What is Scholar-Baiting? When the Watcher is Watched, and the Social Engineering Attacks on Scholars

[Accepted copy]

Cite as:

Lazarus, S. (2025). What is Scholar-Baiting? When the Watcher is Watched, and the Social Engineering Attacks on Scholars. *Journal of Contemporary Ethnography*, *0*(0). https://doi.org/10.1177/08912416251395087

Abstract

I write from the dual position of witness and analyst, using autoethnography to examine a scholar-targeted form of social engineering. The scammers baited me, mimicking academic language, citing published work, and deploying emotionally charged narratives to elicit trust and ethical engagement. From this dual role, I introduce two emergent constructs *("scholar-baiting" and "document staging"*) to describe how epistemic trust and narrative craft are exploited in academic-facing fraud. Scholar-baiting is a sub-genre of spear phishing, defined as a narrative-based form of deception. Document staging, on the other hand, is a dramaturgical tactic in which realistic artefacts are embedded to simulate plausibility and suppress suspicion. I further theorise emotional enmeshment and symbolic entrapment as emerging risks for scholars whose work centres on harm, justice, and vulnerability. I conclude by proposing a framework of defensive scholarship that repositions cyber hygiene as a form of epistemic reflexivity. This framing recognises that scholars' ethical commitments to engagement and vulnerability can be exploited as attack surfaces. By framing scholars as high-trust nodes in digital ecosystems, I highlight a threat to academic labour that remains under-theorised but urgently relevant.

Keywords: scholar-baiting, digital ethnography, document staging, social engineering, spear phishing, academic vulnerability

Introduction

> "Friends and family of the pregnant [British woman] found dead in the bath in a Ghanaian hotel today demanded justice as they paid tribute to their sweet angel" (Watts 2015)

There is a soft violence in academia that we rarely name. It is the cumulative toll of thinking, knowing, and being known (Daily 2024). Not all wounds are equal. Some are physical, a twisted ankle in a protest crowd, the ache of long hours hunched over a laptop. Others are spectral: the chest-tightening before hostile feedback, the sleeplessness no revision can fix. Still others emerge when the very ethics and visibility that shape our scholarship are retooled as instruments of deception. What does it mean to conduct ethical research when the researcher walks not on neutral ground, but across thin ice, mapped and booby-trapped by systems they were trained to navigate but never warned might turn against them? It is from this terrain of epistemic vulnerability and embodied risk that I write.

What happens when the Watcher is watched? This article draws on my positionality as both witness and investigator. I write this piece not simply as a researcher but as the researched. In this inquiry, I occupy both the position of observer and the position of the observed. The event that prompted this analysis exposes a form of deviance that, to my knowledge, has not been named or examined before. Scholars who research cybercriminals are themselves drawn into situations where their ethical commitments and investigative reflexes become points of manipulation. I call this *scholar-baiting*, a tactic that turns professional norms of care, curiosity, and responsibility into openings for exploitation. By situating this inquiry within ongoing debates in digital criminology and cybersecurity research (Bekkers et al. 2025; Birthriya et al. 2025; Chang and Chong 2022; Hall and Yarwood 2024; Blevins and Holt 2009; Holt and Copes 2010; Lazarus et al. 2025a), I argue that scholar-baiting signals a shift in terrain. The academic no longer only studies deception but becomes a surface upon which deception operates. I become the drum whose own rhythms are beaten in mimicry.

I recount a seldom-told tale from the field, one that resists abstraction and demands to be narrated from within. *Scholar-baiting* is not merely a theoretical concern or peripheral hazard. It is a lived, affective, and epistemic disturbance, an experience that unfolded through my own inbox, directly referencing my published work (Lazarus et al. 2025b) and attempting to exploit the ethical and intellectual commitments that anchor my scholarship. To ground this analysis, I briefly outline the incident that triggered this inquiry. Table 1 presents an overview of the April 2025 email, which directly referenced my published work and exemplifies the tactics I term scholar-baiting.

This combination (embedded high-resolution images, "empty" video attachments, and an expiring-files script) was no bot's work. On inspection, I recognised that it bore the hallmarks of deliberate human preparation, crafted to simulate plausibility and suppress suspicion. Table 1 provides the evidentiary basis for analysis and explains the rationale for selective redaction. The table also illustrates how a single message can reveal broader questions about scholarly exposure in digital spaces. It is precisely the scholarly impulse towards openness, sharing, citing, and responding that is mobilised in such entrapment attempts. We live in an era where academics, especially those researching deception, fraud, and manipulation, are encouraged to maintain a digital presence, engage the public, and promote open access to knowledge. Yet, this imperative towards visibility can blur the line between scholarly outreach and personal exposure. Research on digital ethnography highlights the specific risks posed by online environments, thereby complicating researchers' identities and positionality (Lavorgna and Sugiura 2022). While the cyber-surveillance of journalists and human rights defenders has been documented (Krain et al. 2024; Marczak and Scott-Railton 2016), the vulnerabilities of digital criminologists remain under-theorised. Those of us who study online fraud are no longer immune to it. Our research interests,

institutional affiliations, and presumed ethical commitments are increasingly becoming leverage points for engineered trust.

My inquiry advances a new neologism, scholar-baiting. Before defining it, I clarify why a new label is warranted and what it adds to existing vocabulary. The term does not yet appear in the cybercrime literature. However, relevant parallels remain. Research on targeted malware against journalists, NGO workers, and human rights defenders has shown that visibility and moral credibility create digital risk (Marczak and Scott-Railton 2016). Similarly, studies on deepfakes and synthetic identities reveal how narrative plausibility can override even trained scepticism (Chesney and Citron 2019). Existing label phishing, spear phishing, and generic social engineering prioritise credential theft, institutional lures, or broad behavioural manipulation. They do not capture attacks that mobilise a scholar's public work, moral vocabulary, and thematic commitments as the primary trust mechanism. What distinguishes scholar-baiting is not only its target but also its tactic. While it manipulates the scholarly disposition of the academic, it taps the scholarly impulse to engage. It does so, especially with marginalised voices, emotionally charged narratives, and under-reported harms. It is a scam[1] that masquerades as an inquiry.

Table 1. Incident Overview (Email dated 20 April 2025).

Theme	Details
Sender	"Dr Gail John"- drgailjohn@gmail.com (claimed to be a friend of the deceased, Charmain Speirs)
Cc	"Linda Speirs"- speirs.Linda@yahoo.co.uk (identified as the mother of the deceased, Charmain Speirs)
Date & Subject	April 2025 (Subject: "Ghana romance scams")
Reference	Directly cited one of my peer-reviewed articles (Lazarus et al. 2025b) on online romance fraud in Ghana
Core Bait	• Alleged that Charmain Speirs (deceased) was groomed and murdered by a Ghanaian romance fraudster. • Embedded thirteen high-resolution images (wedding photos, passport/registration documents, obituary) and two video file attachments (.MOV, both registering 0 bytes). • Stated the files would expire by May 20, 2025. • The email and its attachments, therefore, constitute a level of document staging inconsistent with automation and indicative of deliberate human preparation.
Tactics	• Narrative saturation (grief, injustice, corruption in Ghana) • Document staging (embedded visuals and empty video files rather than links) • Moral appeal ("since one of the authors of the article is doing a PhD on this subject. . . she might be interested in hearing the story") • Relational triangulation (friend + mother roles invoked to amplify credibility)
My Response	Replied cautiously without downloading any files and suggested offline verification. No reply followed (and there was no bounce-back), further

[1] I use "scam" and "fraud" ("scammer" and "fraudster") interchangeably (see Lazarus et al. 2025b). "Scam" reflects everyday and international usage (e.g. romance or crypto scams), while "fraud" captures the legal gravity of such acts. I prioritise linguistic responsibility over purism, using both terms to ensure accessibility without trivialising the offence.

Theme	Details
	supporting the interpretation of baiting as human-curated rather than automated.
Note	Supplementary files containing screenshots of the email (with author-identifying details removed), embedded images, and video file stubs have been submitted for peer review purposes only (see "Ethical Note on Visual Artefacts"). This decision also reflects logistical constraints, e.g., the journal's 40-page limit, as the artefacts would span 20 figures across 10 pages if included.

Scholar-baiting, as I define it, refers to a mode of social engineering in which scammers, fraudsters, or opportunistic actors fabricate credible, emotionally urgent outreach communications that cite, echo, or directly reference an academic's own research. Unlike conventional phishing, which targets organisational systems or financial gain, *scholar-baiting* operates on an epistemic and relational register. It seeks to entrap researchers by mirroring the narratives, values, and social harms they seek to expose.

One such attempt occurred in April 2025. I received an email from a Gmail account under the name "Dr Gail John." It referenced a peer-reviewed article I had authored on online fraud in Ghana (Lazarus et al. 2025b). The sender claimed to be a close friend of a deceased British woman allegedly murdered by a romance fraudster and requested contact with one of my co-authors. The email invoked grief, research relevance, and advocacy, and offered downloadable pieces of "evidence" set to expire by May 20, 2025 (as outlined in Table 1). Upon closer inspection, the message revealed multiple red flags. These red flags, particularly unverifiable timelines, emotionally coercive appeals, pressure to act before a deadline, and a mix of real and invented names, are hallmarks of advanced phishing ecologies repurposed to exploit scholarly vulnerability. This article conceptualises *scholar-baiting* not as an isolated incident but as an emerging threat within the broader digital ecology of fraud. I ask the following questions:

- How are cybercriminals adapting to the increasing digital visibility of researchers?
- What rhetorical and narrative tactics are used to manipulate scholars' ethical instincts, affective commitments, and disciplinary trust?

