Fragmented, Generic, and Non-Victim-Centric: An Analysis of Japanese Official Online Fraud Reporting Guides and Contact Channels

Rei Yamagishi
NICT, Waseda University,

Misato Matsuda
NICT

Ayako A. Hasegawa
NICT

Takahiro Kasama
NICT

Tatsuya Mori
Waseda University, NICT, Riken AIP

1 Introduction

Online fraud is increasing across many countries [1,5]. Nevertheless, many fraud victims neither report their victimization to law enforcement agencies nor seek help from support organizations [4]. Connecting fraud victims with law enforcement and support services is important for public safety, through the identification of fraudsters, and individual recovery.

Prior work on online fraud victimization has identified barriers to reporting and help-seeking that extend beyond individual emotional factors (e.g., shame, self-blame, and stigma) to include concerns about the poor usability of reporting and support systems and the lack of victim-centered support [2–4, 9, 10]. However, empirical and systematic analyses of the gap between the existing systems and the recommendations proposed by prior work are limited.

To address this gap, we systematically collect and evaluate the online "*official guides*" related to fraud reporting and victim support provided by government and law enforcement agencies as well as the "*contact channels*" available for victims to report or seek help via email, phone, online forms, and other means. As an initial step, we focus on Japanese government and law enforcement agencies, which have been characterized by fragmented administrative structures [8] and delayed digitalization [12]. Specifically, we address the following research questions: **(RQ1) What are the functional scopes of the contact channels listed in the official guides?, (RQ2) What are the roles and services provided by the official guides themselves?**, and **(RQ3) How do these guides communicate with users?**

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

2 Methodology

We systematically collected and analyzed the official guides provided by national and metropolitan (specifically, Tokyo) government agencies.

Data Collection Following the agency-based approach [11] for systematically identifying cybersecurity guidance published by government, we collected official guides. First, we accessed the websites of national and Tokyo metropolitan government agencies using official agency lists [6,7]. Second, for each website, we conducted site searches using the query: "fraud [consult | report | support]"[1] to identify guides offered by each agency, removing any duplicates. Third, starting from the identified guides, we followed menus, sitemaps, and cross-references to discover additional guides. Fourth, to complement the agency-based search, we ran Google searches with the same query terms restricted to "go.jp" and "tokyo.lg.jp" (up to ten pages), yielding no additional guides. Finally, we manually reviewed each guide to identify the contact channels listed for consultation, reporting, and victim support. In total, we identified 31 official guides and 55 contact channels.

Data Analysis We iteratively developed a codebook to analyze the collected data. The initial codebook included deductive codes based on recommendations for government and law enforcement agencies, as proposed in recent representative studies on the experiences of online fraud victims [2–4, 9, 10]. Specifically, the codebook comprised 12 code categories, such as the functional scope of contact channels and coordination with other organizations (RQ1); roles and services provided by the guides (RQ2); and instructions on actions to take, strategies to encourage reporting and help-seeking, and victim-centered considerations (RQ3). Two authors independently updated the codebook based on a random subset of the data and integrated their revisions through multiple rounds of discussion, achieving a final Krippendorff's α above 0.80 across all categories after four iterations. The two authors then independently coded the remaining data.

Ethics Considerations This study analyzes only public web

[1] The original Japanese query:"詐欺 [相談|報告|支援]"

pages with no sensitive personal information. We identified channel characteristics from these public sources, avoiding any unnecessary burden on agencies from investigative false reports. Therefore, this study protocol raised no ethical concerns and was exempt from institutional review.

3 Key Findings

3.1 RQ1: Scope of Contact Channels

Overview The functional scopes of contact channel varied widely, including victim reporting, third-party tip submission, consultation with specialists (law enforcement officers, engineers, psychologists/public health nurses, and lawyers), legal action support, financial recovery, and self-help group referral. Multiple channels served overlapping functions; for instance, 21 channels supported third-party tip submission. While multiple channels may lower barriers to victim access, they also risk causing confusion, as prior work has noted. Documented coordination across agencies was present in 20 channels, including proxy reporting, sharing with relevant government agencies and private sector organizations based on fraud type, and referrals across support stages (e.g., to lawyers or psychologists following fraud reporting).

Extended insights Prior work recommended centralized reporting and coordination across agencies to improve convenience for victims and minimize their re-traumatization [4, 10]; however, even fragmented coordination remains limited in practice. Law enforcement agencies, typically victims' first point of contact, tend to be endpoints rather than hubs in information sharing. We recommend building law-enforcement-centered coordination networks and a unified reporting system, which would reduce the risk of impostor support agencies and help raise low victim reporting rates that remain a recognized challenge.

3.2 RQ2: Services and Roles of Guides

Overview In addition to providing the contact channels in Section 3.1, the guides offered a range of services, including distributable fraud awareness materials, foundational fraud knowledge, updates on the latest fraud techniques, and instructions on financial recovery processes. The National Police Agency played a central role in fraud response, with its cybercrime-related division providing a broad cybercrime guide, and additional dedicated guides covering fraud awareness and crime victim support. The Financial Services Agency and two related agencies focused on legal explanations and referrals for financial recovery, while other ministries and agencies provided awareness guides targeting impostor scams within their own areas of responsibility.

