminology

The document intentionally employs conceptual models and analytical metaphors (e.g., “Cognitive Switch”, “Denial-of-Service analogy”, “Amygdala Hijack”) to facilitate cross-sector understanding among policymakers, community leaders, and non-specialist stakeholders. These constructs are used as functional shorthand to describe states of acute emotional activation and are not presented as clinical diagnoses or neuroscientific absolutes.

Limitations of the current framework and areas for future research

While these strategic levers are grounded in established literature, they require practical testing. Future pilot studies led by national associations will be vital to measure how effectively they work in real-world environments. In addition, frameworks such as the Designated Sceptic fundamentally assume that potential victims have access to a trusted third party. Addressing this “social capital paradox”, where the proposed defence requires social resources the most isolated targets often lack, remains a critical priority for future proactive community outreach initiatives.

The strength of distributed defence

While the effectiveness of a ‘human firewall’ suggests a systematic approach, its strength lies in its adaptability rather than its uniformity. By providing a modular toolkit, the network enables a distributed defence where each association strengthens the collective resilience by tailoring these universal psychological principles to its own cultural, political, and legal reality.

Chapter 1 - The human constant in technological evolution

A common analytical tendency is to frame modern scams as purely technological problems. When we hear terms like phishing, deepfakes, or crypto fraud, our minds instinctively turn to complex algorithms and cybersecurity. However, this is a distraction. In a criminal landscape identified by Europol's latest threat assessment as increasingly professionalised (Europol, 2024), the reality is that the hardware changes, but the software, human nature, remains constant.

As highlighted by security experts and "*Fraudologia*" authors Rampin & Caris (2011), within the information security cycle, the "Human Factor" remains the critical element. Technology is merely the "delivery vector". The payload, the mechanism making the scam effective, is not digital, but psychological. Whether it is a charlatan in the Middle Ages or an AI cloning a voice in 2026, the lever is identical: manipulating fundamental human emotions to bypass rational thought.

1.1 It's not magic, it's OSINT (Open-Source Intelligence)

One of the most frequent questions from victims is: "How did the scammer know my son lives in London or that I bank there?". The answer isn't magic; it's research. Christopher Hadnagy (2018), in his seminal text *Social Engineering*, explains that most sophisticated attacks are preceded by a data collection phase called OSINT (Open-Source Intelligence).

Criminals do not strike blindly. They analyse social media profiles, public records, and even physical refuse to build detailed victim profiles. This data is then weaponised to create the Pretexting scenarios we will explore in Chapter 2. Understanding this is the first step to defence: protecting your data means reducing the informational advantage available to the offender.

1.2 The anatomy of a crime – A historical and legal perspective

To fully grasp the gravity of modern scams, we must look beyond the screen and examine the legal history of deception. Fraud is unique among crimes because it requires the cooperation of the victim. Unlike robbery, which uses violence or threat to bypass the will, fraud uses intellect to hijack the will.

The Roman legacy and the evolution of intent

In Roman Law, the foundation of Continental European legal systems, fraud was initially difficult to define and codify. Jurists drew an initial distinction between *dolus bonus* (tolerated commercial boasting) and *dolus malus*, masterfully defined by the jurist Labeo as "*omnis calliditas, fallacia, machinatio ad circumveniendum, fallendum, decipiendo alterum adhibita*" (any craft, deceit, or machination employed to circumvent or deceive another).

Today, the distinction between *dolus bonus* and *malus* has faded: even mere boasting, if organised and structured, can constitute the offence of fraud. The legal debate has instead shifted to the difference between "unrecognisable" (sophisticated) and "recognisable" (clumsy) scams. One might be led to believe that only the most complex machinations constitute a true crime, but this perspective is misleading as it ignores the interactionist dimension of the crime.

Modern law rejects the myth of the *homo constans* - the ideal, unwavering individual, always vigilant and perfectly rational, summarised in the old maxim "*Vigilantibus non dormientibus iura succurrunt*" (the law assists those who are vigilant, not those who sleep). To consider only sophisticated fraud punishable would mean devaluing and leaving without protection all those victims who, due to frailty, age, loneliness, or naivety, are unable to unmask seemingly trivial deceptions.

Contractual and non-contractual fraud

Moving away from ancient definitions, modern jurisprudence frames deception through two main lenses, both based on the manipulated cooperation of the victim:

- **Contractual fraud:** the victim is induced to conclude an agreement based on artificially altered factual premises, generating a loss for the defrauded and an unfair profit for the scammer. Examples include selling a car with a tampered odometer, or investment fraud (where the criminal collects capital promising high interest, pays the first instalments to gain trust, and then vanishes with the money).
- **Non-contractual fraud:** the patrimonial exploitation occurs outside a typical contractual framework. The perpetrator achieves an unfair profit by creating a false appearance. This category includes romance scams (simulating a romantic relationship, often at a distance, to extort money) or the so-called "broken mirror scam" (a fake traffic accident where the victim is accused of non-existent damage to obtain a cash settlement on the spot).

Stellionatus: the chameleon crime

When a deception didn't fit into standard categories, Romans prosecuted it as *stellionatus*. The term derives from *stellio* (the gecko or starry lizard), an animal believed to change its colours to blend into the background. This metaphor is strikingly relevant today: like the gecko, the modern scammer uses Pretexting to blend perfectly into the victim's environment (the fake bank, the fake utility company).

The evolution of Common Law: from "Caveat Emptor" to the "Confidence Man"

Historically, English Common Law was ruled by the harsh maxim *Caveat Emptor* ("Let the buyer beware"). The law protected the prudent, not the gullible. If a person was foolish enough to believe a lie, the law offered no remedy.

The paradigm shift occurred in the Victorian era with the birth of the term "Confidence Man" (1849), coined during the trial of William Thompson. Thompson didn't steal; he asked strangers to lend him their watches to demonstrate their "confidence" in him.

The Modern Shift (The Fraud Act 2006): Today, UK law has reversed *Caveat Emptor*. Under the Fraud Act 2006, the crime is defined by "False Representation". Crucially, the prosecution does not need to prove that the victim was deceived or suffered a loss. The crime is completed the moment the scammer communicates the lie with the intent to make a gain.

Why this matters today

This legal evolution reflects a moral one: society has moved from blaming the victim for their naivety to criminalising the manipulator for their intent.

Historically, the law asked: "Why were you not more careful?"

Today, the law asks: "Why did the offender choose to lie?"

Modern prevention strategies must align with this legal framework: the goal is to stop stigmatising the victim for "falling for it" and focus instead on the sophisticated mechanisms used to engineer that fall. This historical shift matters because it helps reframe contemporary fraud prevention away from victim blame and towards a clearer understanding of offender strategy.

Chapter 2 - The mind of the manipulator and the ecology of defence

If we wish to build a robust “Ecology of Defence”, we must first dissect the ecology of the attack. It is futile to focus merely on the technological vectors (be it the smartphone or the AI generator) as these are simply the delivery mechanisms. To defend effectively, we must shift our gaze from the tool to the hand that wields it.

In this chapter, we will analyse the manipulative repertoire used by offenders. We will look at how scammers construct a false reality (Meta-Deception) and how they disable their own moral inhibitions to target the vulnerable.