I approach these questions through a reflexive, interpretive, and narrative mode, grounded in my own entanglement with the phenomenon. Rather than treat this encounter as anecdotal, I frame it as data, analysing it through a lens attuned to symbolic violence, positionality, and epistemic precarity. The autoethnographic form enables me to trace the emotional labour, ethical friction, and interpretive dilemmas that accompany such entrapment attempts. It allows me to investigate the conditions under which the field observes, and becomes observed. In a moment when the boundaries between research subject and scholarly self are increasingly unstable, I offer both a warning and an invitation. I warn of emerging digital vulnerabilities, and I invite a rethinking of how ethnographic knowledge is produced, contested, and sometimes weaponised. The rest of the article unfolds in four main parts. Sections "Method and Approach: Autoethnographic Inquiry into Scholar-Baiting" and "Ethical Note on Visual Artefacts" outline the methodological and ethical positioning of the autoethnographic approach. Sections "Situating the Email of Scholar-Baiting" through "The Ghost of Your Own Research" present the case and analysis: the triggering incident, its emotional and narrative mechanics, and the theorisation of scholar-baiting. Sections "The Digital Scholar as Target: Visibility, Vulnerability, and Vigilance" to "Conceptual Contribution and Implications" consolidate the conceptual contributions, develop the typology, and situate the phenomenon in relation to adjacent digital threats. In the *Conclusion* (section "Conclusion: Vigilance as Epistemic Integrity"), I close with reflections on vigilance as an ethical reflex and offer broader implications for scholars and institutions.

Method and Approach: Autoethnographic Inquiry into Scholar-Baiting

Before developing the conceptual scaffolding, I set out my method and positionality. As both the narrator and the object of inquiry, I foreground subjectivity as a method. I use an autoethnography to investigate a hitherto undocumented phenomenon: the targeted harassment and manipulation of cybercrime researchers by online fraudsters, a process I conceptualise as *scholar-baiting*. Given the rarity of this dataset globally and the lack of existing empirical engagement with this form of epistemic vulnerability, autoethnography is both methodologically and ethically apt. It offers a way to analyse the entanglement of personal experience, institutional precarity, and digital power asymmetries through the critical lens of reflexive self-inquiry.

In keeping with established autoethnographic traditions, like many scholars (Anderson 2006; Corkhill (Pseudonym) and Charman 2024; Denshire and Lee 2013; Kingsbury 2022; Lazarus 2024; O'Hagan 2023; Ortiz-Vilarelle 2021b, 2021a; Stanley 2023; Yavuz 2024), I do not aim for statistically representative sampling. Instead, I engage in what Ellis et al. (2011, 279) called "evocative narrative," wherein the researcher uses autobiographical material to produce analytical insights. My goal is twofold: (1) to theorise *scholar-baiting* as a structurally overlooked form of digital threat and (2) to highlight how such threats are experienced through intersecting axes of race, visibility, and scholarly focus.

The study draws from fieldnotes, emails, social media screenshots, personal reflections, and digital artefacts documented during and after attempts by online actors to phish, impersonate, or manipulate me, often using scripts that mimicked my field of expertise. This dataset is exceptional in at least three ways: (1) It documents a researcher becoming the target of the same digital strategies they study, reversing conventional ethnographic flows of power. (2) It captures real-time manipulations from actors embedded in the online fraud economy, allowing for an experiential account of social engineering in the wild from the vantage point of an academic researcher. (3) It highlights how academic visibility can expose scholars to unexpected digital harms.

Rather than anonymising or flattening the data, I use narrative storytelling to preserve the emotional texture, ethical uncertainty, and contextual intricacies that more positivist approaches would mute. This choice reflects a core principle of autoethnography, seeing subjectivity not as bias but as a lens for analysis (Ellis et al. 2011; Ben-Lulu 2024; Lazarus 2021; Ortiz-Vilarelle 2021a; Yavuz 2024). However, with all autoethnographic research, I recognise that my singular positionality shaped and limits my piece. I do not claim to speak for all researchers, nor would I want to. What I offer instead is interpretive depth and analytic richness that are not easily captured by aggregate methods. To make this methodological grounding explicit, Table 2 summarises characteristics of autoethnography.

This approach makes three specific contributions: (1) Conceptually, it introduces *scholar-baiting* as an emergent sub-field of digital harm and calls for its inclusion in debates on academic security, digital ethnography, and the ethics of visibility. (2) Empirically, it provides rare data points drawn from lived experience, offering a textured view into how cybercrime researchers can be both observers and targets. (3) Epistemologically, it challenges the assumption that only *subjects* are at risk in cyber-ethnography and raises urgent questions about the inverse gaze, when the watcher is watched.

Ethical Note on Visual Artefacts

In accordance with the Committee on Publication Ethics (COPE) guidelines, I have chosen not to reproduce the images attached to the original scam email. These visuals, purporting to depict the deceased, legal documents, and family scenes, were instrumental to the manipulation, but their inclusion would risk several ethical breaches. First, presenting potentially fabricated

materials could unintentionally legitimise deception, especially when their authenticity cannot be independently verified. Second, their circulation may indirectly retraumatise individuals linked to the real "Mrs Speirs," whose identity appears to have been appropriated as narrative bait. Third, COPE advises researchers to avoid harm to third parties, particularly in cases involving misinformation or impersonation. In light of these concerns, I prioritise a textual analysis of the scam's rhetorical and narrative strategies over the visual reproduction of images I received. This decision reflects a deliberate commitment to epistemic integrity, emotional care, and ethical responsibility in the study of digital manipulation. With the methodological stance established, I turn to the incident that serves as the anchor for this analysis.

Table 2. Characteristics of Autoethnography with Concise Descriptions.

Feature	Brief description
Personal experience	The researcher is both the subject and interpreter of lived experience
Discomfort	Emotional and ethical unease arises from occupying dual roles
Narrative style	Prioritises storytelling, introspection, and narrative coherence
Cultural context	Anchors personal accounts within broader social and symbolic systems
Subjectivity	Values positionality and reflexivity as tools of knowledge production
Emotion and reflection	Emotions are not marginal but essential to understanding impact
Qualitative format	Uses essays, vignettes, and personal narratives as research outputs

Source: modified from Lazarus (2024: 608).

Situating the Email of Scholar-Baiting

To guide this inquiry, Section "Situating the Email of Scholar-Baiting" introduces the email and develops the conceptual framing, mechanics, and tactics that emerge from it. Section "Naming Scholar-Baiting: When the Bait Is Theory and the Target a Scholar" lays the theoretical groundwork for scholar-baiting. Section "Defining Scholar-Baiting: A Typology of Epistemic Intrusion" defines its core features. Section "Illustrative Case Framing" analyses the triggering message as a situated case, and Section "What is Document Staging?" introduces document staging as a distinct tactic of deception. Section "Narrative Design of Scholar-Baiting Emails" focuses on the narrative design of scholar-baiting emails, showing how affect, evidence, and credibility are structured to pull scholars into compromised interpretation.

I speak from within the phenomenon, not outside it. While many academics may be familiar with scam emails offering titles such as "*Best Researcher Award*," originating from dubious addresses, scholar-baiting operates on a fundamentally different register. The "Best Researcher Award" scheme targets authors of recently published papers with flattering lines such as: "*Your recent publication has been provisionally selected for the Best Researcher Award*." Recipients are then asked to pay a few hundred dollars for a certificate and carved plaque, objects devoid of academic legitimacy. The scammer profits, while the academic is left with trinkets and an empty sense of honour. Scholar-baiting, by contrast, exploits not vanity but vulnerability. It crafts emotionally resonant, intellectually tailored scripts that echo a scholar's identity, idiom, thematic focus, ethical stance, and sense of moral obligation.

These three scams share a reliance on trust. However, each draws on a distinctive register as shown in Figure 1. (1) The "Best Researcher Award" scam depends on a thin, transactional

trust in institutional symbols like logos, certificates, plaques, and formal language. (2) Romance scams build trust through emotional intimacy and the promise of love, care, or imagined futures (Cross and Holt, 2023). These fraudsters use linguistic cues to construct intimacy and credibility (Carter 2024). Studies of West African cases show how offenders craft persuasive personas using grandiose narratives, royal or aristocratic claims, or urgent tales of financial hardship (Abubakari 2024, 2025; Soares and Lazarus 2024; Soares et al. 2025; Yushawu and Jaishankar 2025). Broader scholarship on romance scams has examined their psychological mechanisms, narrative strategies, and affective manipulations (Bilz et al. 2023; Lazarus et al. 2023a; Schokkenbroek and Snaphaan 2025). (3) Scholar-baiting forges trust through intellectual kinship, shared language, ethical commitments, and visions of justice that render the exchange authentic.

It is within this expanding ecosystem that my own experience unfolded. Over two decades of systematic reviews have shown that scholarly attention has largely centred on the primary victims of online scams (Bilz et al. 2023; Lazarus et al. 2023a). Yet, a quieter evolution has been unfolding beneath the radar in the form of post-victim scam adaptations (Abubakari 2024, 2025). In my own empirical research, including interviews with a convicted high-profile cybercriminal (Lazarus 2025), active online fraudsters (Button et al. 2025a, 2025b), and analyses of conviction files of offenders (Lazarus et al. 2025a), I have encountered cases in which fraudsters take strategic actions typical of adaptive enterprises. They revise, recycle, and redirect narratives, much like actors adjusting to shifting moral and situational constraints. Emerging reports from the banking sector also document the repurposing of grieving narratives, now redirected towards secondary audiences such as family members (Barclays 2025; Zempler 2025). This tactic, sometimes referred to as *grief phishing*, or bereavement scamming, exploits moral urgency and weaponises the politics of care (Barclays 2025; Zempler 2025).

