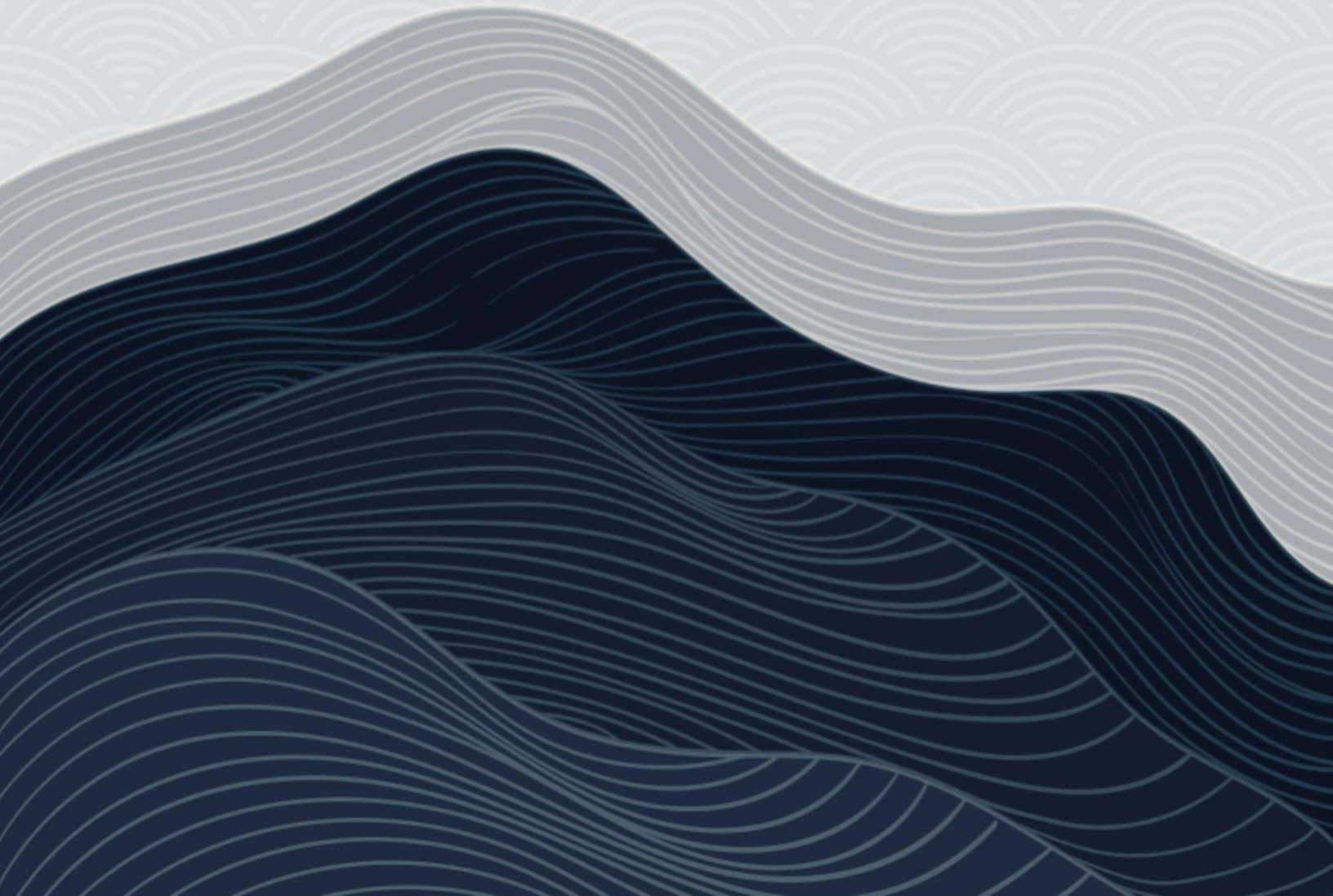
NISOS

Research | March 2023

Catphishing the Catphisher

A Guide for Protecting Vulnerable Populations Online



Executive Summary

Nisos researchers investigated how scammers on social media target and exploit vulnerable populations in an effort to extort money and personal information from victims. The purpose of this report is to better inform individuals and caretakers about common tactics, methods, procedures, and warning signs associated with potential threats.

