Appendix to “Is this a scam?”: The Nature and Quality of Reddit Discussion about Scams

A Codebook

A.1 Post Type

This category describes the apparent purpose of a post. Only a single one of these codes is assigned

Irrelevant: Post is off-topic or incomprehensible. Includes spam.

Media Missing: Post links to images, videos, news articles, etc. that are not available. Does not include cases where the user links to the scam website and it has since been taken down. Does not include irrelevant posts.

Scambaiting: Post describes interacting with a scammer to waste their time or enact vigilante justice. Includes examples where users ask questions about how to scambait, posts where users request that others spam or report a scammer.

Report of Victimization: User shares their experience of being victimized by a scam without asking for advice or emotional support. If the post includes a question about whether something is a scam, code it as "Scam identification." If the post includes a question, code it as "Request for support."

Scam Identification: User describes a situation/shows media with the goal of determining whether something is a scam.

Request for Support: User asks for advice, information, or emotional support related to scam victimization, scam communications, or scam prevention. If the post also includes a question about whether something is a scam, code it as "Scam identification."

Discussion of Scam Communications: Post contains text, media, or other descriptions of communication from a scammer. The user seems to think the communication they encountered was fraudulent. They have not fallen victim to the scam (i.e., they have not been deceived into providing sensitive personal information or money).

Scam Related Media: User shares media related to scams that does not convey something they or a friend/relative experienced (e.g., YouTube videos, news reporting, documentaries, etc.).

Other: Post seems to be about scams, but does not fall into one of the above categories. Often, discussion of scams in general.

A.2 Technologies & Communication Methods

This category describes what technologies are used to facilitate social engineering or otherwise conduct the scam. Include all technologies that are used or mentioned by a scammer, unless it is obvious that the technology is not actually being used (e.g., if they spoof a PayPal email, non-crypto payment processing is not involved). Where a service has multiple components, the relevant component should be selected. For example, if someone found an item on Facebook marketplace, the initial communication method should be described as “Ecommerce website/service.”

Due to space constraints, the paper only discusses initial communication methods; however, all posts were also assigned separate codes to describe other technologies used.

Unclear: Post does not mention what technologies were used to initiate/facilitate a scam.

Multiple Stories: Post involves multiple fraud victimization experiences. Do not code other categories for this column.

Author’s Contact Information:

A.2.1 Websites & Online Services:

Ecommerce Website/Service: Scam involves websites used to sell goods and services online, such as Amazon, eBay, Etsy, Facebook Marketplace, Uber, etc. Includes any messaging that occurs on these platforms. Includes potentially fraudulent ecommerce websites.

Social Media: Social media services such as YouTube, Facebook, Instagram, etc. are used as part of the scam. Includes cases where the scammer uses social media to obtain information about the victim (e.g., photos of their friends). Messaging on social media platforms and dating-based social media services are coded separately. If someone says something like "they contacted me on social media," assume this code applies.

Dating Service: A social media service dedicated to dating services such as Tinder, Grindr, Bumble, etc. Includes potentially fraudulent dating services.

Job Board: Websites or services like Indeed, CareerBuilder, etc. that are dedicated to finding or sharing employment opportunities.

Classified Website: Websites like Craigslist that are used to post general classified advertisements.

Other Website or Online Service: Another website or online service that doesn’t fit into the categories above. Most often, this will be a website designed for a scam (e.g., a fake bank login page for phishing, a fake business webpage, etc.).

A.2.2 Communications Technologies:

Phone Call: Calling via traditional land-line telephones, mobile phones, or VoIP services. If a user states that they were called or called someone without specifying the platform/medium, assume it falls into this category.

Video Call: Calling via FaceTime, Zoom, Skype, etc., where video is transmitted alongside audio.

Email: Messages via email, including the mention of specific email providers (e.g., Gmail, Hotmail, etc.).