In April 2025, I received an email. It was not seeking money or romantic attention. It did not beg, seduce, or flatter. Instead, it referenced a peer-reviewed article I had co-authored. The sender, under the name "Dr Gail John," praised the work's theoretical contribution and offered what they framed as "evidence" related to a fabricated case involving a deceased British woman named Charmain Speirs. The tone was urgent. The emotional register was high. And the attachments were set to expire by a specific date ("20 May 2025"), adding pressure cloaked in procedural courtesy:

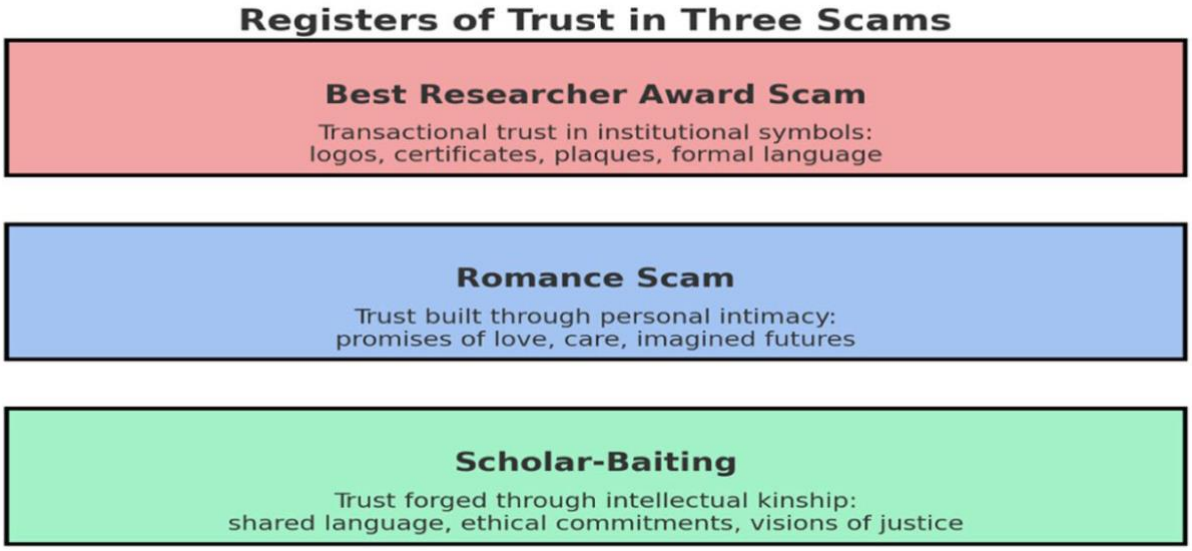

Figure 1. The three registers of trust.

> A lot of the characteristics you outlined in your paper are exact. . . He love-bombed her, telling her that he was from a royal family. . . They married. . . and she was dead within six months. —Excerpt from email (lightly redacted)

The message drew directly from the very themes I had written about, love-bombing, deception, ritualised personas, and folded them into a new narrative in which I was positioned not as an analyst, but as an ethical respondent. This was not romance fraud. It was scholar-baiting: a targeted, relational manipulation designed to lure researchers into engagement by mimicking the affective, intellectual, and thematic patterns of their own scholarship. Where spear phishing targets financial systems or administrative authority, scholar-baiting weaponises the moral architecture of academia itself. It exploits the very things we are trained to value, such as relevance, citation, empathy, reflexivity, and the impulse to *listen*. As a scholar working in deception studies, I was being deceived not in spite of my expertise, but *because of it*.

This case forced me to rethink my assumptions about visibility and trust. I had always imagined public scholarship as a contribution, a way of opening knowledge to broader publics. But this encounter revealed that open access can also serve as an open invitation. Citation becomes bait. Ethical language becomes a vector. Visibility becomes vulnerability. As justified earlier, the term scholar-baiting names a pattern distinct from adjacent threats. In what follows, I develop a conceptual framework, outline its mechanics, and situate it alongside related phenomena. What distinguishes scholar-baiting is not just its target, but its tactic. It influences academics' intellectual orientation. It taps into the scholarly tendency to engage, especially with marginalised voices, emotional narratives, or underreported harms. It is a scam masquerading as an inquiry. In what follows, I offer a conceptual framework for understanding this new phenomenon. I define its mechanics, differentiate it from adjacent digital threats, and explore how it reflects a deeper inversion in which the researcher becomes the field and knowing itself becomes the point of exploitation. This context sets the stage for the theoretical framing and naming of the pattern I encountered.

Naming Scholar-Baiting: When the Bait Is Theory and the Target a Scholar

The events described are simultaneously my data and my life. When I first received the email, I didn't have a name for what it was. I knew it wasn't a romance scam, at least not in the conventional sense. It also wasn't spear phishing, which typically targets officials or institutions. But it felt close, methodical, emotionally disarming, and epistemically familiar. What made it all the more unsettling was its invocation of a real tragedy I remembered vividly: the death of Charmain Speirs, a British woman who died in Ghana under contested circumstances. During my doctoral years, I followed the story in the media. I read her mother's public appeals for answers, and I remember feeling a quiet sorrow at the cruelty of it all. A friend of the deceased, I recall, had set up a crowdfunding page to bring her body back to Scotland for burial. The language of that campaign stayed with me:

> "I am raising funds on behalf of the family of my dear friend Charmain Speirs whose life was cruelly taken whilst visiting Ghana. She was three months pregnant. . . Any remaining funds will go into a trust for her son."

So, when the email arrived, allegedly from a "Dr Gail John," referencing my own co-authored article on romance scams in Ghana and CC'ing a "Linda Speirs," I couldn't quite detach. Part of me knew it was a scam. The indicators were there. Unverifiable claims, urgency, and downloadable attachments, as shown in Figure 2. But another part of me, the part shaped by years of studying deception and harm, could not bear the possibility, however remote, that I might be ignoring someone real. The name "Mrs Speirs" did exist. That much was verifiable. What remained uncertain was whether the person contacting me had any genuine connection to

her story or was exploiting it. I copied both email addresses and replied cautiously, signalling a willingness to engage further if they were indeed based in the United Kingdom, where I also live. Perhaps a simple chat over coffee might offer clarity, a flicker of light where doubt and shadow linger.

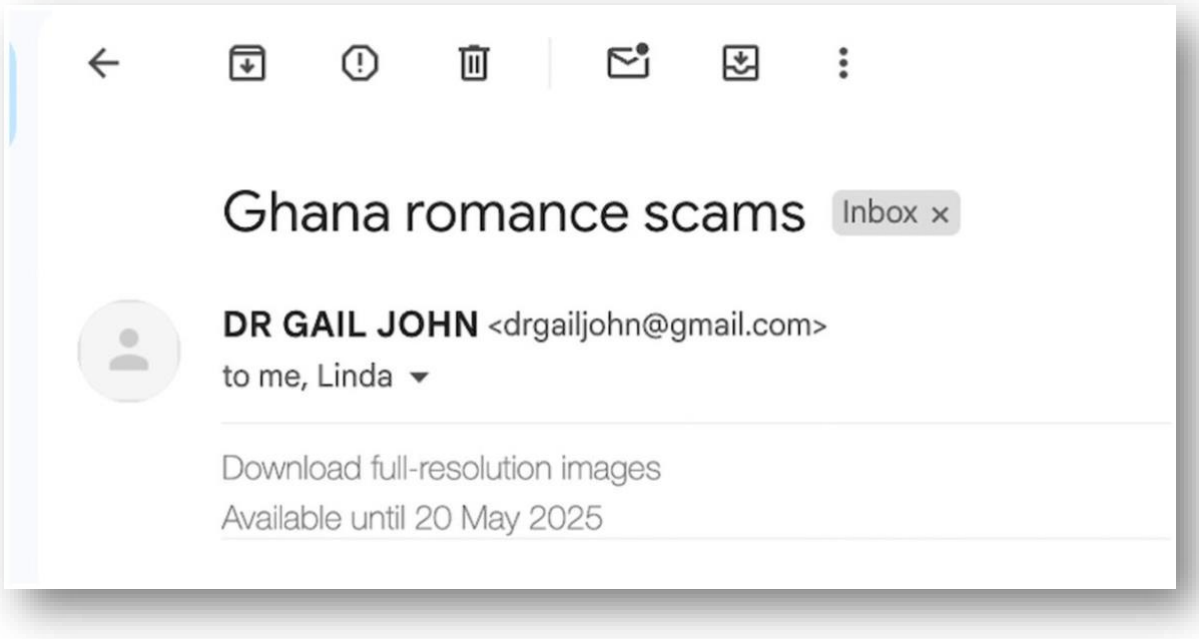

Figure 2. Example of expiring attachments used to induce urgency.

After all, I did not need to download anything, compromised or not, when, if genuine, they could post the documents directly to my university address, which they clearly knew, having cited the very publication in question. The possibility that I might be dismissing a real plea for help, from Mrs Speirs herself, whose wailing and pain I still recall from the news, was, I admit, a vulnerability. But I chose to navigate it, not through trust, but through precaution. Just in case the real Mrs Speirs had indeed been wronged, and her daughter's friend was reaching out in earnest. But as my research expertise expected, before the fact! No reply from the scammers. No bounce. No further attempt. Just silence. *When the trickster's trap is exposed, his laughter falters, and silence finishes the tale.*[2] The silence was not incidental. It marked the collapse of a rehearsed deception once its anonymity and narrative scaffolding were simultaneously challenged. In my reply, I exercised *adversarial control* (a deliberate countermeasure through which the target of social engineering reclaims the power dynamic). I used a Virtual Private Network (VPN) for all related correspondence, ensuring that my location and metadata remained obscured. I then proposed a face-to-face meeting with *Mrs Speirs* and *Dr John* at specific venues in the United Kingdom, within the very locality that anchored their real-world identities. The proposal itself functioned as a *verification manoeuvre*, grounded in the geographies the scammer had appropriated. Had the real *Mrs Speirs* contacted me, she would likely have welcomed such a meeting, and having seen photographs of her in the media, I would have recognised her. By invoking an embodied social context, anchored in verifiable people and places, I forced the exchange into tangible space, where anonymity collapses. This strategic shift neutralised the attacker's digital leverage by eliminating all technical vectors of compromise. There were no links to click, attachments to open, or credentials to exchange. *Even the clever chameleon cannot hide from the sun*. Once the interaction was forced into verifiable reality, the performance of deceit disintegrated. The baited

[2] This aphorism is original and stylistically inspired by the idiomatic texture of African proverbial wisdom.

narrative could not survive embodied accountability. In effect, the response dismantled not only the mask of deception but also the architecture that sustained it.