Criminals most frequently target the elderly, those whose online presence indicates that they may be looking for a relationship, and/or people who appear to be emotionally vulnerable. However, these scammers generally cast a wide net and will engage with all who respond, at least to vet the potential victim's willingness and ability to meet their requests. Anyone can be a victim.

During the course of our investigation, we received numerous flattering messages via social media accounts prior to the scammers asking for significant sums of money. While all of the users of these social media accounts claimed to be US citizens or to live in the United States, we identified the actual location for four of these individuals to be operating from Nigeria and Ghana. Based on similarities in methodology and lexicon, we assert that the others were also similarly located.

Nisos began this investigation with the expectation of it taking weeks or even months to establish a social media presence that would entice scammers to contact us. ***In less than 24 hours after our first social media post, multiple accounts contacted us with flattering language and requests to migrate the conversation to other chat platforms to avoid detection***.

We gathered the examples outlined in this report over the course of four days. This time frame was significantly shorter than initially planned due to the volume of results we collected. This window demonstrates how quickly scammers work to identify and approach users on social media accounts that they deem as potentially vulnerable.

Nisos prepared for this investigation by interviewing victims who had been scammed within the last 18 months. Their feedback helped to identify the following methods of targeting and attack, which we corroborated through our similar experience.

- Using repurposed images from other social media accounts
- Claiming to be working out of the country, while also returning in the near future
- Asking personal questions early in their communications to gauge the susceptibility of a potential victim
- Moving off of social media accounts to other chat platforms where they are less likely to have their accounts removed
- Denying requests or making excuses as to why they are unable to video chat
- Eliciting sympathy from a victim through sad tales about their life
- Copying and pasting generic messages that they likely employ in all their chats with potential victims, usually for long, flattering prose
- Using inconsistent stories, based on their likely numerous chats with other individuals

Note: Many scammers also impersonate US military personnel to gain immediate respect and explain why they are unable to physically visit or regularly chat with their victim.

Recommendations

Nisos researchers expected scammers to conduct unsolicited outreach in the course of our investigation. However, vulnerable populations who experience the same deluge of contact and solicitation for money are often not prepared for, or aware of, the risks involved with online communication. People looking for connections and friends online, and people who may have limited technological literacy, may be susceptible to becoming easy targets.

To avoid becoming a victim of a social media scam, Nisos recommends the following best practices when operating a social media account:

- Increase privacy settings on all social media accounts so that personal information — such as a date of birth, photos, friends lists, and posts — is not publicly available.
- Do not friend or accept friend requests from individuals that you do not know in person and with whom you have not confirmed to be the actual user of that account.
- Avoid pivoting to alternate social media or chat platforms when an individual claims to be unable to reliably use the platform on which they first reached out.
- Immediately block and report any accounts who are attempting to steal money or other information.
- If you or someone you care for are in communication with individuals who appear suspicious, refer to the information in this report that identifies the methodology used by scammers to help determine if you may be interacting with a scammer.
- Report incidents to the authorities as well as elder abuse hotlines, whose state-specific resources can be found here.

Analyst Note

Through the course of our investigation, Nisos researchers did not forget that the users of these scammer accounts and their potential victims are real people. We sympathize with those, particularly in vulnerable populations, who rely on online communications and relationships to stave off feelings of loneliness and who may be willing to place increased trust in individuals they meet online. We hope that our efforts can help populations who have been consistently victimized, and their caretakers, to identify warning signs.

Overview

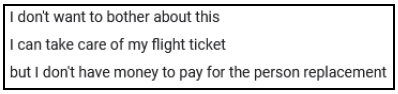
Nisos researchers established an online presence that mirrored common attributes of individuals targeted in romance scams. Our profile represented a woman in her sixties who shared her date of birth and indicated that she was widowed. To a scammer, the victim's status as a widow can stereotypically mean the victim is lonely but may have financial stability through their or their late spouse's previous employment or life insurance policies. Access to the victim's full birthday provides additional personally identifiable information that the scammer may be able to use to identify financial or other accounts. This data point is particularly valuable in conjunction with any additional information from the victim they elicit through the course of their discussions.