Instant Messaging: Messaging via SMS or other comparable internet technologies (e.g., iMessage, RCS, etc.). Does NOT include messaging on social media or messaging platforms with social media features (see Social media messaging). If a user states that they "texted" or "messaged" someone without specifying the platform, assume it falls under this category.

Social Media Messaging: Messaging via social media platforms (E.g., Facebook Messenger, Twitter Direct Messages, etc.). Also applies to messaging platforms like Discord, Telegram, WhatsApp, and Snapchat that have social media features like a directory and stories.

A.2.3 Payment Methods:

Crypto Assets: Scam involves the use of cryptocurrencies (e.g., Bitcoin, Ethereum, USDT, etc.) or other cryptocurrency-based technologies (e.g., NFTs, smart contracts, etc.).

Non-Crypto Digital Payment Processing: Scam involves PayPal, Venmo, Zelle, or other similar online payment processors that are not cryptocurrency. Doesn’t include checks, credit/debit cards, or ACH transfers.

Gift Cards: Any gift card (e.g., Apple gift cards, Amazon gift cards, Walmart gift cards, etc.).

A.2.4 Analogue Communication Methods:

Mail: Scam involves material sent through the mail, including commercial parcel services (e.g., UPS, FedEx, DHL, etc.).

In-Person Interaction: Scam involves communicating with a person face-to-face.

A.2.5 Other Technologies:

Remote Access: Scam involves software that is used to remotely control or view a device. Typically employed in customer service scams.

File Download: Scam involves downloading a file, such as an email attachment or software package. May or may not be malware.
Other technologies: Scam involves other technologies or communication methods not listed above.

A.3 Type of Scam

This category captures the distinctive features of the scam described by a post. On `/r/Sextortion`, we assumed posts met the definition of financial sextortion, unless other details were provided that contradicted this assumption.
Likely not a scam: The post describes something that seems not to be an illegal scam. May be another type of crime or just business practices that the user finds distasteful.
Multiple stories: The post involves multiple fraud victimization experiences or attempts at fraud. Do not assign other codes if this code applies.
Unclear: The post lacks enough information to categorize the type of scam. Paired with other codes where it is likely to be a particular type of scam, but there isn’t enough information to be sure.

A.3.1 Imposter Scams:

Phishing: Post describes/shows communications that falsely purport to be from a trusted entity that directs people to provide sensitive information. Only applied where a user is explicitly directed to provide information.
Government imposter: Post describes/shows communications that falsely purport to be from a government entity (i.e., police, the Internal Revenue Service, USPS, etc.).
Corporate imposter: Post describes/shows communications that falsely purport to be from a trusted company or service (i.e., a bank, a social media service, etc.).
Customer support scam: Post describes a scam where the victim is led to believe that they are communicating with tech support or customer support for some business. They are convinced to share access to a computer, provide information, or pay for a service. Almost always paired with "Corporate imposter."
Public figure imposter: Post describes/shows communications that falsely claim to be from a prominent person, like a celebrity, politician, or social media influencer.
Family/friend imposter: Post describes/shows communications that falsely claim to be from a friend or family member. May come from a hacked account that belongs to that person.
Other imposter: Post describes/shows communications that impersonate a different type of person/entity than listed above (i.e., an employee or customer).

A.3.2 Commerce:

Ecommerce seller: Post describes an apparent scam involving a scammer who is the seller of goods or services online. Often paired with "Non-delivery" or "Fake/defective product."
Ecommerce buyer: Post describes a scam involving a scammer who is the purchaser of goods/services. Often paired with "Non-payment" or "Fake payment."
Non-delivery: Post describes a scam where the victim pays for a product/service but never receives it. Almost always paired with "Ecommerce seller."
Non-payment: Post describes a scam where the victim sells a product/service but never receives payment. Almost always paired with "Ecommerce buyer."
Unauthorized subscription: Post describes a scam involving a subscription that is hidden, unrequested, or impossible to cancel.