Operational outcome, in the plainest sense: I sent a reply; I received no response; I did not open or download any attachments. That silence confirmed my instinct. And yet, it also deepened my conviction that something new was taking shape. Only after sitting with the discomfort, re-reading the message through the lens of my own work, and tracing its structure back to the very concepts I had theorised, did I begin to name it: *scholar-baiting*. The novelty lies in naming scholar-baiting and document staging as emergent tactics that target academics as high-trust nodes, and in analysing their affective and epistemic effects through lived experience.

Defining Scholar-Baiting: A Typology of Epistemic Intrusion

Having defined scholar-baiting in the Introduction, I focus on what I experienced. As a Kiswahili saying has it, "*Kupotea njia ndiko kujua njia*," meaning to lose the way is to know the way. I write from what I encountered to make sense of it. I use scholar-baiting to name the pattern I faced. I define scholar-baiting as a targeted, emotionally calibrated form of social engineering that exploits the thematic commitments and public visibility of academics, particularly those researching trauma, fraud, cybercrime, or injustice. These deceptive messages do not aim to seduce, threaten, or sell. Instead, they mirror. They echo the scholar's tone and diction, cite full reference details of their publications, highlight career-stage cues, such as identifying a co-author as a PhD student ("*since one of the authors of the article is doing a PhD on the topic. . .*"), and inhabit the moral vocabulary of justice, loss, and care. The contact is unsolicited but precisely crafted to pull the researcher into an epistemic and emotional entanglement under the guise of testimony, collaboration, or shared concern. Unlike generic phishing, which casts a wide net, or spear phishing, which targets bureaucratic access, scholar-baiting manipulates symbolic authority. It transforms the legitimacy of scholarly work into an attack surface. It builds trust through thematic mimicry and intellectual flattery. To clarify these dynamics, Table 3 introduces a reflexive typology of the structural mechanisms of scholar-baiting.

These mechanisms do not rely on technical prowess. They work because they exploit a deeper vulnerability, particularly, our intellectual reflexes, our openness to difficult truths, and our willingness to listen. Scholar-baiting is, in this sense, not merely a digital threat but an epistemic ambush, one that invades the moral economy of scholarship and retools its principles for deception. To situate scholar-baiting in relation to neighbouring concepts, Table 4 compares it with adjacent digital threats.

Though the term is new, its contours echo familiar concerns. Research on attacks against journalists and human rights defenders has shown how visibility and narrative alignment increase one's exposure to digital intrusion (Marczak and Scott-Railton 2016). Similarly, studies of deepfakes and digital extortion demonstrate how emotional believability outpaces technical detection (Chesney and Citron 2019). But scholar-baiting is distinct in how it weaponises the care labour and interpretive vulnerability that define engaged academic work.

This tactic is not aimed at what the scholar exposes, but at what they embody, their values, their intellectual investments, and their ethical posture. It mimics our moral resonance, not to honour it, but to turn it against us. Scholar-baiting is therefore best understood as a sub-genre of spear phishing, one that operates within the moral economy of academia, utilising affective resonance and intellectual mimicry rather than financial incentives or institutional lures. Having outlined the mechanics, I turn to the specific message that operationalised them.

Illustrative Case Framing

The boundary between researcher and researched collapses in this account. The scam email that prompted this article was not merely a message: it was a precision-crafted artefact of targeted

manipulation. Sent by a person identifying as "Dr Gail John," it referenced a peer-reviewed article I had co-authored on romance fraud in Ghana (Lazarus et al. 2025b) and praised its theoretical insight. But beyond flattery, the email staged a grief-saturated narrative: the murder of a pregnant British woman in Ghana, alleged institutional cover-ups, and a moral appeal to truth-seeking scholarship. It carried the tone of a whistleblower, the intimacy of a bereaved family member, and the urgency of someone with no one else to turn to. It did not just ask me to act. It made inaction feel like complicity.

This is what I have come to understand as *narrative saturation as bait*: a social engineering tactic in which dense, emotionally charged storytelling is used to suppress suspicion and prompt immediate, affective engagement. The emotional precision of this scam email was sharpened by its invocation of verifiable tragedy. Charmain Speirs, also known by her married name, Charmain Adusah, was a forty-one-year-old British woman who was three months pregnant when her body was discovered by hotel staff in Ghana. She had lived in Rayleigh, Essex, spent part of her life in Scotland, and had worked for the NHS during her years in Swansea. The scammer's ability to graft this real-life death onto a fictional narrative illustrates a chilling tactic: anchoring deception in genuine loss. This is not deception through fabrication alone; it is deception through appropriation.

Table 3. Structure of Scholar-Baiting: A Reflexive Typology.

Characteristic	Description
Targeted referencing	Cites the scholar's actual publications, talks, or interviews to establish credibility and a thematic bridge.
Emotive or moral appeal	Draws on narratives of injustice, loss, or victimisation that align with the scholar's values and field of study.
Attachment or link bait	Offers "evidence," "files," or "testimonies" for download—often with an expiry date or urgency hook.
False authority impersonation	Poses as a survivor, whistleblower, NGO actor, or bereaved relative, figures with moral gravity in the scholar's research domain.
Urgency and exclusivity	Frames the scholar as uniquely positioned to respond, using time pressure and appeal to ethical duty.
Narrative triangulation	References additional names, organisations, or CC'd recipients to create a false web of authenticity.

Table 4. Situating Scholar-Baiting Among Adjacent Threats.

Term	Focus	Primary Target	Key Distinction
Phishing	Generic credential theft	General public	Impersonal; often financially motivated
Spear phishing	Institutional compromise	Executives, officials	Highly targeted; the goal is system access or surveillance
Social engineering	Behavioural manipulation for digital intrusion	Any user	Broad technique; includes pretexting, baiting, and more
Scholar-baiting	Thematic, moral, and intellectual manipulation	Public-facing academics	Leverages the scholar's *own* work, ethics, and visibility to fabricate a credible scenario

A poignant example comes from Charmain's mother, Mrs Linda Speirs, who posted publicly on Facebook: "*My lovely daughter, in memory to your son we will get justice for you Charmain, love mammy.*" She also shared an ultrasound image, captioned: "*Thinking of all our sweet angels who are spending Easter in Heaven*" (Watts 2015). These maternal utterances, charged with grief and love, were not merely background context. By exploiting real biographical data, the scammer collapsed the boundary between empathy and exposure, overwhelming critical reflexes through emotional saturation. The inclusion of pregnancy, motherhood, and a cross-continental tragedy was not incidental. It was instrumental. It was not ornamental. It was strategic. It was engineered to short-circuit scepticism and activate the ethical posture of scholars attuned to harm, injustice, and marginal loss.

The emotional force of the scam email was not merely rooted in historical tragedy. It was sharpened by *contemporaneity*. On May 5, 2025, just fifteen days after I received the message, a major national newspaper ran a feature headlined: "*Mum of pregnant Scot found dead in Ghana hotel bath demands fresh murder probe*" (Hind 2025). The article detailed the unresolved death of Charmain Speirs, who died under suspicious circumstances in a hotel in Koforidua, Ghana, in 2015. Her husband, a Christian preacher, had been arrested for murder, though the case later collapsed. On the tenth anniversary of her death, her mother, Mrs Linda Speirs, called for a new investigation, expressing that "Charmain had no voice in Ghana when this happened." Figure 3 shows Linda Speirs examining paperwork related to the investigation into her daughter's death. This effort was covered in the *Daily Record* (Hind 2025), which published the accompanying image.

The article included quotes, biographical facts, and images that eerily mirrored the content of the scam email I received shortly afterwards. This overlap was not accidental. It was strategic, emotional engineering executed with uncanny narrative timing. By piggybacking on a fresh media cycle, the scammer magnified plausibility and collapsed the space between mourning and manipulation. The emotional saturation of the email thus rested not only on the appropriation of real loss, but on the manipulation of real time.

It was designed to provoke a kind of moral urgency I had spent years studying, but now felt in my gut. The scammer wrote in my register, citing injustice, evoking memory, and positioning the outreach as part of a shared intellectual and ethical struggle. It mirrored my work in both tone and urgency. But the manipulation extended beyond language. The email contained no clickable links or malware-laced attachments. Instead, it embedded thirteen high-resolution images directly into the body of the message, viewable without activation. These included supposed wedding photographs, UK business registration documents, a scanned passport, and a fabricated obituary. Their quality and variety bypassed the technical red flags associated with phishing. The message also included a file-expiry notice and a suggestion of time-sensitive disclosure, adding procedural realism to the emotional urgency.

Figure 3. Linda Speirs reviewing the investigation paperwork.
Source: Image reproduced with permission from the Daily Record (Hind 2025).

What I encountered, in retrospect, was a form of *document staging* (i.e., the deliberate crafting and presentation of emotionally resonant yet fraudulent materials to simulate credibility and provoke scholarly engagement). These were not generic visuals; they were contextually loaded artefacts that mimicked the evidentiary aesthetics of trauma journalism and ethnographic fieldwork. This concept, document staging, becomes critical for understanding how scams now exploit not only emotional empathy but also methodological trust. As researchers, we are trained to recognise depth, contextual detail, and narrative coherence as signs of authenticity. Here, those same cues were weaponised. The following section provides a closer forensic examination of the email itself, its narrative architectural fabric, rhetorical organisation, and psychological triggers.

What is Document Staging?