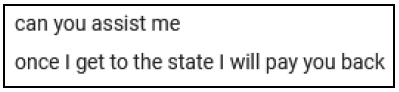
On 6 February 2023, Nisos researchers first began joining online communities dedicated to senior singles and dating. We intentionally joined communities associated with US-based dating and not internationally-focused groups, as most scammers pretend to be US citizens. We also joined multiple communities that support US veterans because scammers tend to identify and exploit seniors in these types of groups.[1] [2] This is likely because they recognize that these supporters may be empathetic to individuals who have suffered in some capacity and also have some level of financial flexibility they will put towards causes or individuals they care about.

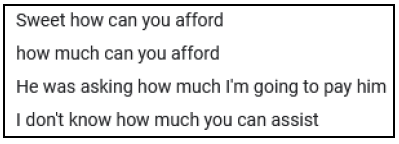
Scamming Methodology

Before our investigation, Nisos researchers had an informed understanding of what to expect during the course of research. Discussions with victims of these types of scams over the course of over a year-and-a-half helped to target key actions commonly performed by romance scammers.

The ultimate goal of romance scammers is to obtain money from victims. The request for money generally comes soon after establishing a relationship with the victim, when the scammer has determined that the victim likely would be amenable to requests. During the process of building a relationship, the scammer will generally incorporate most, if not all, of the aspects listed below in their methodology to achieve a successful outcome.