Extended insights Prior work has shown that regularly sharing fraud techniques, particularly psychological manipulation, effectively protects potential victims [9, 10]. However, such information was fragmented across agency pages, infrequently updated, and limited in coverage. Future work should focus on designing systems that effectively convey factual fraud techniques from actual cases while safeguarding victims' personal information.

3.3 RQ3: Communication Styles of Guides

Overview Of the 26 guides linking to the next recommended channel, only 14 included descriptions of the link. Broken links and outdated information were also observed, suggesting poor usability and maintenance. The benefits of victim reporting were rarely explained, and where present, such explanations lacked sufficient emphasis. While multilingual and accessibility support was available in some guides, most offered only English translation and font size adjustment. Two guides addressed victim isolation by disclosing fraud statistics and including encouraging messages such as "don't suffer alone."

Extended insights Prior work has identified the lack of clear procedural guidance as a barrier to victim reporting [4]; our analysis reveals three specific problems. First, there was a lack of comprehensive flow guides covering all necessary steps across fraud types, the provision of which by law enforcement could considerably encourage victims to report. Second, sophisticated fraud techniques have led to inconsistent terminology, making it difficult for victims to accurately identify the fraud type they experienced. To address this problem, systems leveraging large language models could help guide victims from ambiguous input to the appropriate fraud type. Third, descriptions of other agencies were often incomplete, outdated, or contained broken links, requiring closer coordination and mechanisms to keep information current.

In terms of victim-centered considerations, only two guides reflected prior work's recommendations. This may partly reflect the lack of dedicated guides for fraud victims, who are often directed to guides designed for general crime victims despite facing distinct emotional barriers such as shame. Governments and law enforcement would benefit from providing dedicated guides that include fraud statistics and messages highlighting the availability of support. Future work should explore and evaluate approaches that address fraud victims' distinct emotional barriers.

4 Conclusion and Further Work

This study systematically analyzed official Japanese online fraud guides and contact channels, highlighting gaps between prior work's recommendations and current practice in coordination, usability, and victim-centered design. Further work will expand to additional countries, aiming to identify country-specific challenges, enable cross-country comparisons, and recommend exemplary practices.

References

[1] GLOBAL FINANCIAL FRAUD THREAT ASSESSMENT, 2026. Accessed: 2026-5-19.

[2] Elijah Bouma-Sims, Mandy Lanyon, and Lorrie Faith Cranor. 'Is This a Scam?': The Nature and Quality of Reddit Discussion about Scams. In *Proc. of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS'25)*, pages 2444–2458, 2025.

[3] Jake Chanenson, Tara Matthews, Sunny Consolvo, Patrick Gage Kelley, Jessica McClearn, Sarah Meiklejohn, Abhishek Roy, Renee Shelby, Kurt Thomas, and Amelia Hassoun. "It didn't feel right but I needed a job so desperately": Understanding People's Emotions & Help Needs During Financial Scams. In *Proc. of the 2026 CHI Conference on Human Factors in Computing Systems (CHI'26)*, 2026.

[4] Xiaowei Chen, Mindy Tran, Yue Deng, Bhupendra Acharya, and Yixin Zou. From Harm to Healing: Understanding Individual Resilience after Cybercrimes. In *Proc. of the 2026 CHI Conference on Human Factors in Computing Systems (CHI'26)*, 2026.

[5] Federal Trade Commission. New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024. Accessed: 2026-5-19.

[6] e Gov Japan. Government Ministries And Agencies. https://www.e-gov.go.jp/government-directory/ministries-and-agencies.html. Accessed: 2026-5-23.

[7] Tokyo Metropolitan Government. Organizational Information. https://www.metro.tokyo.lg.jp/about. Accessed: 2026-5-23.

[8] Ministry of Internal Affairs and Communications. White paper on information and communications in japan 2023. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/00zentai.pdf, 2023. Accessed: 2026-5-26.

[9] Rajvardhan Oak and Zubair Shafiq. "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams. In *Proc. of the Twenty-First Symposium on Usable Privacy and Security (SOUPS'25)*, 2025.

[10] Rajvardhan Oak and Zubair Shafiq. Victims, Vigilantes, and Advice Givers: An Analysis of Scam-Related Discourse on Reddit. In *Proc. of the Twenty-First Symposium on Usable Privacy and Security (SOUPS'25)*, 2025.

[11] Kimberly Ruth, Raymond Buernor Obu, Ifeoluwa Shode, Gavin Li, Carrie Gates, Grant Ho, and Zakir Durumeric. A First Look at Governments' Enterprise Security Guidance. In *Proc. of 34th USENIX Security Symposium (SEC'25)*, pages 119–138, 2025.

[12] World Bank. Riding the Wave of Digital Transformation: Insights from Japan's Journey. https://documents1.worldbank.org/curated/en/099352305232428567/pdf/P177977145b03308b19ef61f321c4e404f4.pdf, 2024. Accessed: 2026-5-26.