Document staging is defined as a dramaturgical deception tactic within scholar-baiting scams, characterised by the presentation of emotionally potent, realistic artefacts at the outset of engagement, to suppress suspicion and engineer trust through evidentiary aesthetics. It refers to a narrative-technical strategy within social engineering whereby scammers embed or present realistic, emotionally potent artefacts, such as ID cards, certificates, chat screenshots, or family photographs, at the outset of a deceptive interaction. These artefacts are frontloaded not as proof requests but as trust scaffolding. They serve to establish narrative coherence, simulate transparency, and suppress scrutiny before any explicit request or escalation occurs. Document staging functions as a dramaturgical tactic: not a cold ask, but an invitation into a story. Common

elements include: (1) Embedded visual artefacts that circumvent cybersecurity defences by avoiding links or attachments; (2) urgency cues, such as expiry language or impending danger, to prompt engagement; and (3) progressive trust-building, where benign artefacts establish realism that legitimises subsequent manipulative steps.

In scholar-baiting scenarios, this technique turns the academic's strengths, pattern recognition, care-labour, and thematic attentiveness into vulnerabilities. The artefacts echo familiar tropes from our research, rendering us more receptive not despite our expertise, but *because of it*. The table elucidates why existing terms discussed in existing scholarship (Abdullah and Mohd 2019; Birthriya et al. 2025) are inadequate in scholar-baiting contexts. These limitations are demonstrated in Table 5. It outlines why existing terms from the literature fall short in capturing the specificity of scholar-baiting contexts. Document staging, therefore, is a sub-genre of spear phishing. Hence, I distinguish document staging from adjacent terms.

By contrast, document staging, as introduced here, captures the hybrid logic of artefact-driven deception. It is neither purely emotional nor purely technical. It is architecturally designed to build a compelling, immersive story world that engineers trust through evidentiary aesthetics. In what follows, I offer a forensic reading of the email, tracing its narrative arcs, affective pivots, and semiotic textures. This close analysis reveals not only how the scammer constructed a story to ensnare a scholar, but how the contours of public knowledge production have become vulnerable surfaces of digital deception.

Narrative Design of Scholar-Baiting Emails

My role in this inquiry is both experiential and analytical. Scholar-baiting, as I define it, is not just a novel extension of spear phishing into academic domains; it is also an epistemic performance. Thus, I turn to the artefact that triggered this inquiry: an unsolicited email I received in April 2025. Sent by an alleged "Dr Gail John," the message referenced my published work on romance fraudsters in Ghana (Lazarus et al. 2025b). But this was no generic appeal. It was a tightly wound narrative, brimming with grief, corruption, and spiritual deception. It offered me a role, implicitly ethical, explicitly intellectual, in what it framed as a quest for justice.

Table 5. Why Existing Terms Fall Short in Scholar-Baiting Contexts.

Term	Definition	Limitations
Pretexting	Use of fabricated identity to gain trust	Focuses on persona, not the artefactual architecture of deception
Credential phishing	Deceptive links or forms to harvest data	Lacks narrative immersion or thematic alignment
Bait documents	Malware-infested files used in penetration testing	Primarily technical; not concerned with emotional manipulation
Social proof tactics	Use of fake endorsements/testimonials to enhance credibility	Not centred on documentary artefacts or epistemic mimicry

This was not just a scam. It was a dramaturgy of deceit. The message was carefully composed to exploit moral vocabularies, researcher affect, and thematic familiarity. It functioned as what I call narrative social engineering: the construction of a persuasive message that blurs the

lines between research subject, moral cause, and digital trap. So, I write from within the experience I seek to analyse. What follows is a close ethnographic analysis of this artefact.

The scam message followed a layered narrative arc. While it mimicked the basic stages of a phishing attempt, it moved with the precision of an ethnographic method, beginning with thematic flattery and ending in epistemic entrapment (as outlined in the table). Table 6 summarises the staged phases of the email and the specific functions each phase performs.

What distinguishes this email from ordinary phishing is not its content alone but its choreography. It knew how to echo. My own experiences constitute both the starting point and the subject matter of this email, which performed the tropes I have studied, cited, and critiqued, drawing me not only into contact but also into complicity. The email was designed to position me as a potential witness, ally, and co-investigator. Its genius was its mirroring research.

Table 6. Narrative Structure of the Scholar-Baiting Email.

Phase	Content Summary	Function
Opening praise	"I read your paper with great interest. . ."	Establishes legitimacy; flatters the scholar's intellectual stance
Personal testimony	Recounts the murder of a British woman who was allegedly groomed and killed in Ghana	Evokes empathy; resonates with the scholar's area of study
Narrative expansion	Includes the story of marriage, fake documents, spiritual abuse, and surveillance	Builds density; deepens emotional commitment and plausibility
Institutional anchoring	Names religious leaders (e.g. Colin Urquhart), churches, and registries	Simulates verifiability and insider knowledge
Call to action	Offers further evidence; invites academic engagement	Exploits the researcher's moral and investigative reflexes
Urgency tactic	"Download before 20 May 2025"	Enforces immediacy; suppresses deliberation and digital caution

Psychological Levers and Thematic Lures

The scam activated a precise set of psychological triggers, each selected to disarm, engage, and recruit. (1) Empathy: The protagonist was not a stranger, but a grieving mother. The victim was not anonymous, but named, pregnant, British, and allegedly murdered. The tone: intimate and aching. (2) Authority: Names of preachers, churches, and registries created the illusion of traceability. There were no outlandish claims, only plausibly unverifiable ones. (3) Curiosity: "We have gathered documentation" was not a threat; it was bait. The suggestion of evidence was an invitation to verify, to investigate, and to do the work. (4) Urgency: The downloadable content was described as time-sensitive. "Expires 20 May 2025." This is a pressured reflex, not a reflection. (5) Moral Flattery: The message affirmed that I was "uniquely positioned" to understand. It did not ask for help; it assigned it.

In short, the email did not just manipulate. It mimicked my research ethics. It colonised my intellectual instincts. What makes scholar-baiting distinctive is not only the psychological precision but its mimicry of the ethical reflexes that underpin academic practice (responsiveness, empathy, and epistemic responsibility). It was both phishing and ethnography, deception and fieldnotes. These manipulations align with established psychological levers in the persuasion and social engineering literature (Albladi and Weir 2018; Ferreira et al. 2015). However, my experience does more than confirm those frameworks. It extends them by demonstrating how scholarly

ethics themselves can become attack surfaces. They were not random; they were precisely staged. The table below dissects the email's composite structure, illustrating how each element was engineered to perform a role in the broader choreography of deception. I map the email's fabric piece by piece, tracing how it retools academic cues into social engineering tactics. Table 7 details the email's architecture by pairing each element with its role in social engineering.

The email was instructive. It sought to deceive by fostering intimacy rather than obscurity. Biblically, it implies an attempt to ensnare even the "elect."[3] The sender did not hide behind anonymity; they constructed an identity. They did not bypass the scholar's gatekeeping reflex. They entered through the front door, bearing citations. Surely, this case reveals a new tactic within the repertoire of digital deception. The deceptive strategy exploits not only the weaknesses of systems but also the virtues of academic practice. Scholar-baiting, as executed, is not merely about technical access or financial theft. It is about thematic seduction. It repurposes the very tools, visibility, curiosity, and openness that define scholarly engagement and uses them to stage a trap. Now, I turn to a granular analysis of the embedded artefacts (the images, documents, and metadata) that constituted what I earlier called *document staging*. I explore how deception resides within the very syntax of scholarship.

The Affective Architecture of Trust

The email did not simply seek to deceive. It sought to conscript. Unlike conventional phishing, which often impersonates banks or bureaucracies, this message impersonated solidarity. It posed not as an outsider hacking the system but as an insider mirroring it, drawing from the idioms of trauma advocacy, postcolonial justice, and digital activism. The sender spoke as if they knew the field and knew me.

Table 7. Structure of the Scholar-Baiting Email.

Element	Excerpt or Feature	Function in Social Engineering
Research citation	"I read your paper with great interest. . ."	Anchors the scam in scholarly credibility; disarms through flattery
Victim narrative	"Charmain Speirs. . . was dead within six months of marriage."	Elicits empathy; aligns with themes of romance fraud and structural violence
Moral call to action	"She deserves justice. . . I believe your co-author might want to hear her story."	Triggers ethical obligation; invokes scholarly care-labour
False authority	"He was the son of a bishop. . . he attended a course with Colin Urquhart (deceased)."	Simulates inside knowledge; manufactures legitimacy
Attachment bait	"Download full-resolution images. . . available until 20 May 2025."	Encourages unsafe behaviour via urgency; primes for malware
Triangulation	CC'd "Linda Speirs (mother)"	Adds emotional texture and the illusion of a relational network

[3] *Elect* is used here as a theological term. "For there shall arise false Christs, and false prophets, and shall shew great signs and wonders; insomuch that, if it were possible, they shall deceive the very elect" (Matthew 24:24, KJV).

They invoked language I had used in my own writing. They summoned harms I cared about. They aligned themselves with the values that had shaped my scholarship. In mimicking scholarly concern, the scam activated what I call the ethics of attentiveness. These include the obligation to read with care, to respond with humility, and to engage narratives of harm as if they mattered. What emerged was not a generic scam but a bespoke narrative trap, an affective architecture engineered to co-opt the very ethical and intellectual circuits I had spent years constructing. This, I argue, signals a shift in the emotional economy of digital fraud, from financial seduction to narrative entrapment. The scammer did not ask for money. They asked for recognition, engagement, and care. A click, a reply, a download. A reading of grief, a parsing of loss.

The affective precision of the message, its careful appeal to moral, emotional, and epistemic cues, demanded more than digital caution. It required interpretive labour. In what follows, I unpack three interlocking modes of manipulation embedded in this single communication, each targeting the scholar not as a user, but as a moral agent, an empathetic narrator, and a seeker of knowledge. I now step back to synthesise the pattern and its implications.