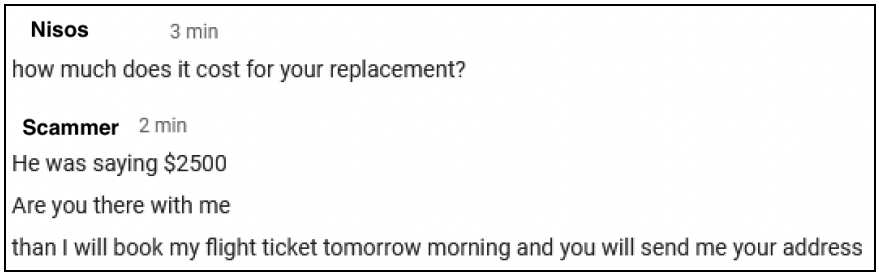


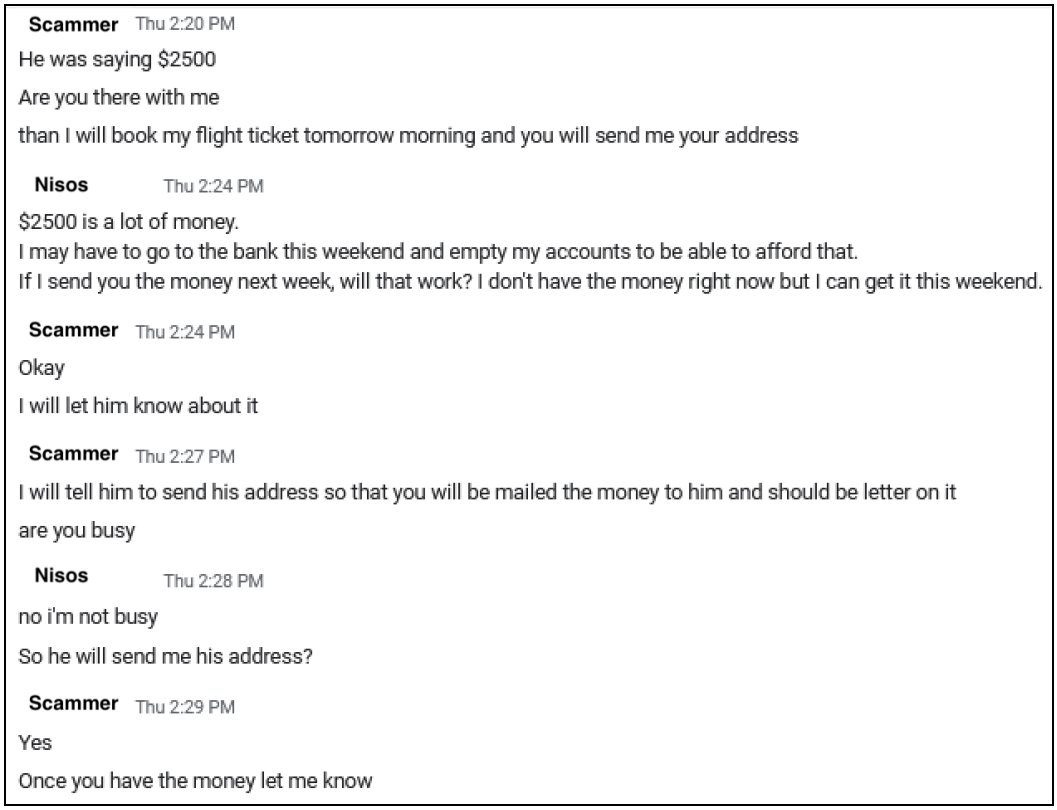




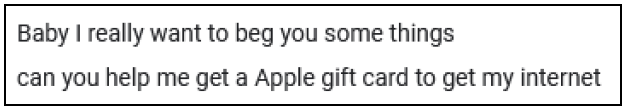
Graphics 1 - 3: Examples of requests for financial assistance by scammers.

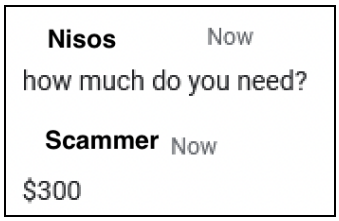
[1] https://southportseniorliving[.]com/blog/avoid-these-scams-targeting-veterans/
[2] https://www.aura[.]com/learn/veteran-scams





Graphics 4 and 5: Examples of requests for significant funds by mail.



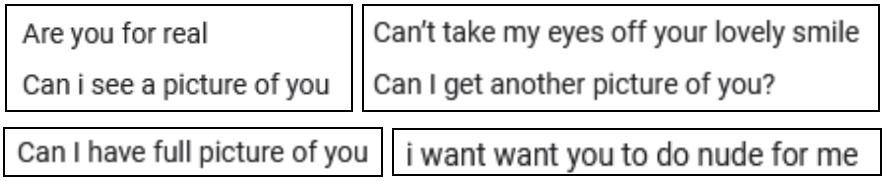


Graphics 6 and 7: Examples of typical asks for gift card assistance.

Repurposed Images

On 7 February — less than 24 hours after our account's initial activity — we received a connection request. Based on its first posts, this profile likely was created on 5 February. The profile used pictures found on other fake social media accounts. Scammers prefer these particular images because they are able to acquire multiple pictures of the same individual, enabling them to send additional images as "proof" of being a real individual. Scammers know that having multiple images of someone can convince victims they are talking to a real person. Conversely, they will regularly ask their potential victims for multiple photos — including custom or explicit photos — in order to determine that they are not talking to another scammer or law enforcement.

We also encountered scammers who shared photos of homes while claiming to be the owner. In one example, the scammer stated they owned a home in Texas, while reverse image searches identified that the home was located in France.

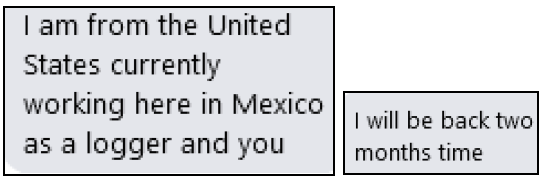


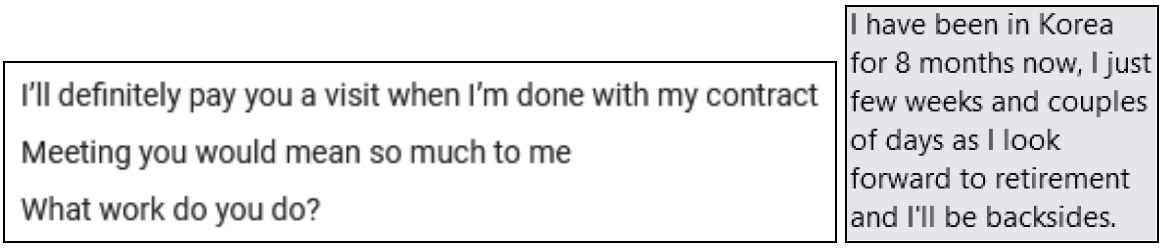
Graphics 8 - 11: Examples of a scam account requesting photos to verify that we are legitimate users.