Fake or defective product: Post describes a scam where the victim receives or is offered a product that is defective, counterfeit, or otherwise not as advertised.
Non-internet commerce: Post describes an apparent scam involving a scammer who is the seller of goods/services using phone, mail, or in-person interaction.

A.3.3 Opportunity Schemes:

Relationship scam: A scam characterized by building a false relationship (typically romantic) with a victim in order to manipulate and/or steal from the victim. Does not apply to shorter-term scams that do not involve a long-term relationship (i.e., sextortion).
Advance fee: Post describes a scheme where a victim is asked to pay a fee before they can receive something of value (i.e., a prize, investment windfall, inheritance, housing, etc.). May be paired with codes like "Prize scam", "Investment scam", etc.
Rental scam: Post describes a scam where a victim is offered a short-term or long-term rental. It may be paired with "Advance fee."
Investment scam: Post describes a scam where a victim is offered an investment opportunity, usually with absurdly high returns. The investment is not real or otherwise fraudulent (like a Ponzi scheme).
Prize scam: Post describes a scam where the victim is led to believe that they have been selected to receive a prize, grant, inheritance, or other windfall. It may be paired with an "Imposter scheme" and/or involve an "Advance fee" or "Fake payment." Includes “sugar mama” scams.
Employment scam: Post describes a scheme where a user is offered a fake job. May involve performing real tasks as a ruse to obtain money or information. User may be an unknowing accessory to crime (i.e., sending/receiving stolen funds). Includes cases where someone is commissioned to produce a good, like art.

A.3.4 Threat-based Schemes:

Fake warning: Post describes or shows a pop-up, notification, or other communication that is meant to mimic OS/software warnings.
Fake debt: Post describes a scam where the victim is led to believe that they owe a debt that they must pay. May be paired with "Government or Corporate imposter."
Sextortion: Post describes a scam where the victim is threatened with the releasing of explicit media featuring the victim. The material may actually exist or be fictitious.
Sympathy scam: Post describes a scam where the victim is led to believe that the scammer is facing some adverse personal circumstances (i.e., illness, imprisonment, etc.) and requires money. May be paired with "Family/friend imposter."
Other threat: Post describes another scam where the victim is threatened with some harm (i.e., arrest, physical harm, etc.) in order to convince them to pay. This code does not apply where another, more specific category applies.

A.3.5 Other ruses:

Pin scam: Post describes a scam where a scammer attempts to get a user to provide a verification code sent via instant messaging, phone call, or via mail. This is usually framed as wanting to verify a user’s identity. Most often, this is a Google Voice authentication code, used to falsely verify possession of the victim’s phone number. Does NOT include cases where the code is an MFA authentication code. Often paired with "Ecommerce buyer."
Fake payment: Post describes a scheme where a victim is led to believe they have been paid (most often via a fake

check). Many variants of the scheme involve a victim receiving an apparent overpayment and being asked to send part of the money back.
Wrong number: Conversation initiated by a person posing as an individual who has mistakenly texted the wrong account. Often not enough information to tell if it's a genuine wrong number or a scam.

A.4 Type of Harm

None: User does not state that they experienced financial or privacy-related harms.
Unclear: User seems to describe harm, but it's not specified what type (e.g., they say they were scammed, but don't say what that means). May be paired with other harm codes if one or more types of harm seems likely, but is not clearly specified.
Exposure: User describes intimate imagery being shared publicly without permission.
Account compromise: Attacker gains access to one or more of a victim's online accounts.
Financial harm: Victim is financially harmed. Includes loss of money, loss of goods, or uncompensated labor.
Financial charges reversed: The user lost money but had the charge successfully reversed.
Personal information disclosed: User describes that a scammer obtained their personal information (see A.7).
Intimate imagery shared: It is implied by their post or explicitly stated that the scammer has intimate imagery of the victim.