Moral Responsibility: "Help Expose This Injustice"

The scam's emotional core was a story of unredressed harm: a murdered British woman, a fraudulent marriage, spiritual coercion, and a compromised legal system in Ghana. These were not abstract themes; they were vivid, specific, and narratively urgent. The message was steeped in the moral grammar of human rights and activist scholarship. It did not simply describe injustice. It assigned responsibility. Phrases like "*she deserves justice*" and "*perhaps your co-author might want to hear this story*" were not invitations. They were obligations, ethically coded in the language of advocacy. The appeal was not transactional; it was testimonial. It positioned me not as an academic but as a vessel for moral witnessing. This tactic weaponised one of the central features of critical scholarship. It drew on the belief that knowledge production is a form of care. Non-response, in this frame, risked feeling like complicity. To ignore the message would not merely be to avoid a scam; it might be to betray the very commitments my work had professed. This is how the affective economy of scholar-baiting functions. It turns moral reflex into a vector of risk.

Academic Empathy: "Your Paper Spoke to Me"

The message began with flattery but not empty praise. It referenced my actual work (Lazarus et al. 2025b) and cited arguments I had made about romance fraudsters. This was not a mass-produced bait or spam. It was curated. It created the illusion of mutual understanding. It suggested that the scammer and I were aligned, that our concerns were shared, and that our vocabularies overlapped. This is what I call affective mirroring. The scammer entered through the doorway of empathy. They appropriated the tone of critical ethnography. They borrowed the register of trauma-informed research. And in doing so, they reanimated the logic of fieldwork, not to illuminate, but to ensnare. The manipulation here was not about facts, but about feeling. The message resonated not because it was verifiable, but because it was familiar. It echoed the rhythms of my own work back to me, making the deception feel like a form of recognition.

Investigative Instinct: "*We Have Documents to Share*"

Perhaps the most insidious of all was the final lever, which relied on the appeal to inquiry. The email offered artefacts, images, documents, and registration records, framed as time-sensitive and exclusive. This was not a crude download link. It was a breadcrumb trail, designed to awaken the researcher's epistemic reflexes (to verify, interpret, and follow the lead). The scammer mimicked the rhythm of inquiry, presenting fragments, allusions, and narrative gaps, designed to provoke

interpretive labour. What was activated here was not digital naïveté, but methodological curiosity. The scammer imitated legitimate requests for scholarly collaboration, investigative support, and advocacy. They summoned the core instinct of qualitative research (to listen to the silenced, to follow the marginal, and to pursue the unresolved). Curiosity has been conceptualised in the broader research canon as a core cognitive drive that overrides caution in uncertain contexts (Loewenstein 1994), and investigative compulsion can be tactically exploited in phishing-style lures (Albladi and Weir 2018). Placed in this light, the scam did not just trigger an intellectual reflex. It weaponised it.

This tactic transformed my professional disposition into a liability. It reconfigured the open-ended stance of the ethnographer, the willingness to sit with ambiguity, as a surface of attack. The message did not seek access to my system alone. It also sought access to my curiosity. It turned the act of interpretation into a digital risk.

The Risks of Emotional Enmeshment and Symbolic Entrapment

These appeals (moral, emotional, intellectual) do not operate in isolation. Together, they form what I now recognise as an immersive psychological net. The risk, I came to see, was not merely that I might download a malware-infected file. The deeper risk was symbolic. I might be drawn into the emotional logic of the scam, swept into a script written for me, using my own language, my own research, and my own ethical posture. What unfolded was not a digital intrusion, but mimetic entrapment. The message did not just echo my ethical posture. It simulated the methodological cadence of inquiry itself, blurring the line between interpretation and manipulation. The deeper the message aligned with the world I had studied, particularly online fraud, the harder it became to separate academic curiosity from emotional complicity. So, the message did not just reference my work. It performed it. This experience forced me to confront a rarely acknowledged vulnerability in justice-oriented and interpretive scholarship. That vulnerability is emotional enmeshment. Hence, this work reflects a scholar's encounter with their own vulnerability. We are trained to lean in, to listen, to interpret, and to care. But when an attacker mimics these scholarly virtues, they become liabilities.

The scammer's method is not crude. It does not prey on ignorance. It preys on affective investment. It exploits not the scholar's lack of knowledge but the depth of their moral engagement. The terrain of compromise, in this case, is not technical infrastructure. It is an ethical response. The mechanisms of persuasion and manipulation work precisely because they harness our highest values rather than our weakest reasoning. In this sense, the attack does not bypass rationality. It co-opts virtue. What I encountered was not simply a scam. It was a mirrored performance of my own scholarly commitments.

The Ghost of Your Own Research

This brings me to a metaphor that has quietly shaped my understanding of scholar-baiting. I describe it as the ghost of your own research. What I encountered was not just a scam; it was a haunting. A spectral return of my own published arguments, repackaged as a plea. The themes I had once theorised, online fraud as a form of counter-colonial reparation (Lazarus et al. 2025b), affective fraud (Lazarus et al. 2025c), moral disengagement (Lazarus 2018; Lazarus et al. 2023b), moral economies of deception (Lazarus and Okolorie 2019), and aesthetic deception (Lazarus 2025), returned to me not as abstract, but as characters in an urgent, emotive narrative. The message was not simply *about* a victim. It was about *me*, or at least the narrative self-constructed through my scholarship. This ghosting operated on multiple levels: (1) epistemically, the message mimicked the language and framing of my field. (2) Affectively, it echoed the emotional cadences that had shaped my interviews, my analysis, and my positionality. (3) Ontologically, it blurred the boundary between the representational and the real, between the studied and the summoned.

What results is not mere confusion, but a deep form of ethical disorientation. The question is no longer: *is this a scam?* But *what if it's not?* What if my own work, through its visibility and thematic intimacy, has conjured something real? Or worse, what if it has invited the unreal to pass for the real? In this way, scholar-baiting weaponises the very trust infrastructures of qualitative research. It turns our interpretive openness into a snare. We are forced to ask whether we are encountering data or being recruited into someone else's narrative architecture.

The Digital Scholar as Target: Visibility, Vulnerability, and Vigilance

In the age of open-access publishing and algorithmic visibility, scholars no longer reside solely within the seminar room or the journal page. We are searchable, quotable, and retweetable. Our institutional affiliations travel with us into digital space. Our arguments circulate far beyond their intended readership. We are exposed to audiences whose interactions we cannot always predict. As a researcher implicated in the very dynamics I study, my perspective is both subjective and situated. Scholar-baiting crystallises this shift. It reveals how the academic, especially one working on themes of harm, exploitation, and injustice, can be repositioned not merely as an observer of cybercrime but as a target of it. The very attributes that give a scholar reach, citability, thematic consistency, and moral clarity also make them legible to those who seek to manipulate trust. My analysis is rooted in direct encounter, not abstraction. I am speaking from the aftermath of a message that cited my work, mirrored my values, and mimicked the rhythms of my intellectual commitments. In that moment, I was no longer just a writer of knowledge. I was a node of vulnerability.

Researchers as High-Trust Actors in Digital Epistemic Ecosystems

In digital landscapes, academics function as high-trust actors. We are presumed to verify, to cross-check, to care. This presumption is amplified when one's research traverses domains of trauma, fraud, or systemic injustice. Our inboxes become porous spaces, sites where invitations, disclosures, and cries for justice arrive without warning. We are trained to be open, to treat unsolicited correspondence not as spam, but as data, leads, or collaborative potential. This openness is methodologically virtuous, but operationally hazardous. Unlike corporate actors protected by digital gatekeeping infrastructures, most researchers, especially independent or early-career scholars, navigate these encounters alone. There is no firewall for thematic alignment. No antivirus for empathy. What emerges is a new figure in the cybercrime ecosystem, the scholar as epistemic touchpoint, and a human interface where moral authority meets emotional manipulation.

Balancing visibility with privacy requires a calibrated approach to openness rather than retreat. While detailed strategies are outlined in section "Toward a Framework of Defensive Scholarship" and section "Cyber Hygiene Checklist," I highlight broad principles here: (a) minimise personal identifiers (e.g. home addresses, phone numbers), (b) treat unsolicited digital contact as provisional and subject to verification rather than immediate engagement, and (c) establish an institutional escalation pathway. With these balancing principles in mind, I now turn to the specific threat vectors through which scholar-baiting operates.

Threat Vectors in Scholar-Targeted Social Engineering

Scholar-baiting is not a technical attack wearing emotional clothing. It is a hybrid strategy that braids affect and architecture, trust and technique. Scholar-baiting's aim is not always to steal, but to enmesh. In Table 8, I outline the primary threat vectors identified in scholar-targeted social engineering. I also specify how each operates and the potential impacts.

Table 8. Threat Vectors in Scholar-Targeted Social Engineering.

Threat Vector	Mechanism of Action	Potential Impact
Malware and spyware	Embedded "evidence" files or images, sent under the guise of urgent documentation	Compromise of devices; infiltration of university networks; surveillance
Emotional coercion	Trauma-saturated narratives aligned with scholar's research themes	Psychological stress, loss of clarity, and ethical confusion
Data harvesting	Posing as victims, whistleblowers, or activists to elicit interviews, contacts, or unpublished work	Leak of sensitive data, breach of confidentiality, reputational harm
Reputational entrapment	Use of CC'd fake "victims," staged outrage, or moral panic to provoke a public or private response	Co-optation of scholar's identity, false attribution, risk of citation in bad faith

Together, these vectors demonstrate that the danger lies less in technical sophistication than in the intimate repurposing of scholarly commitments. They turn the very ethos of academic work into an avenue of exploitation. These are not generic phishing techniques. They are customised manipulations based on the researcher's own intellectual footprint. They do not bypass technical firewalls. They bypass cognitive and interpretive ones.

Reframing Risk: From Institutional IT to Scholarly Ethics

Institutional digital security tends to focus on passwords, storage policies, and compliance training. What it overlooks are the emotional and interpretive infrastructures of risk. Scholars open messages not because they are inattentive, but because they are trained to be curious, to engage, to listen, and to assess. Our susceptibility is not just technological but also cognitive, professional, and ethical. If ethical clearance processes are designed to protect the research participants, then the scholar-baiting phenomenon raises a parallel question: who protects the researcher? Security should extend beyond digital hygiene to include interpretive safeguards that acknowledge the researcher as a trust-bearing actor who can also be targeted. As noted in the "Introduction," this concern echoes an earlier question: "What does it mean to conduct ethical research when the researcher walks not on neutral ground, but across thin ice, mapped and booby-trapped by systems they were trained to navigate but never warned might turn against them? It is from this terrain of epistemic vulnerability and embodied risk that I write."