However, it is worth noting that this analysis does not exist in a vacuum. The techniques described here are not random; they are evolutionary adaptations designed to exploit specific cognitive vulnerabilities such as Truth Bias. While Chapter 3 examines our psychological vulnerabilities, this section focuses on the techniques designed to exploit them.

2.1 Meta-deception and the art of "pretexting": constructing the stage

The expert scammer does not merely tell lies; they orchestrate a complete, alternative reality. Rampin & Caris define this crucial concept as "Meta-Deception" or "Invisibility". The danger lies in the fact that the deception is not located in the specific request (e.g., "transfer this money"), but in the entire context created to justify it. By the time the request is made, it appears not as a demand, but as a logical, necessary step within the established narrative.

Christopher Hadnagy distinguishes between a simple lie and the advanced technique of "Pretexting". While a lie is a verbal falsehood, Pretexting is the art of "becoming anyone you want to be" through the manipulation of the environment.

To achieve this, the scammer uses "Reality Anchors":

- **Aural Staging:** using background soundscapes (e.g., the hum of a busy call centre, police sirens, hospital monitors) to bypass the victim's scepticism via the auditory channel.
- **Data Weaponisation (OSINT):** as established in Chapter 1, the scammer uses gathered intelligence to cement the pretext. When a caller knows the victim's last transaction date or their branch manager's name, the victim's brain, seeking patterns, concludes: "Only the real bank could know this."

The theatre of the mind

Effectively, the scammer invites the victim to become an unwitting actor in a scripted play. Whether posing as a technical support agent or a distressed relative, the scammer creates a scenario where the victim does not feel like "prey," but rather like a protagonist in a necessary procedure. This camouflage makes the threat effectively invisible until the damage is done.

2.2 Sellers of meaning

There is a pervasive myth in the field of fraud prevention suggesting that victims fall for scams simply due to greed. However, this represents a dangerous oversimplification of the dynamic. Maria Konnikova (2016), in her extensive study *The Confidence Game*, reveals a more uncomfortable truth: scams succeed because they satisfy our profound human need for meaning, magic, and hope.

The Confidence Loop

Why scams don't stop by themselves

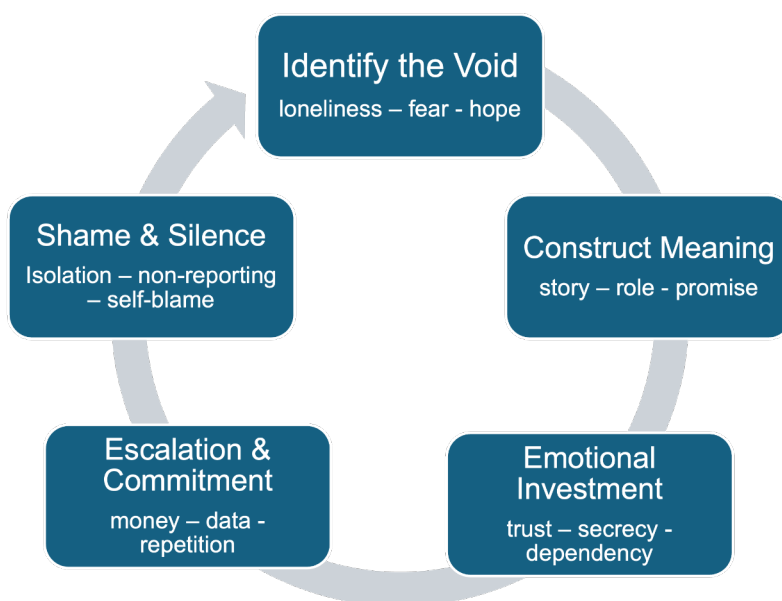


Figure 2. The Confidence Loop. A recurring psychological process through which scams develop and persist: from the identification of emotional vulnerability, to meaning construction and emotional investment, followed by escalating commitment and reinforced silence. The loop explains why scams rarely stop spontaneously and why external interruption is required to prevent repetition.

Identifying the void

Before the scam begins, the fraudster performs what confidence artists call the "Put-up": scanning the victim to identify what is missing in their life.

- For the lonely, they sell connection (Romance Scams).
- For the financially insecure, they sell stability (Investment Fraud).
- For the elderly fearing irrelevance, they sell significance (Grandchild Scams the chance to be a hero).

Ultimately, the scammer does not sell a product; **they are often offering a psychologically attractive alternative reality.** They offer a seductive world where the victim is smarter, richer, or more loved than they actually are.

As Konnikova explains, "the eternal lure of the con is the same reason religions arise... People join something that will give them meaning". The scam provides a coherent narrative in a chaotic world. When a victim transfers money to a "crypto guru" or a "secret fiancé," they are not just buying a promise; they are purchasing a dopamine hit of hope.

This emotional transaction creates a powerful psychological bond that is hard to break. The scammer becomes the source of the victim's happiness and self-worth.

This explains the baffling phenomenon where victims become hostile towards family members or police who try to intervene. For them, to admit the scam is real is to destroy the very hope that has sustained them. The victim may resist intervention strongly because, subconsciously, defending the scammer means defending their own dream. The fraudster has successfully intertwined their identity with the victim's deepest aspirations, making the deception emotionally impossible to reject.

2.3 Silencing the conscience

We often find ourselves wondering how one human being can perpetrate such financially and emotionally devastating crimes against the most vulnerable. The answer provided by criminal psychology suggests that scammers are not necessarily psychopaths lacking empathy, but rather that they are experts in **Moral Neutralisation**.

The process of dehumanisation

To operate effectively, the scammer must surgically remove empathy from the equation. They employ a psychological defence mechanism, first identified by criminologists Sykes and Matza (1957), known as **Neutralisation Techniques**. This process involves constructing a sophisticated internal narrative that justifies their behaviour, allowing them to bypass their own moral compass.

- **Denial of injury:** the scammer convinces themselves that "no one is really getting hurt". They rationalise their actions by telling themselves that banks will reimburse the loss, or that the victim is wealthy enough to absorb it without pain.
- **Denial of the victim (blaming the target):** this is the most insidious technique. The scammer reframes the victim not as an innocent party, but as a guilty one. They tell themselves: "They are greedy," "They are stupid," or

"They asked for it by trying to get rich quick." By devaluing the victim's intelligence or morality, the scammer feels justified in punishing them.

- **Recharacterisation of the event (the scam disguised as a calculated risk):** capitalising on the proximity between fraud (especially contractual fraud) and normal commercial or financial transactions, the scammer redefines the committed acts. In their own eyes, they are not perpetrating a deception that causes unfair patrimonial damage, but simply managing a contract or investment characterised by a high degree of risk that has unfortunately failed. It is the perfect psychological alibi to absolve themselves of responsibility, especially in frauds related to trading or cryptocurrencies.

The screen as a shield

In the modern digital landscape, this process is amplified by technology. The physical distance created by the phone or computer screen facilitates **depersonalisation**. The victim is no longer perceived as a grandmother losing her life savings, but merely as a "lead," a "mark," or a row of data in a CRM system.