A.5 Type of Support Requested

This category was used to define the types of support requested by users in posts.
Understanding of victimization experience: Poster requests information or clarification about how a scam they were victimized by works.
Other users' experiences: Post/comment requests for users to share their personal or similar experiences.
Scam prevention advice: Poster requests advice on blocking scam communications or otherwise avoiding scams.
How to report scam: Poster requests advice on reporting a scammer or scam communications.
Financial recovery advice: Poster requests advice on recovering funds after being victimized by a scam.
Advice on collecting evidence: Poster requests advice on collecting evidence about their scam experience (i.e., tracing IP, identifying a photo, finding posted nudes, etc.).
General scam remediation advice: Poster requests advice on other aspects of remediation. May be specific or general (i.e., what should I do?).
Reassurance about scam outlook: Poster seeks reassurance about whether or not they will be fine after being victimized by a scam. Often relates to wanting assurance that the steps they have taken are sufficient.
General emotional support: Poster seeks emotional or therapeutic support connected to scam victimization.
Request to DM: Poster requests to DM other users. This code only occurred in comments.

A.6 Remediation Steps and Other Advice

These codes describe the advice given to users by commenters. These codes were also applied to describe the steps taken by the posters of requests for support, but this was not described in the paper due to space constraints.

Remediation is defined as the actions taken to restore the status quo after scam victimization, including technical and non-technical actions. Security/scam avoidance advice is defined as actions meant to improve one's security, which may be employed after scam victimization but are more generally beneficial.

A.6.1 Scam Remediation Advice:

Contact financial institution/payment processor: Recommendation or remediation step of reporting the crime to a financial institution/payment processor in order to lock a payment card, get a replacement card, reverse the charge, or otherwise report the crime.
Contact service provider: Recommendation or remediation step of contacting a non-financial service that was involved in perpetrating the scam (i.e., social media company, ecommerce platform, etc.) to report a scam. Includes moderators or admins of a community). When someone says ''Report" without explicitly specifying an entity, assume this code applies unless that contextually doesn't make sense.
Contact law enforcement: Recommendation or remediation step of contacting law enforcement (i.e., local police, FBI, etc.) to report the scam or otherwise aid in remediation.
Contact recovery service: Recommendation or remediation step of contacting a paid service that claims to help recover lost money. Seems like these are mostly scams.
Contact credit bureau: Recommendation or remediation step of freezing credit, placing an identity theft warning, or otherwise contacting a credit bureau related to a scam.
Contact other government entity: Recommendation or remediation step of contacting a non-law enforcement government entity like the Federal Trade Commission.
Contact NGO: Recommendation or remediation step of contacting a non-governmental organization connected to scams, such as StopNCII.
Contact lawyer: Recommendation or remediation step of contacting a lawyer to aid in remediation of a crime. Includes cases where someone suggests that they want to initiate legal proceedings.
Contact scammer for redress: Recommendation or remediation step of contacting the alleged scammer to obtain redress, such as a refund. Typically in the ecommerce context.
Contact personal connection(s): Recommendation or remediation step of discussing the crime with a friend, family member (i.e., parent), or other trusted individual (i.e., school counselor).
Contact (Unclear): Recommendation or remediation step of contacting a type of entity that is unspecified or unclear.
Write review/report to crowdsourced anti-scam list: Recommendation or remediation step of leaving a review for a scammer or otherwise reporting to a crowdsourced anti-scam resource.
Cut-off communication: Recommendation or remediation step of blocking a scammer, deleting communications, or otherwise ignoring their attempts at communication.
Disable/delete social media account: Recommendation or remediation step of deleting or otherwise disabling social media accounts.
Change identifier: Recommendation or remediation step of changing phone number, username, email address, or other identifier.
Change password: Recommendation or remediation step of changing password to account(s).
Change security/privacy setting: Recommendation or remediation step of changing security or privacy settings for a social media account such as make the account private, make the follower list private, disable DMs, enable a PIN, etc.
Collect/preserve evidence: Recommendation or remediation step of obtaining/preserving evidence to aid in remediation.
Other remediation step(s): Other remediation step(s) that the poster takes or are recommended.