Towards a Framework of Defensive Scholarship

As researchers gain visibility and citational traceability, they become increasingly legible to those seeking to exploit thematic alignment. What is required is not only institutional cybersecurity measures but a recalibration of scholarly orientation attuned to the affective, cognitive, and infrastructural vectors of compromise. The same visibility that enables impact also creates pathways for unsolicited and manipulative contact. This framework rests on three interlocking pillars. (1) Scholar-oriented cyber hygiene: Institutional training is often generic. Researchers working on fraud, deception, or trauma require discipline-specific digital reflexes. Knowing how social engineering operates in one's thematic terrain is as vital as knowing how to analyse it. (2) Clear engagement boundaries: We must establish protocols for triaging unsolicited messages, particularly those that cite our work or offer emotionally charged narratives. Verification is not a betrayal of empathy. It is a precondition for ethical engagement. (3) Institutional escalation pathways: Universities must stop treating researcher security as an afterthought. There is a need

for streamlined, confidential, and expert-led systems for reporting suspicious digital approaches, especially those that mimic research leads or collaboration requests. These measures recognise that researchers are not only producers of knowledge but also potential entry points for manipulation.

Researcher Cyber Hygiene Checklist

Cyber hygiene is vital for researchers working on "sensitive" topics and across disciplines. Drawing on existing scholarship (Kalhoro et al. 2021; Katsarakes et al. 2024; Kocsis et al. 2025) and my own experience, Table 9 outlines core practices. These measures are not technical add-ons but safeguards against phishing, surveillance, and narrative manipulation. Cyber hygiene operates both as protection and as an ethical obligation within research practice. It addresses both technical vulnerabilities and the risks arising from thematic visibility.

Table 9. Cyber Hygiene Checklist for Researchers.

Category	Action Item	Purpose/Benefit
Prevention and digital hygiene	Use institutional email for all research correspondence	Reduces risk of impersonation and improves traceability
	Verify sender identity before responding to urgent or emotional messages	Prevents manipulation through urgency or affect
	Do not click on links or download attachments unless fully vetted	Avoids malware infection or phishing attempts
	Hover over links to preview URLs; inspect for unusual or deceptive domains	Detects spoofed or malicious domains
	Keep the operating system, antivirus, and browser up to date	Protects against known vulnerabilities
	Use two-factor authentication (2FA) and encrypted storage for sensitive files	Strengthens access control and data protection
	Disable auto-preview of images and attachments in email clients	Prevents stealth malware activation
	Schedule regular scans for malware and spyware using trusted software	Ensures early detection and removal of threats
Visibility and public profile	Limit personal details on CVs, bios, and public profiles	Minimises exposure to identity misuse
	Never publish home addresses, phone numbers, or real-time location data	Prevents doxxing and physical risk
	Set Google Alerts for your name and paper titles	Monitors for impersonation or misuse of scholarship
	Refrain from posting fieldwork dates or locations publicly	Reduces personal security vulnerabilities
Emergency protocols	Back up your data routinely and securely	Ensures recovery after an attack or device failure
	If compromised, change all passwords, notify collaborators, and enable 2FA	Limits spread and impact of breach

Category	Action Item	Purpose/Benefit
	Report breaches to institutional CERT teams, Action Fraud UK, or NCSC	Ensures legal/technical response is triggered
	Contact your legal or data protection officer if identity theft or a breach is suspected	Provides institutional and legal safeguards

Cyber Hygiene as Epistemic Reflexivity

As with the old scouting principle, preparedness is not panic. It is readiness. Defensive scholarship is not withdrawal but a refusal to be naïve about how visibility can be exploited. As the boundary between public scholarship and digital exposure narrows, vigilance becomes a scholarly ethic. The same qualities (openness, empathy, and thematic proximity) that sustain qualitative research also create points of vulnerability. Cyber hygiene is not merely technical. It is epistemic. It is not enough to train scholars in consent protocols or trauma handling. They must also be equipped to recognise narrative impersonation, especially when scams adopt research tones, thematic language, or testimonial cadence. Emotional overreach and unsolicited appeals are not, in themselves, signs of vulnerability. They are strategic manipulations. Just as ethnographers manage ambiguity and deception in physical contexts, digital scholarship requires new reflexes for encounters that arrive through unsolicited messages. Scholar-baiting does not simply imitate phishing tactics; it exposes the porousness of academic labour in an era of networked visibility. The issue is not retreat, but critical alertness, involving openness without unguarded exposure. Cyber hygiene, in this sense, is a form of epistemic self-defence grounded in reflexivity tuned to power, persuasion, and digital threat. As academic work becomes more public, performative, and "datafied,"[4] scholars are rendered both authors and potential objects of digital surveillance and manipulation, raising ethical and organisational challenges that current institutional models are not built to manage.

Conceptual Contribution and Implications

By theorising scholar-baiting and document staging as neologisms, the article contributes to the lexicon of digital threat studies by identifying attacks that blur the boundaries between evidence, narrative, and deception. This framing distinguishes superficial impersonation from deeper forms of subversion that exploit the tone, form, and ethos of scholarship itself. This conceptual reframing enables several interventions: (1) repositions the academic as a digital target. The scholar becomes a subject of narrative manipulation rather than solely an observer of deception. (2) Expands the scope of social engineering. Existing typologies prioritise institutional breaches and financial theft; scholar-baiting introduces an epistemic vector rooted in thematic and ethical alignment. (3) Reassesses open-access visibility. Citation practices and public scholarship can unintentionally facilitate narrative intrusion. (4) Foregrounds affective exploitation. These tactics rely less on technical sophistication than on emotional plausibility, drawing on the infrastructures of empathy, curiosity, and care that shape qualitative inquiry.

Conclusion: Vigilance as Epistemic Integrity

[4] "Datafied" signals how scholars are not just visible but digitally captured and made legible through metrics (e.g. citations, altmetrics, downloads), platforms (e.g. ORCID, Google Scholar, ResearchGate), and surveillance infrastructures (e.g. tracking of IP addresses, email behaviours, or location data).

I write as both observer and observed, because I am implicated in the phenomenon I examine. In doing so, I coined the terms scholar-baiting and document staging to name a novel and under-theorised mode of narrative phishing. Scholar-baiting denotes a form of social engineering entangled with scholarly identity and moral obligation, operating as a narrative entrapment that exploits ethical and thematic commitments. Document staging refers to the performative use of crafted artefacts and visuals to manufacture credibility and dull suspicion. I treat this encounter as data, an artefact that exposes the porousness of academic labour in an era of networked manipulation.

These neologisms, outlined in Table 10, offer scholars a vocabulary for recognising affective forms of cyber risk. Such threats bypass institutional firewalls and infiltrate the soft architectures of care, curiosity, and citation, mirroring the very values that underpin engaged scholarship. The idea of defensive scholarship advanced here is not a call for withdrawal but for recalibration. If visibility invites targeting, vigilance must become an ethical reflex, not paranoia, but preparedness; not silence, but critical attunement. I also recognise that my account is both subjective and situated. As a researcher entangled in the dynamics I analyse, the narrative that emerges is necessarily personal and interpretive, grounded in documented experience and lived risk.

Table 10. Boxed Glossary of Key Neologisms.

Term	Definition
Scholar-baiting	A targeted, emotionally calibrated form of social engineering that mimics academic language, values, and citations to lure researchers into engagement.
Document staging	The deliberate embedding of fabricated visual or textual artefacts to simulate credibility and suppress suspicion.
Narrative saturation	The use of dense, emotionally charged storytelling to overwhelm critical reflexes and elicit affective engagement.
Epistemic mimicry	The replication of scholarly tone, themes, and ethical postures as a tactic to exploit academic trust and identity.
Affective mirroring	The tactical use of empathy-aligned language and emotional cadence to establish false relational proximity with scholars.

As with all autoethnographic research, this study is shaped by singularity, and I recognise that my experience cannot stand as representative. Its strength lies in interpretive depth rather than scale, and its limitation is that it cannot capture the full variability of how scholar-baiting might manifest across disciplines, institutions, or geographies. The closeness of the account also carries the risk of over-identification, making it harder to maintain analytical distance. These constraints do not negate the value of the findings; instead, they position them as partial, situated, and open to further corroboration.

Future work should investigate the prevalence and modalities of scholar-targeted phishing across disciplines, platforms, and cultural contexts, including comparative research beyond Africa south of the Sahara. Cross-national surveys, multi-institutional case studies, and interviews with both researchers and institutional IT/security staff could produce broader insights into targeting patterns. There is also scope to examine the psychological and professional impacts of such attacks, as well as the adequacy of institutional responses and support systems. In this sense, autoethnography provides the conceptual spark, but wider empirical approaches are needed to map the scale and diversity of the phenomenon.

More urgently, universities must reconsider how they support researchers who face unsolicited disclosures that appear urgent but may be engineered. At stake is not only data security

but also epistemic security (i.e. the ability to think, feel, and respond without manipulation). Vigilance, then, cannot rest on individual scholars alone. It must become a shared ethic in which researchers and institutions together defend the fragile space in which knowledge is made. To consolidate the conceptual contributions of this study, Table 10 presents a glossary of the key neologisms introduced. In that sense, preparedness is not paranoia but integrity under digital scrutiny.

References

Abdullah, A. S., & Masnizah, M. (2019). *Spear phishing simulation in critical sector: Telecommunication and defense sub-sector*. In 2019 International Conference on Cybersecurity (ICoCSec) (pp. 26–31). Negeri Sembilan, Malaysia.