This industrialisation of fraud allows the operator to detach completely. They are not stealing; they are simply "following the script" or "closing a deal." This psychological distancing is what enables the scammer to maintain a friendly, professional tone (rapport) while systematically dismantling the victim's life.

2.4 Sensory overload: The DoS attack on the brain

Why do intelligent victims obey absurd commands, such as throwing jewellery out of a window or transferring savings to a "safe account" in a foreign country? It is not a matter of stupidity; rather, it is the result of a calculated psychological assault known in this paper as **Sensory Overload**.

TRUE STORY

"It wasn't me". The power of artificial intelligence

"My daughter called me. She was crying. She said she had crashed into a luxury car and needed €2,000 immediately to avoid the police being involved. The voice was hers. The crying was hers. How could I not believe it?"

In reality, that was not her daughter. It was AI voice cloning software that replicated her voice using a 15-second video found on Instagram.

The Lesson: Today, sensory cues alone may no longer be sufficient; verification protocols matter more than ever.

Had the victim asked for the family "Safe Word", the AI would not have known how to answer.

The Amygdala hijack

In cybersecurity, a Denial of Service (DoS) attack crashes a server by flooding it with more traffic than it can handle. A scam can produce a comparable effect in human decision-making.

By bombarding the target with high-intensity stimuli, fear, urgency, aggressive tones, and background noise, the offender may push the person into what behavioural literature often describes as a “hot state”. Under these conditions, as neurobiological research demonstrates that acute stress impairs prefrontal cortex cognitive function (Arnsten, 1998), reflective judgement is severely reduced, and reactive responding becomes the default mode.

Rampin & Caris highlight a specific technique used to induce this collapse: **forced multitasking** or “polychronic demands”.

Crucially, the scammer never allows the victim to focus on a single task. They will demand the victim:

1. Stay on the phone (audio engagement).
2. Log into their online banking (visual/manual engagement).
3. Write down codes (motor engagement).
4. Listen to threats of imminent arrest (emotional engagement).

By saturating every cognitive channel simultaneously, the scammer consumes the victim's entire “working memory”. The victim simply does not have the “bandwidth” left to question the legitimacy of the request.

This overload may produce a state that is sometimes described, in applied contexts, as a **confusion trance**. The brain, unable to process the conflicting stream of data, freezes (the “rabbit in the headlights” effect). In this moment of cognitive vacuum, the scammer inserts a simple, direct command (“Read me the code”). The target may comply not because they agree with the request, but because compliance seems the only way to stop the overwhelming noise and reduce the psychological pressure.

To defuse this emotional overload, the preventive adoption of a safe word represents the quickest countermeasure. For a practical guide on how to establish and use this fundamental family circuit breaker, please refer to Annex F.

Chapter 3 - The psychology of the target - why vulnerability is widely distributed

Perhaps the most persistent myth in the field of fraud prevention is that victims are greedy, uneducated, or cognitively impaired. We must realise that this stereotype is not only false but dangerous, as it fuels the false sense of security that scammers rely upon.

The reality, supported by current psychological research, is that vulnerability to scams cannot be reduced to IQ and is better understood in relation to common human cognitive tendencies. People broadly share common cognitive architectures and heuristics: mental shortcuts that evolved to help us survive in a tribal environment, not to navigate a digital minefield. As Maria Konnikova notes, "The con [confidence game] doesn't work because we are stupid; it works because we are human". The scammer targets System 1 (fast, emotional thinking), as described by Daniel Kahneman (2011), bypassing System 2 (slow, deliberative thinking), including among individuals with high levels of education or professional experience. In some contexts, highly confident or cognitively sophisticated individuals may be especially prone to rationalising implausible scenarios.

3.1 The "Lake Wobegon Effect": the paradox of intelligence

Which profiles may become particularly susceptible under specific scam conditions? Contrary to popular belief, susceptibility does not map neatly onto insecurity or isolation alone; in some cases, overconfidence may itself become a risk factor.

The illusion of superiority

Maria Konnikova identifies this phenomenon as the "Lake Wobegon Effect"¹, named after the fictional town where "all the children are above average." Psychologically, it refers to Illusory Superiority: the statistical tendency for most people to believe they possess above-average intelligence, moral character, and judgement.

This cognitive bias creates a dangerous blind spot in our defences. Because we believe we are astute observers of human nature, we assume we would effortlessly spot a scam. We incorrectly think: "I would certainly know if someone was lying to me."

¹ The term originates from Garrison Keillor's fictional town of Lake Wobegon, a place where "all the children are above average". Psychologically, it refers to the "Illusion of Superiority": the cognitive bias where individuals systematically overestimate their own intelligence, judgement, and morality compared to others. In the context of fraud, this overconfidence becomes a critical vulnerability. Individuals who believe they are too astute to be deceived ("It won't happen to me") lower their critical defences and ignore obvious red flags, paradoxically making themselves ideal targets for scammers who expertly exploit this ego-driven blind spot.

This illusion of immunity can become a major asset for the scammer. A person who perceives themselves as unlikely to be deceived may be less inclined to verify facts, seek second opinions, or pause to reflect. They trust their "gut instinct," unaware that their instinct is being manipulated.

In addition, Konnikova suggests that intelligent people can be more vulnerable to complex scams (like financial fraud) because they are accustomed to understanding things quickly. When a scammer presents a convoluted investment scheme, the intelligent victim's ego prevents them from admitting they don't understand, or worse, their intellect works overtime to construct a logical explanation for the scammer's lies. As the adage goes: "You can't cheat an honest man, but you can easily cheat a confident one".

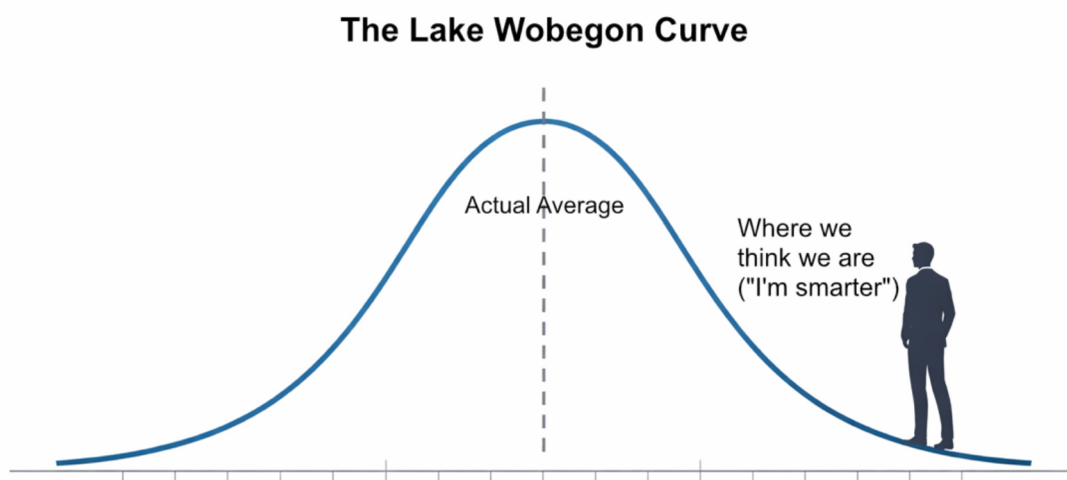


Figure 3. The Lake Wobegon Curve. The Lake Wobegon Effect describes the systematic tendency of individuals to believe they are more intelligent, competent, or discerning than the average. In the context of fraud, this illusion of superiority reduces vigilance and increases susceptibility, as confidence in one's own judgement discourages verification, external consultation, and critical doubt.