A.6.2 General Security or Scam Avoidance Practices:

Enable MFA: Recommendation or remediation step of enabling 2FA or other MFA technology.
Don't send nudes: Recommendation to not take or share intimate pictures/videos/video calls with others online.
Don't click links: Advice not to click on links from communications.
Don't answer communications from unknown sources: Advice not to answer calls, texts, etc. from unrecognized sources.
Use anti-virus/security scan: Recommendation or remediation step to use anti-virus/other security software on a device.
Use unique passwords: Recommendation or remediation step to use different passwords on each account.
Watch out for recovery services/scams: Recommendation to avoid any service/individual that claims to help recover lost money or otherwise remediate scams.
Don't pay scammer: Recommendation to not pay/stop paying a scammer. Includes cases where the commenter advises the poster that paying was a bad idea after they already paid.
Be careful: Non-specific advice to be careful or avoid scams.
Advice on helping friend/relative identify scam: Recommendation on how to convince someone that something is a scam.
Advice on ecommerce payment: Advice about how to accept/send payment in ecommerce. Includes recommendations on using a particular platform for sales.
Advice on where to shop: Recommendations about how to avoid scams when online shopping, such as doing research, avoiding unknown sellers, looking at DNS, etc.
Other Security/Scam avoidance advice: The post or comment includes other advice for technical security or avoiding scams not covered by the above codes.

A.7 Types of Personal Information

This category is used to describe the type of information disclosed to a scammer. Includes only that which is explicitly stated to have been given to the scammer.
Unclear: Poster says PI was exposed, but it's unclear what it was.
Name: Person's real legal name, in-part or whole.
Location: Person's address or location, in-part or whole.
Account identifier: Username or other method of identifying the account.
Card number: Credit or debit card number.
Bank account number: Account number for bank.
Bank identifier: Bank name or routing number.
Password: Password to one or more accounts.
OTP: A code used for authentication, usually sent to email or text.
Date of birth: Person's date of birth.
Phone number: Person's phone number.
Email: Person's email.
Non-explicit photo: An identifying photo.
Tax ID: Social security number or other similar tax ID.
Part of tax ID: Part of SSN or other similar tax ID.

Identity documents: ID, passport, social security card, birth certificate or other similar identity documents.
Other information: Other information not covered above.

A.8 Other Comment Types

This category is used to characterize other aspects of comments that do not relate to security/remediation advice for the poster
Deleted: The comment was deleted or removed before collection by PushShift/ArcticShift.
OP: The commenter is the original poster.
Clarification question: The commenter asks a clarification question about the someone’s experience.
Additional detail: Commenter is the original poster, who provides additional detail about their experience.
External resource: User points to an external resource. Includes looking at other posts on the same subreddit. (i.e., website) to provide advice.
Explain scam: The commenter attempts to explain the type of scam and/or its mechanics. Includes cases where they might be wrong. Also includes cases where user just states that situation is a scam without explaining the type. May be paired with "Reassurance. "
Similar experience: Comment provides an example of a similar experience to the scam provided.
Non-OP request for support: Commenter is a person other than original poster who is requesting support.
Reassurance: The comment provides reassurance that poster will be OK or other emotional support.
Chastise: The comment criticizes or makes fun of poster for falling for scam.
Money is gone: The comment tells the poster that their money is gone and recovery is unlikely/impossible. May also be couched as ‘accepting the loss.’
you can DM me: The comment tells the user that they can/should DM the commenter, typically for emotional support.
Automod: Comment is written by the Automoderator. Other codes are not applied to these comments.
Other advice: Commenter provides other advice not related to scam remediation or security/scam avoidance.
Other/irrelevant comment: The comment is not advice and doesn’t fit in any of the other categories. Includes general discussion about scams unrelated to a victim’s experience and off-topic content.