Abubakari, Y. (2024). Modelling the modus operandi of online romance fraud: Perspectives of online romance fraudsters. *Journal of Economic Criminology, 6*, 100112. https://doi.org/10.1016/j.jeconc.2024.100112

Abubakari, Y. (2025). Forgiveness-seeking behaviors among online romance fraudsters: Insights from Sakawa actors in Ghana. *International Journal of Offender Therapy and Comparative Criminology*. Advance online publication. https://doi.org/10.1177/0306624X251322533

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences, 8*(1), 5. https://doi.org/10.1186/s13673-018-0128-7

Anderson, L. (2006). Analytic autoethnography. *Journal of Contemporary Ethnography, 35*(4), 373–395. https://doi.org/10.1177/0891241605280449

Barclays. (2025). *Bereavement scams*. https://www.barclays.co.uk/fraud-and-scams/bereavement-scams

Bekkers, L. M. J., Moneva, A., & Leukfeldt, R. (2025). Distinct group, distinct traits? A comparison of risk factors across cybercrime offenders, traditional offenders and non-offenders. *Psychiatry, Psychology and Law*, 1–25. https://doi.org/10.1080/13218719.2025.2546311

Ben-Lulu, E. (2024). Navigating academic identity: Autoethnography of otherness and embarrassment among first-generation college students. *Journal of Contemporary Ethnography, 53*(3), 327–350. https://doi.org/10.1177/08912416241233697

Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted love: A systematic literature review of online romance scam research. *Interacting with Computers, 35*(6), 773–788. https://doi.org/10.1093/iwc/iwad048

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). Detection and prevention of spear phishing attacks: A comprehensive survey. *Computers & Security, 151*, 104317. https://doi.org/10.1016/j.cose.2025.104317

Blevins, K. R., & Holt, T. J. (2009). Examining the virtual subculture of johns. *Journal of Contemporary Ethnography, 38*(5), 619–648. https://doi.org/10.1177/0891241609342239

Button, M., Lazarus, S., Hock, B., Sabia, J., Gilmour, P., & Pandey, D. (2025a). Nigerian confraternities and mass cross-border fraud. *Trends in Organized Crime*, 1–21. https://doi.org/10.1007/s12117-025-09576-2

Button, M., Lazarus, S., Hock, B., Sabia, J. B., Pandey, D., & Gilmour, P. (2025b). Factors influencing involvement in cyber-frauds in West Africa and the implications for policy. *European Journal on Criminal Policy and Research*, 1–23. https://doi.org/10.1007/s10610-025-09649-6

Carter, E. (2024). *The language of romance crimes: Interactions of love, money, and threat*. Cambridge University Press.

Chang, J., & Chong, M. D. (2022). Cognitive heuristics and risk evaluation in crisis fraud. *Journal of Financial Crime, 29*(2), 447–459. https://doi.org/10.1108/JFC-02-2021-0030

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*, 1753.

Corkhill, P. (Pseudonym), & Charman, S. (2024). The show must go on! An autoethnography of (re)socialization into senior policing in England and the prominence of "leadership theatre." *Journal of Contemporary Ethnography, 53*(6), 758–795. https://doi.org/10.1177/08912416241271282

Cross, C., & Holt, T. J. (2023). More than money: Examining the potential exposure of romance fraud victims to identity crime. *Global Crime, 24*(2), 107–121. https://doi.org/10.1080/17440572.2023.2185607

Daily, The Researcher. (2024). *Staying safe and sane in research.* https://researcherdaily.com/p/staying-safe-and-sane-in-research

Denshire, S., & Lee, A. (2013). Conceptualizing autoethnography as assemblage: Accounts of occupational therapy practice. *International Journal of Qualitative Methods, 12*(1), 221–236. https://doi.org/10.1177/160940691301200110

Ellis, C., Adams, T. E., & Bochner, A. P. (2011). Autoethnography: An overview. *Historical Social Research, 36*(4), 273–290. https://www.jstor.org/stable/23032294

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In T. Tryfonas & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust* (Vol. 9190, pp. 36–47). Springer.

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography, 48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Hind, S. (2025). Mum of pregnant Scot found dead in Ghana hotel bath demands fresh murder probe. https://www.dailyrecord.co.uk/news/scottish-news/mum-pregnant-scot-found-dead-35139876

Holt, T. J., & Copes, H. (2010). Transferring subcultural knowledge online: Practices and beliefs of persistent digital pirates. *Deviant Behavior, 31*(7), 625–654. https://doi.org/10.1080/01639620903231548

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access, 9*, 99339–99363. https://doi.org/10.1109/ACCESS.2021.3097144

Katsarakes, A., Morris, T., & Still, J. D. (2024). Hidden in onboarding: Cyber hygiene training and assessment. In A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust* (Vol. 14728, pp. 53–63). Springer.

Kingsbury, K. (2022). Autoethnography of Holy Death: Belief, dividuality, and family in the study of Santa Muerte. *Journal of Contemporary Ethnography, 51*(6), 784–815. https://doi.org/10.1177/08912416221075374

Kocsis, D., Shepherd, M., & Segal, D. (2025). Teaching tip: Cyber hygiene training using a Salesforce developer module to improve student online behaviors. *Journal of Information Systems Education, 36*(2), 90–110. https://doi.org/10.62273/CUEU6233

Krain, M., Murdie, A., & Beard, A. (2024). Silencing human rights defenders once and for all? Determinants of human rights defenders' killings. *Political Research Quarterly, 77*(1), 401–416. https://doi.org/10.1177/10659129231217282

Lavorgna, A., & Sugiura, L. (2022). Blurring boundaries: Negotiating researchers' positionality and identities in digital qualitative research. *Italian Sociological Review, 12*(7S), 709–727. https://doi.org/10.13136/isr.v12i7S.578

Lazarus, S. (2018). Birds of a feather flock together: The Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. *Criminology, Criminal Justice, Law & Society, 19*(2), 63–81.

Lazarus, S. (2021). Demonstrating the therapeutic values of poetry in doctoral research: Autoethnographic steps from the enchanted forest to a PhD by publication path. *Methodological Innovations, 14*(2), 20597991211022014. https://doi.org/10.1177/20597991211022014

Lazarus, S. (2024). An autoethnographic perspective on scholarly impact, citation politics, and North–South power dynamics. *Life Writing, 22*(3), 603–629. https://doi.org/10.1080/14484528.2024.2430666

Lazarus, S. (2025). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "Black Axe" confraternity. *Deviant Behavior, 46*(4), 456–480. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of EFCC agents. *Telematics and Informatics, 40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Soares, A. B., & Button, M. (2025a). Pathways, pressure, and profit: Adaptive innovation and strain in a convicted cybercrime academy called Hustle Kingdom. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2025.2551790

Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023a). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000–2021). *Journal of Economic Criminology, 2*, 100013. https://doi.org/10.1016/j.jeconc.2023.100013

Lazarus, S., Hughes, M., Button, M., & Garba, K. H. (2025b). Fraud as legitimate retribution for colonial injustice: Neutralization techniques in interviews with police and online romance fraud offenders. *Deviant Behavior*, 1–22. https://doi.org/10.1080/01639625.2024.2446328

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023b). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology, 2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Lazarus, S., Tickner, P., & Button, M. (2025c). Pulpit, power, and predation: "Yahoo Men of God," prosperity theology, and the twin fraud triangles. *Critical Research on Religion.* Advance online publication. https://doi.org/10.1177/20503032251381309

Loewenstein, G. (1994). The psychology of curiosity: A review and reinterpretation. *Psychological Bulletin, 116*(1), 75–98. https://doi.org/10.1037/0033-2909.116.1.75

Marczak, B., & Scott-Railton, J. (2016). *The million dollar dissident: NSO Group's iPhone zero-days used against a UAE human rights defender*. https://hdl.handle.net/1807/96976

O'Hagan, L. A. (2023). Music for mental health: An autoethnography of the Rory Gallagher Instagram fan community. *Journal of Contemporary Ethnography, 52*(5), 633–663. https://doi.org/10.1177/08912416231162077

Ortiz-Vilarelle, L. (2021a). Autoethnography and beyond: Colonialism, immigration, embodiment, and belonging. *Life Writing, 18*(3), 307–314. https://doi.org/10.1080/14484528.2021.1964920

Ortiz-Vilarelle, L. (2021b). Autoethnography and beyond: Genealogy, memory, media, witness. *Life Writing, 18*(4), 475–482. https://doi.org/10.1080/14484528.2021.1982161

Schokkenbroek, J. M., & Snaphaan, T. (2025). Love as bait: A scoping review and crime script analysis of online romance scams. *Trauma, Violence, & Abuse.* Advance online publication. https://doi.org/10.1177/15248380251361046

Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. *Criminal Justice Studies, 37*(4), 328–351. https://doi.org/10.1080/1478601X.2024.2429088

Soares, A. B., Lazarus, S., & Button, M. (2025). Love, lies, and larceny: One hundred convicted case files of cybercriminals, with eighty involving online romance fraud. *Deviant Behavior*, 1–24. https://doi.org/10.1080/01639625.2025.2482824

Stanley, P. (2023). An autoethnography of "making it" in academia: Writing an ECR "journey" of Facebook, assemblage, affect, and the outdoors. *Journal of Contemporary Ethnography, 52*(3), 404–431. https://doi.org/10.1177/08912416221120819

Watts, M. (2015). Tributes to pregnant wife found dead in hotel in Ghana as Tottenham pastor is questioned. *The Standard.*

Yavuz, D. A. (2024). The companion: A hospital autoethnography on the relationship between informal and formal institutions. *Journal of Contemporary Ethnography, 53*(4), 488–515. https://doi.org/10.1177/08912416241248459

Yushawu, A., & Jaishankar, K. (2025). Sakawa in Ghana: The influence of weak ties on economic cybercrime offender networks. *Deviant Behavior*, 1–21. https://doi.org/10.1080/01639625.2025.2459681

Zempler Bank. (2025). *Bereavement scams: How to spot and protect yourself.* https://www.zemplerbank.com/help/security-and-fraud/different-types-of-scams/bereavement/