3.2 The fear-relief loop

As Rampin & Caris illustrate, the scammer artificially generates a crisis (e.g., "Your bank account has been compromised by hackers" or "Your nephew is in police custody"). This instantly places the victim in a state of high anxiety (System 1). Then, immediately after creating this panic, the scammer graciously offers the antidote: a safety procedure, a secure account, or immediate legal assistance. This triggers a powerful psychological response known as "Fear-Then-Relief": the immense relief of finding a solution floods the brain with chemicals that suppress caution and generate premature gratitude.

Christopher Hadnagy notes that successful social engineers act to create a bond of rapport (empathy/connection) with the victim. Effectively, they position themselves on

the same side of the desk as the target. It becomes an alliance: "You and I need to work together to stop these thieves" or "We need to act fast to fix this bureaucracy".

This creates a dangerous "Us vs. Them" dynamic. The victim ceases to be a passive observer and becomes an active collaborator. They are not merely obeying orders; they believe they are proactively protecting their assets alongside a professional. This explains why victims often ignore warnings from genuine bank tellers or police officers - they have been coached by the scammer to view everyone else as an obstacle to the "rescue operation".

3.3 The psychology of shame after fraud

While the aftermath of a scam is often described solely in financial terms, the psychological damage is frequently far more enduring. The victim suffers what we might call a profound "injury of trust", not just towards others but, perhaps more damagingly, towards their own judgement.

Maria Konnikova explains that professional scammers deliberately engineer this shame. In a phase technically known as "The Blow-Off", the fraudster manages the reveal of the scam in a way that makes the victim feel foolish rather than victimised. Here, the psychological logic is harsh but often effective: most people value their social reputation more than their money. The victim may reason: "If I report this, everyone will know I was duped. Better to absorb the loss in silence." In some criminal variants (such as romance scams or sexual extortion), the scammer transforms this fear into an active weapon, threatening to publicly expose the victim's naivety or intimate secrets to force continuous payments.

For the elderly demographic, this silence is enforced by a specific, paralysing fear: the loss of independence. The victim deeply fears that admitting to being scammed will be interpreted by family members not as a crime suffered, but as a symptom of cognitive decline or senility. The thought "If I tell my children, they will take away control of my bank account or move me to a care home" may become a stronger deterrent to reporting than the pursuit of justice.

Secondary victimisation and non-judgemental listening

This dynamic often leads to a spiral of isolation. Victims withdraw from the community to hide their "mistake", unwittingly removing the very safety net (neighbours, friends) that could protect them from future attacks. This generates so-called "secondary victimisation": further psychological damage caused not by the scammer, but by the reactions of the social and institutional environment. When family members, bank tellers, or law enforcement react with phrases like "*How could you not realise?*", they blame the target and reinforce their sense of inadequacy.

It is in this context that the role of community networks becomes crucial: offering a space for strictly non-judgemental listening, helping the victim recognise that they were not "stupid", but rather subjected to manipulation by a highly skilled offender using structured psychological techniques.

3.4 The cognitive arsenal: the biases that betray us

It is important to recognise that our brains are not designed for scepticism, but rather for efficiency. To save energy, we use mental shortcuts called Cognitive Biases. Scammers simply "hack" these shortcuts:

- **Truth Bias (The default setting).** By default, our brains are programmed to believe that others are telling us the truth. Evolution has taught us that trust is essential for social cooperation. The scammer ruthlessly exploits this "factory setting": doubt is not our first reaction, but a cognitive effort that requires energy (System 2) and time that we are often not granted.
- **Optimism Bias: "It won't happen to me".** As Maria Konnikova explains, we are biologically wired to think the future will be better than the past. This leads us to drastically underestimate the probability of personal negative events. When faced with an offer that is "too good to be true", the Optimism Bias silences critical thinking simply because we desperately want it to be true.
- **Authority Bias: Automatic obedience.** Robert Cialdini (2007) highlights how we are conditioned from childhood to obey authority figures (parents, teachers, police officers) without question. When a scammer wears a uniform or uses an institutional tone ("This is the Fraud Squad"), our brain suspends critical judgement and activates "obey mode".
- **Confirmation Bias: Selective blindness.** Once we have "taken the bait" (e.g., "I found love online" or "this investment will make me rich"), our brain starts filtering reality. We accept only the information that confirms our hope and actively ignore Red Flags. As Konnikova notes, we interpret facts to serve our theory, becoming the scammer's best allies.
- **Sunk Cost Fallacy: The final trap.** This is the bias that prevents the victim from stopping. When we start to suspect deception, we have often already invested time, money, or emotions. The brain reasons: "If I stop now, I've lost everything and I'm a fool. If I pay a little more, maybe I can get it all back". It is the psychological lever that turns a loss into financial ruin.

Understanding these biases leads us to a disturbing but necessary conclusion: intelligence alone is not a reliable shield under conditions of emotional manipulation. Since these cognitive shortcuts are biological adaptations for efficiency, they operate below the threshold of conscious awareness. As Konnikova demonstrates, the scammer does not need to 'hack' a complex code; they merely need to present the right stimulus to trigger a pre-installed behavioural sequence, effectively bypassing our rational defences.

This is why traditional 'be careful' campaigns often fail. One cannot override evolutionarily ingrained response systems through willpower alone, especially in moments of high emotional stress or sensory overload. To defeat a scam, we do not

need a smarter brain alone; we need structural external support mechanisms. This is a strategic role that Neighbourhood Watch networks are particularly well positioned to fulfil, in complementarity with institutional actors: to provide objective, external verification that a victim's brain, temporarily compromised by cognitive and emotional biases, cannot be reliably accessed or sustained under acute stress conditions.

Chapter 4 - From theory to practice

This chapter moves away from traditional operational guidelines. Instead of prescribing standard procedures, it presents **strategic levers** designed to address the cognitive vulnerabilities that emerge under stress and isolation.

The goal is to support **strategic deliberation** rather than impose operational replication. National Neighbourhood Watch Associations are invited to view the following sections as:

- **conceptual tools**, not instructions
- **modular options**, not a linear programme
- **adaptable frameworks**, not uniform standards

Each lever aims to **activate the cognitive switch**: restoring deliberative judgement when automatic emotional responses dominate.

The previous chapters have demonstrated a critical limitation of traditional fraud prevention strategies: **psychological awareness alone may not constitute an effective defence**. Under conditions of emotional stress, urgency, or sensory overload, individual cognitive control mechanisms are temporarily impaired. In such moments, knowledge is present but inaccessible.

This chapter translates the analytical framework developed so far into a set of strategic options that National Neighbourhood Watch Associations may consider when shaping their prevention policies. At this stage, the strategic question is no longer whether fraud exploits psychological mechanisms (this has been established) but **how community-based structures can systematically compensate for predictable cognitive failures**.