Working Out of the United States

In most fraudulent situations, scammers will craft a story that makes them currently unavailable but leaves hope they will eventually be accessible to their victim. For example, many of these individuals will claim that they are working out of the country or are military personnel deployed overseas, but who will return in only a matter of weeks. This also provides plausible scenarios where the scammer experiences an issue in their attempts to return home and can request financial support from their victim.

During the course of our research, three accounts that reached out to our profile claimed that they were US citizens who were working as a logger in Mexico, on an oil-rig in Romania, and as a military officer stationed in South Korea. In all cases, the contracts for these individuals were ending within two to three months, making the anticipation of their return and their ability to come and marry our persona close enough in the future to motivate continued communication and planning.



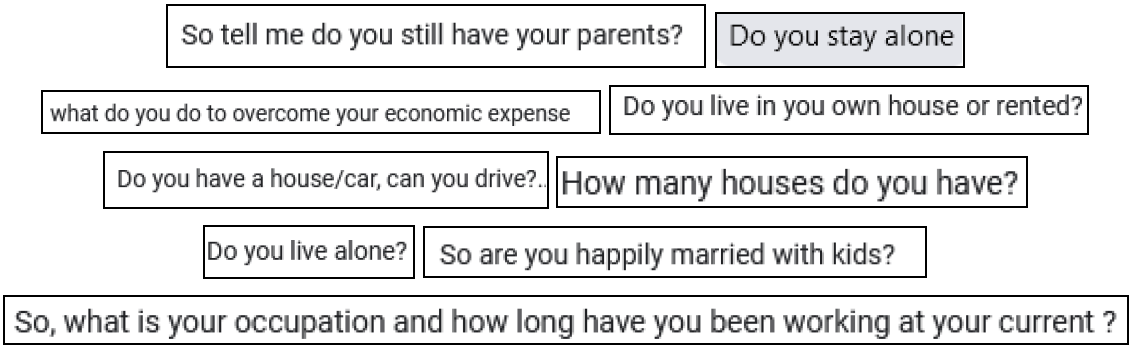


Graphics 12 - 16: Examples of cover stories provided by scammers.

Cursory Vetting

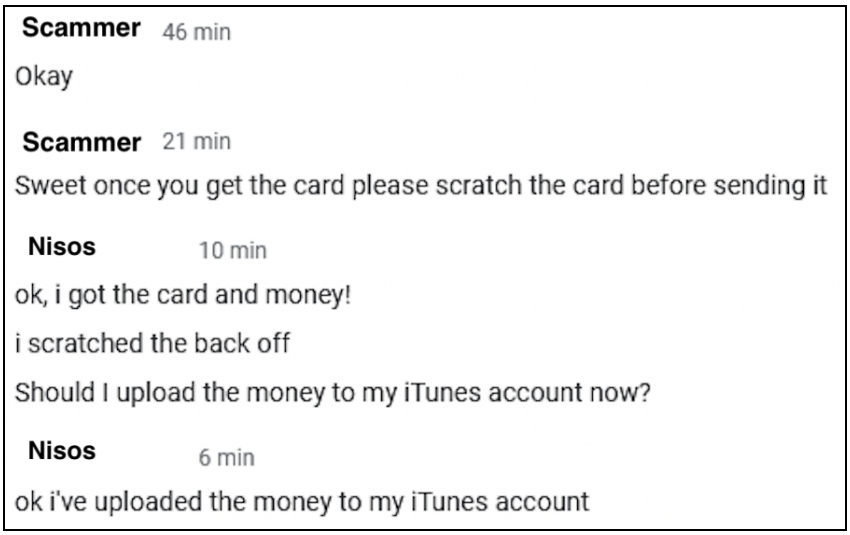
One of the most important parts of a scammer's process is to identify potential victims, which involves vetting their new contacts. Almost immediately, the scammer will ask qualifying questions such as: if they are financially stable, if they live alone or have family close by, and if they own a home or a vehicle. Other questions are used to solicit basic information about a victim, such as the names of their pets or other family members. This information can be helpful to a scammer, as many people use these names as passwords on their accounts.