Strategic orientation

National Associations may consider adopting one or more of the following strategic levers, independently or in combination:

- **Recognition Frameworks** (Cognitive Literacy)
- **Social Circuit Breakers** (The Designated Sceptic)
- **Environmental Nudging**
- **Stress Inoculation and Simulation**

Each lever addresses a distinct vulnerability identified in Chapters 1–3 and is grounded in established research in psychology, criminology, and behavioural science.

4.1 The cognitive switch: from automatic reaction to deliberative control

The core of these strategies is the cognitive switch. Under pressure, decision-making shifts automatically from reasoning to reaction. This is not a personal failure, but a biological response. Once this shift occurs, it is nearly impossible to restore rational control through willpower alone.

Drawing on foundational principles of emotion regulation (Gross, 1998), the Cognitive Switch describes the moment at which an external stimulus interrupts this automatic reaction, allowing deliberative reasoning to re-engage. This stimulus may take different forms: a trusted third party, an environmental cue, a procedural pause, or a rehearsed interruption. What these interventions share is not their format, but their function: they act as external triggers that support the re-engagement of deliberative assessment.

Figure 4 illustrates this mechanism schematically, highlighting the structural asymmetry between the speed of emotional activation and the slower recovery of rational control.

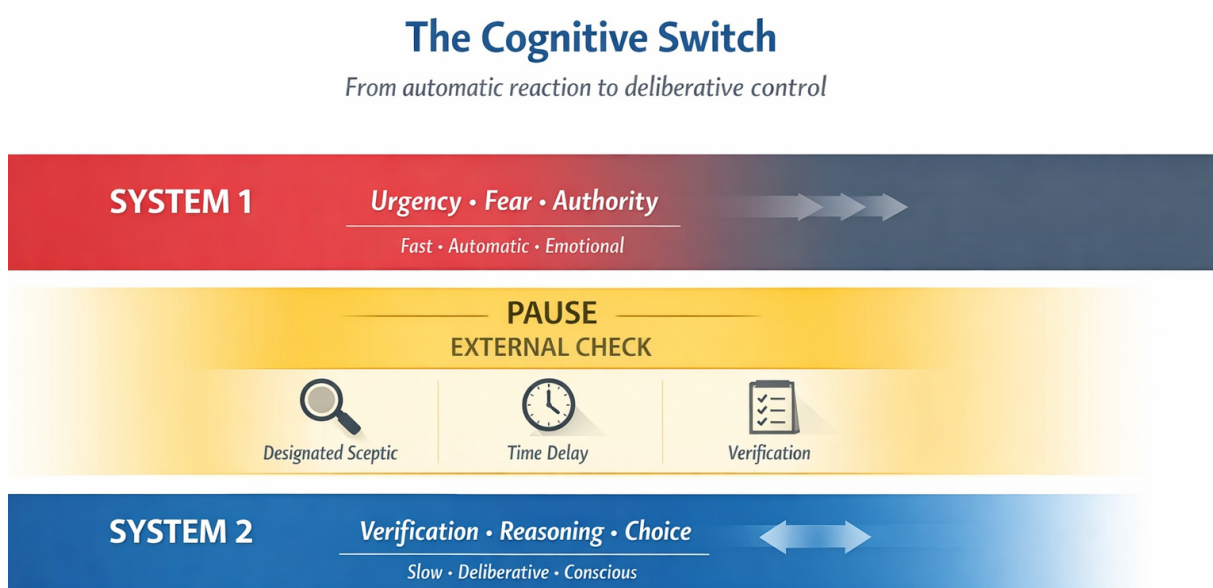


Figure 4. The Cognitive Switch. Under conditions of urgency, fear, or authority pressure, decision-making shifts from deliberative reasoning (System 2) to automatic emotional response (System 1). The “Cognitive Switch” is activated not by individual willpower, but by external interruption, such as time delay, verification, or consultation with a trusted third party, restoring access to rational judgement.

From a strategic perspective, this has a critical implication: effective fraud prevention cannot rely exclusively on individual awareness or self-control. It must instead focus on designing social, environmental, and organisational conditions that increase the

likelihood of activating what this paper terms the Cognitive Switch when it is most needed.

The strategic options outlined in this chapter should therefore be read as different pathways to the same objective: ensuring that, at critical moments, no individual is left cognitively isolated.

A strategic shift in prevention logic

The following options are based on a specific analytical logic.

Regardless of whether the caller claims to be a police officer, a bank clerk, or a grandchild, the underlying psychological structure often remains recognisably similar. **By teaching members to recognise the emotional signature of an attack rather than the specific story, we improve their preparedness for future and evolving scam variants.**

Recognition frameworks encourage a shift away from asking "Is this story plausible?" (as the Lake Wobegon Effect often leads us to believe it is) and towards asking "What psychological lever is being pulled?". To facilitate this, we use the **Rapid Recognition Matrix**.

The good news is that you do not need to memorise every possible scenario. From a strategic perspective, focusing on a limited set of recurrent warning signals reduces cognitive load. The model prioritises three recurrent warning signs as a practical recognition aid. If you spot one, activate your defences.

Traditional prevention models focus on identifying and cataloguing fraud narratives. While intuitive, this approach assumes that deception operates primarily at the level of content.

Professionalised fraud, however, functions at the level of syntax: the underlying psychological structure that governs how pressure, authority, urgency, and isolation are deployed to bypass deliberative judgement.

Decoding this syntax allows prevention strategies to remain effective even as specific scam narratives evolve. From a strategic perspective, this shift reframes fraud recognition from a reactive activity into a structural competence.

Rapid Recognition Matrix



RED FLAG 1: Urgency (The Panic Button)

- **What happens:** They rush you ("Your account is blocked!", "Your grandson is under arrest!").
- **Why:** They want to switch off your rational brain.
- **Your reaction: STOP.** Hang up the phone. Count to 10. No real emergency requires money in 2 minutes.



RED FLAG 2: Flattery (The Ego Trap)

- **What happens:** They make you feel special, intelligent, or lucky ("You have won!", "You are the only one who can help us").
- **Why:** They want to lower your defences by exploiting vanity.
- **Your reaction: DOUBT.** Ask yourself: "Why me?". If it is too good to be true, it is fake.



RED FLAG 3: Secrecy (Isolation)

- **What happens:** They ask you not to tell anyone ("It is a secret investigation", "Do not worry your children").
- **Why:** They want to isolate you from your "pack".
- **Your reaction: CALL.** Break the secrecy. Call your "Designated Sceptic" immediately.

The following table does not represent an operational protocol. It is an analytical framework designed to illustrate the recurrent psychological structures underlying different fraud typologies and their corresponding cognitive vulnerabilities. It does not prescribe behavioural responses, nor does it imply standardised intervention models. The complete technical table can be consulted in Annex A.

Table 1. Analytical Mapping of Fraud Syntax and Cognitive Vulnerabilities

ATTACK TYPE	TYPICAL SCENARIO	PSYCHOLOGICAL LEVER	COGNITIVE VULNERABILITY	RED FLAG (Signal)	COGNITIVE COUNTERMEASURE ACTIVE SILENCE
ELICITATION Data Harvesting Subtle extraction	Friendly chat Wrong number text Fake surveys	Rapport Building Artificial intimacy Empathy / Vanity Scammer makes you feel heard or important	Truth Bias Assumption of honesty	<ul style="list-style-type: none"> ▶ The Wrong Statement: Stranger makes a wrong claim to make you correct them ("I guess you're new here...") 	<ul style="list-style-type: none"> 🚫 Do not correct 🚫 Do not give details ✅ Close: <i>"I don't discuss personal matters with strangers"</i>
PRETEXTING Meta-Deception (Constructed Scenario)	Fake Bank Fraud Team Fake Utility Technician	Meta-Deception False reality via jargon Authority / Fear Uses uniform or jargon to inhibit control	Authority Bias Obedience to titles	<ul style="list-style-type: none"> ▶ Polychronic Demand: Forced to talk + log in simultaneously ▶ Induced Urgency: "Act now to avoid fine" 	<p>CHANNEL VERIFICATION</p> <ul style="list-style-type: none"> 🚫 Do not use provided numbers ✅ Call-Back: Call official entity ✅ Visual Check: Ask for ID outside
VISCERAL ATTACK Shock & Awe Direct Attack	"Grandchild arrested" "Account drained" Legal threat	Sensory Overload Crashing logic	Amygdala Hijack Panic overrides logic	<ul style="list-style-type: none"> ▶ Forced Isolation: "Don't tell anyone" ▶ Immediate Money request: for emergency 	<p>STOP & FREEZE</p> <ul style="list-style-type: none"> 🚫 Sensory Stop: Hang up phone ✅ Breathe: Wait 5 mins ✅ Safe Word: Call relative (see Annex F)
HOPE SCAM (The Long Con) (Scam of Hope)	Crypto / Investment Romance Scam	Selling Meaning Fulfilling a void Promise of a better life (Konnikova)	Optimism Bias & Sunk Cost Fallacy	<ul style="list-style-type: none"> ▶ Too good to be true ▶ The "Put-up": Fits dreams perfectly ▶ Exclusivity: "Offer just for you" 	<p>DESIGNATED SCEPTIC</p> <ul style="list-style-type: none"> 🚫 Do not decide alone ✅ Show offer to "Circuit Breaker"/to your Sceptic

Refining the mechanism: habit over reasoning

It may appear paradoxical to propose a deliberative defence for a brain under acute stress. However, the objective is not to rely on spontaneous reasoning during a crisis, but to transform the “cognitive switch” into a conditioned reflex. Much like emergency drills, this defence relies on pre-learned habits that can bypass emotional blockage through repetition and social support, rather than through complex analysis in the moment of danger.

4.2 Social circuit breakers

The designated sceptic as external cognitive support

Successful fraud almost always relies on isolating the target. In moments of crisis, scammers encourage people to act alone, whether explicitly or through the pressure of the situation, to prevent them from seeking a second opinion. This isolation amplifies cognitive overload and prevents corrective feedback at precisely the moment when judgement is most impaired.

Psychological research demonstrates that decision-making under emotional pressure is often less reliable. Once reactive processing dominates, internal deliberation cannot always be restored through information or self-assurance alone. What may prove especially valuable instead is **external verification**: the intervention of a third party who is not subject to the same emotional activation.

The concept of the Designated Sceptic operationalises this principle at a social level. It introduces a pre-existing relational checkpoint capable of interrupting the reactive response and re-engaging deliberative reasoning.

The Designated Sceptic acts as an **external trigger of the Cognitive Switch**. By requiring consultation before irreversible action, it introduces a pause, shifts attention away from the manipulative stimulus, and supports the re-engagement of rational assessment. Crucially, this function does not primarily depend on technical expertise, but on emotional distance and trust.

National Associations may consider framing the Designated Sceptic:

- as a cultural norm rather than a formal role
- as a dignity-preserving safeguard, not a sign of incapacity
- as a complement to existing community or safeguarding structures

The specific form of implementation remains context dependent. The strategic objective is not standardisation, but the normalisation of consultation under pressure.

4.3 Environmental nudging

Designing friction into decision-making

Under conditions of fear, urgency, or emotional arousal, individuals experience a marked reduction in memory recall and abstract reasoning. Even well-established knowledge, such as awareness of common scams, may become temporarily inaccessible. Prevention strategies that rely on recall alone therefore fail at the critical moment.

Environmental cues often influence our choices without us realising it (Thaler & Sunstein, 2008). Introducing small points of 'friction' during a crisis can break the cycle of automatic compliance, giving the person just enough time to stop and think.

Unlike more information-heavy warnings, nudges may require less deliberative interpretation in the moment. Their effectiveness lies in their immediacy and physical presence.

Environmental nudges act as non-verbal activators of the Cognitive Switch. By disrupting the stimulus–response sequence engineered by the offender, they create a micro-pause that allows emotional intensity to subside and deliberative processing to re-engage.

Depending on national context, Associations may explore:

- visual prompts at common points of compromise (phones, doors, screens)
- integration with existing public awareness materials
- culturally appropriate symbols or phrasing

The strategic goal is not instruction, but interruption.

4.4 Stress inoculation and simulation

Building resistance through controlled exposure

Knowledge that is not reinforced through practice degrades rapidly under stress. Social norms, such as politeness, deference to authority, and reluctance to interrupt, further inhibit defensive behaviour, even when risk is perceived.

Research on resistance to persuasion indicates that controlled exposure to manipulative techniques may strengthen later resistance (McGuire, 1961). Practised responses may be more readily accessible under pressure than abstract principles. This approach shifts prevention from passive understanding to rehearsed response.

Stress inoculation may increase the likelihood of activating the Cognitive Switch under pressure. By rehearsing interruption, refusal, or verification in low-stakes contexts, these practices may help reduce hesitation in real-world situations.

National Associations may evaluate:

- simulation-based training for coordinators or leadership
- role-based exercises focused on refusal and interruption
- internal stress-testing of communication protocols

Such initiatives are not intended as operational drills, but as **strategic investments in cognitive resilience**.

Chapter 5 - Strategic considerations for National Boards

EUNWA identifies five key areas where a shift in strategy could significantly improve community safety:

1. **Facilitate shared approaches (The terminology proposal):** Scam reporting is currently fragmented. To fight a transnational threat, we need a shared language. We encourage National Boards to adopt the categories defined in this paper—such as distinguishing "sensory overload" from generic confusion. Using a common lexicon professionalises the volunteer force and simplifies cross-border knowledge exchange.
2. **Mainstreaming the "Designated Sceptic":** This concept should move from a niche tip to a **mainstream cultural habit**. National campaigns could frame this as a standard household safety measure, much like a smoke alarm. This normalises asking for help and reduces the psychological barrier for victims who fear judgement.
3. **From information to inoculation (Active training):** Given the limits of passive leaflets, we propose that National Boards explore **interactive workshops** based on "stress inoculation", such as role-playing and simulations. Moving from lecturing to rehearsal helps make interruption, refusal, and verification responses accessible under emotional pressure.
4. **De-stigmatisation and changing the narrative:** We invite all associations to align their communication with the modern legal framework: fraud is professionalised manipulation. Falling for a con is a result of widespread human vulnerability, not stupidity. **Promoting this view encourages reporting and deprives scammers of their greatest asset: the victim's silence.**
5. **Commitment to empirical validation (Pilot testing):** We encourage national associations to treat early implementations of these frameworks as pilot studies. Sharing qualitative and quantitative feedback within the European network is essential for refining our collective strategy. This transforms local initiatives into shared insights, bridging the gap between theory and evidence-based defence.

The synergistic integration of these five priorities does not require overhauling existing protocols but rather reorienting them. By embracing these priorities, National Boards

have the opportunity to transform prevention: from a fragmented distribution of warnings into a robust, shared defence architecture across Europe.

5.1 The Resilience of the Community

The modern scammer represents an unequal threat: they possess sophisticated psychological scripts, unlimited patience, and technological anonymity, while the victim often stands alone, relying on cognitive and emotional systems that may be poorly suited to resisting manipulative pressure in digital environments. However, this asymmetry is reversed the moment the individual steps out of isolation and into a network.

By transforming Neighbourhood Watch groups from passive observers of physical space into active contributors to cognitive resilience within their communities, we create a layer of defence that software alone cannot provide. Ultimately, the “Human Firewall” described in this paper is not built of code, but of conversation, non-judgemental support, and the simple act of asking a neighbour: “Does this sound right to you?”

EUNWA offers this framework as a living toolkit. We invite every National Association to take these insights, adapt them to their local reality, and help build a Europe where, thanks to the bond between neighbours, no one should face manipulative fraud alone.






This page intentionally left blank.

References

- Arnsten, A.F.T.** (1998). *Stress impairs prefrontal cortex cognitive function*. *Science*, 280, 1711–1712.
- Cialdini, R. B.** (2007). *Influence: The Psychology of Persuasion*. HarperCollins.
- Europol.** (2024). *Internet Organised Crime Threat Assessment (IOCTA)*.
- Goleman, D.** (1995). *Emotional Intelligence*. Bantam Books.
- Gross, J.J.** (1998). *The emerging field of emotion regulation: An integrative review*. *Review of General Psychology*, 2(3), 271–299.
- Hadnagy, C.** (2018). *Social Engineering: The Science of Human Hacking* (2nd Edition). Wiley.
- Kahneman, D.** (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux.
- Konnikova, M.** (2016). *The Confidence Game: Why We Fall for It... Every Time*. Viking.
- McGuire, W. J.** (1961). *Resistance to Persuasion Conferred by Active and Passive Prior Refutation*. *Journal of Abnormal and Social Psychology*.
- Rampin, M., & Caris, R.** (2011). *Fraudologia: Teoria e tecniche della truffa*. (*Fraudology: Theory and techniques of fraud.*) Edizioni Scuola di Palo Alto.
- Sykes, G. M., & Matza, D.** (1957). *Techniques of Neutralization: A Theory of Delinquency*. *American Sociological Review*.
- Thaler, R. H., & Sunstein, C. R.** (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press.

ANNEX A: Advanced Psych - Ops Classification

Table 2. Mapping Threats to Cognitive Vulnerabilities

MACRO-CATEGORY	SPECIFIC TYPOLOGY	OFFENDER'S TECHNIQUE	TARGET'S BIAS	PSYCHOLOGICAL DYNAMIC	ACTION
1. RELATIONAL <i>(Emotional)</i>	Romance Scam 	The Put-up (Identifying the void)	Confirmation Bias (Ignoring red flags)	The Shield of Hope Victim defends scammer to protect self-worth.	BREAK ISOLATION
	Grandchild Scam 	Sensory Overload (Artificial urgency)	Amygdala Hijack (Biological bypass of logic)	Fear-Then-Relief Scammer creates pain, then offers the cure.	STOP & FREEZE
2. AUTHORITY <i>(Institutional)</i>	Vishing / Spoofing 	Meta-Deception (Invisibility via context)	Authority Bias (Learned obedience)	Role Reversal Victim becomes an "active collaborator".	CHANNEL VERIFICATION
	Fake Officials 	Pretexting (Theatrical performance)	Truth Bias (Default honesty)	Chameleon Effect <i>(Stellionatus)</i> Scammer blends into environment.	VISUAL CHECK
3. OPPORTUNITY <i>(Financial)</i>	Crypto / Investment 	Rapport Building (Grooming)	Lake Wobegon Effect (Illusion of superiority)	Rationalisation Intelligence used to justify the impossible return.	DESIGNATED SCEPTIC

ANNEX B: Action Card

The “STOP & CHECK” Protocol

Use when you feel **URGENCY**, **FEAR**, or **EUPHORIA**.

1. **STOP** (Stop the Emotion)

DO NOT open the door.

HANG UP the phone.

WAIT 5 minutes. The scammer is in a hurry, you are not.

2. **CHECK** (Unmask the Pretext)

WHO IS IT REALLY? “Did they use “OSINT” on me?”

WHY NOW? “Banks never call with urgency to ask for money.”

AM I THE FOOL? “Am I thinking “it won’t happen to me?””

3. **CALL** (Break Isolation)

Call your Designated Sceptic.

Call 112/999.

Anti-Trickery Guide

The scammer doesn't ask, they make you talk.

Watch out if a stranger:

- **✗** Makes wrong statements to make you correct them (“Your son lives here, right?” -> “No, in Milan!”).
- **✗** Gives too many compliments.

Your Shield Response:

“Excuse me, I don't share personal information with strangers.
Goodbye.”

ANNEX C: Cognitive Defence Glossary

Essential Terminology

Amygdala Hijack: In this paper, the term is used as an analytical shorthand for a state of acute emotional activation (such as fear or panic) in which deliberative reasoning may be significantly impaired. It is not intended as a precise neuroscientific category.

Authority Bias: The human brain's automatic tendency to obey and believe anyone wearing a uniform or using a formal/institutional tone.

Blow-Off, The: The final phase of a scam where the fraudster manages their exit, so the victim feels too ashamed to report the crime.

Contractual fraud: A model of deception where the victim is induced to enter an agreement (e.g., a fake financial investment or purchasing goods with hidden defects) based on premises altered by the scammer to gain an unfair profit.

Designated Sceptic: In this paper, the term refers to a trusted person identified in advance to provide an external verification or “circuit-breaker” function before irreversible action is taken.

Dolus bonus / Dolus malus: In Roman law, the distinction between tolerated commercial boasting (*bonus*) and the malevolent intent to deceive and circumvent (*malus*). Modern jurisprudence and prevention have moved beyond this rigid division: even a seemingly clumsy deception, if structured to exploit the vulnerabilities of others, constitutes a crime.

Elicitation: The art of extracting sensitive information through seemingly casual conversation, often by making wrong statements to prompt a correction.

Homo constans: An ideal and abstract figure in classical law describing an unwavering individual, always vigilant, perfectly rational, and immune to flattery. Modern victim protection and community approaches reject this myth, recognising the need to protect those who fall into traps due to temporary frailty, isolation, or naivety.

Inoculation Theory: A psychological approach suggesting that controlled exposure to weaker or simulated persuasive challenges may strengthen later resistance.

Lake Wobegon Effect (Illusory Superiority): A cognitive bias in which people tend to view themselves as more discerning or less vulnerable than average, potentially reducing verification and increasing exposure to fraud.

Meta-Deception: Used here as an analytical label for strategies that manipulate the surrounding context so that the scam appears procedurally normal or institutionally legitimate.

Non-contractual fraud: Patrimonial exploitation that occurs outside a typical contractual framework. The criminal obtains money by creating a false emotional or emergency appearance (e.g., the romance scam, the fake grandchild scam, or the broken mirror scam).

Nudge Theory: Designing the physical environment (e.g., placing a warning sticker on the phone) to alter behaviour in a positive way without coercion.

Polychronicity: Used here as an analytical label for forms of forced multitasking (e.g. talking, typing, and reading simultaneously) that may overload attention and reduce reflective judgement.

Pretexting: The construction and performance of an invented scenario, often supported by props, jargon, or contextual cues, in order to elicit trust, information, or compliance.

Stellionatus: An ancient Roman legal term for fraud, referring to the "gecko" or lizard, symbolising the scammer's ability to blend into the victim's environment.

ANNEX D: Your "Security Companion" (The Designated Sceptic)

This annex provides illustrative examples of how the strategic lever “Designated Sceptic”, described in Chapter 4, may be translated into practical arrangements.

We can forget forms and bureaucracy here. The concept of the Designated Sceptic is much simpler: it is a **pact between friends**. The logic behind this is straightforward: when we are under strong emotional pressure (such as fear or euphoria), our capacity for reflective judgement may be reduced. What may help in such moments is an external point of reference: someone more detached from the emotional pressure of the situation.

The role of the designated sceptic is not to replace individual agency, but to provide an external 'cognitive anchor'. This partnership is a voluntary exercise of autonomy: the individual proactively chooses to delegate a moment of verification to a trusted peer to protect their own interests against deceptive emotional manipulation.

How to activate it in your neighbourhood: You certainly do not need an official title to do this. You just need to say to a trusted neighbour or family member: "Let's make a deal: if anyone asks me for money or data in a strange way, I promise I will not do anything until I have called you. You must always pick up, okay?"

Essentially, they serve as a trusted source of external verification and emotional distance. They do not need to be a cybersecurity expert; they just need to be someone who cares about you and, not being under pressure, can see the deception that you might miss.

ANNEX E: Illustrative scenarios for stress inoculation

The following exercises are provided as conceptual frameworks, not as official training modules. Local training officers are encouraged to adapt these illustrative scenarios to align with their established methodologies and specific community needs.

One of the structural limitations of purely informational approaches is the **decay of knowledge under stress**. While reading this White Paper may increase cognitive awareness, awareness alone does not create behavioural readiness. In high-pressure situations, individuals do not rise to the level of their expectations; they revert to the level of their prior conditioning.

From a strategic perspective, in this paper stress inoculation refers to **controlled exposure to simplified or simulated forms of manipulation**, intended to strengthen preparedness and response under pressure. Research in persuasion psychology suggests that rehearsed responses are more readily accessible under emotional pressure than abstract rules or principles.

In practice, stress inoculation may take different forms depending on context and resources. Illustrative examples observed in some settings include:

- **Role-based simulations**, in which participants are exposed to simplified manipulative scripts in a controlled environment, with the explicit aim of practising interruption or refusal rather than successful resolution.
- **Verification exercises**, in which intentionally ambiguous or simulated alerts are used to observe and reinforce verification behaviours before information is disseminated within a group.

Such activities are not designed to replicate real attacks, but to **normalise interruption and refusal**. One of the scammer's most reliable advantages is social conditioning: politeness, deference, and reluctance to disengage. By lowering the psychological cost of saying "no" in low-stakes contexts, these practices may help reduce hesitation in real-world situations.

From a cognitive perspective, repeated exposure to refusal behaviours may increase the likelihood that the **Cognitive Switch** will be activated under stress. The objective is not technical proficiency, but the rehearsal of a behavioural response that interrupts automatic compliance during moments of sensory overload.

ANNEX F: The family safe word

The basic concept (the circuit breaker)

Within our Neighbourhood Watch networks, we know well that the most effective defence is often the simplest. In emergency-based scams (such as the fake accident or the arrested grandchild), the criminal relies entirely on the "amygdala hijack": inducing such a level of panic and urgency that the victim's logic is temporarily disabled.

The "safe word" is a preventive agreement within the family unit that acts as a true circuit breaker. It shatters the emotional intensity of the moment, forcing the situation back to a rational and verifiable level.

How to choose the right word

To be truly effective, the safe word must follow two fundamental rules:

- **The rule of unpredictability:** Absolutely avoid the names of pets, dates of birth, favourite sports teams, or holiday destinations. Professional scammers easily extract this data from the family's social media profiles (the elicitation phase).
- **The rule of family non-sense:** Choose an object, a colour, or a concept that is entirely decontextualised but easy for you to remember. An unusual combination like "yellow penguin" or "spanner" is impossible for a stranger to guess, yet unforgettable for family members.

How and when to use it: the operational protocol

Share this word exclusively with close family members or your "Designated Sceptic". If you receive an alarming phone call from someone claiming to be a relative in danger (often with a voice altered by fake crying or a bad connection), or from a supposed lawyer, doctor, or police officer calling on their behalf, apply this protocol:

- **The unlocking question:** Interrupt the caller's flow of words and ask firmly: "Before we continue, what is our safe word?".
- **The defensive action:** A scammer will try to evade the question, get angry ("There is no time for this nonsense, your grandson is in prison!"), or attempt to make you feel guilty for doubting them in a moment of crisis. If you do not receive the exact word, you are facing a scam. Terminate the communication immediately without providing further explanations.

Practical simulation (role-play)

Share this brief scenario with the members of your community to help them visualise the practical application of the technique:

Scammer (Fake Lawyer): "Madam, your son has caused a serious accident. He faces immediate arrest if we do not pay the bail right now. He is right here next to me crying, please hurry!"

Victim (Prepared): "I understand. Put my son on the phone for a second and have him say our family safe word. Otherwise, I am not taking another step and I will call the police myself."

Scammer: "Madam, there is no time, the line is bad, you must trust me...".

Victim: (Hangs up the phone immediately and contacts her son on his real number).

Regaining control of the situation in a matter of seconds is the true power of this tool. Sharing and pre-testing a safe word transforms the anxiety of the unexpected into a clear procedure, making every single family the first and most impenetrable bulwark of our community defence network.

This page intentionally left blank.

ABOUT EUNWA

Founded in 2014, **EUNWA (European Neighbourhood Watch Association)** aims to enable member nations to learn from one another, sharing best practices, operational protocols, and crime prevention strategies.

EUNWA acts as a bridge to facilitate mutual understanding and cooperation among National Neighbourhood Watch associations across Europe.

Our strategic objective is to establish a collaborative network with National Boards and security experts to provide a platform for exchange, respecting the autonomy of each country while building a safer, more connected Europe



EUNWA - European Neighbourhood Watch Association

www.eunwa.eu

head-office@eunwa.eu

Via Terraglio 64, 30174 Venice, Italy, CF 90194770278