Throughout this vetting process, the scammer will develop a better understanding of the likelihood that this potential victim could be willing and able to send money. These questions also help the scammer scope their requests to the victim. For example, one scammer asked us if we owned a car and could drive. By responding in the affirmative, they then requested we travel to Walmart to purchase Steam, iTunes, and Apple gift cards for them to use that money to improve their internet connection.



Graphics 17 - 25: Examples of vetting questions presented early after talking with scammers.

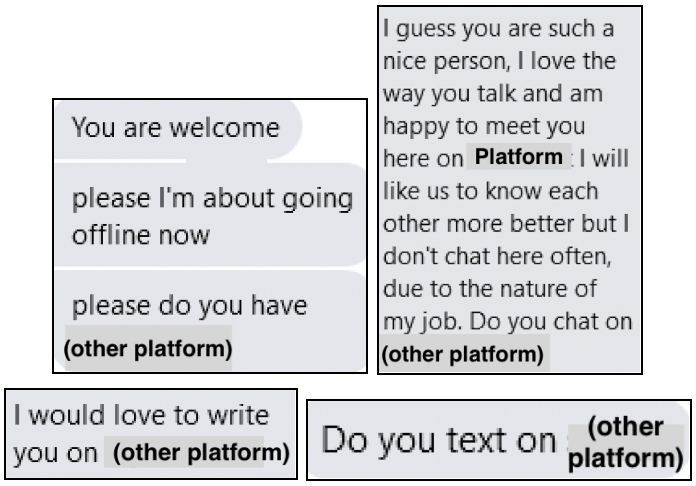
Once a scammer identifies a potential victim as a good candidate who will respond to their asks, the scammers persistently pursue the individual, increasing their requests. The scammers will likely show patience with errors rather than move on. For example, when our persona pretended to respond to a scammer's request to get gift cards from Walmart, we acted as if we had uploaded the money to our own personal account, thinking it was what the scammer wanted. Rather than determine that we were someone unable to meet the technological needs required to assist in money transfers, the scammer let us know very strongly that this was incorrect. Instead of moving on to another victim who demonstrated more aptitude for following directions, the scammer instead sent us a bitcoin address, two bank accounts, and two alternative mailing addresses in the US — likely attributed to other victims — for us to attempt additional financial transactions.



Graphic 26: Example of pretending to attempt to follow instructions in purchasing a gift card.

Moving to External Chat Platforms

While some scam accounts have existed for many months or even years, others do not last as long. This is likely because each social media platform's internal monitoring mechanisms identify these accounts as scams and remove them, or because a potential victim who became wise to the scam reported the account as fraudulent. Because of their unpredictable lifespan on social media, scammers will often request to move to alternate chat platforms. By moving a victim off of social media and gaining their personal email address in this process, the scammer is able to continue contact with a victim even if their social media account is removed.



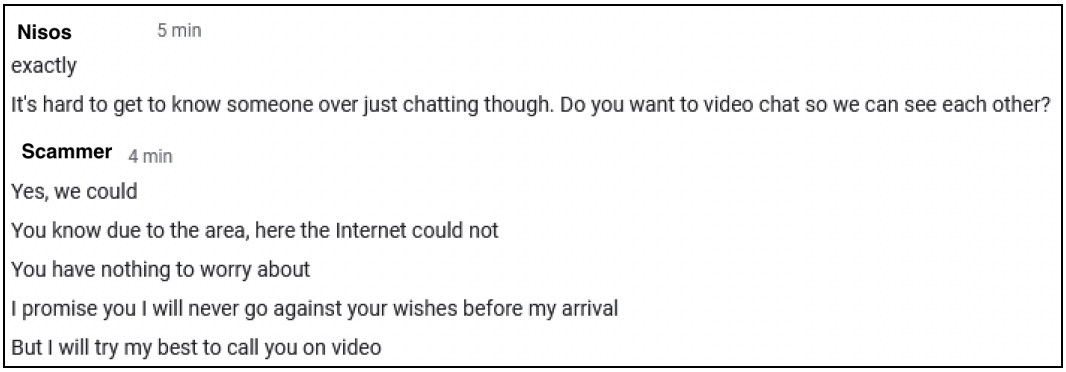
Graphics 27 - 30: Examples of scammers who requested within the first few interactions to move to other chatting platforms.

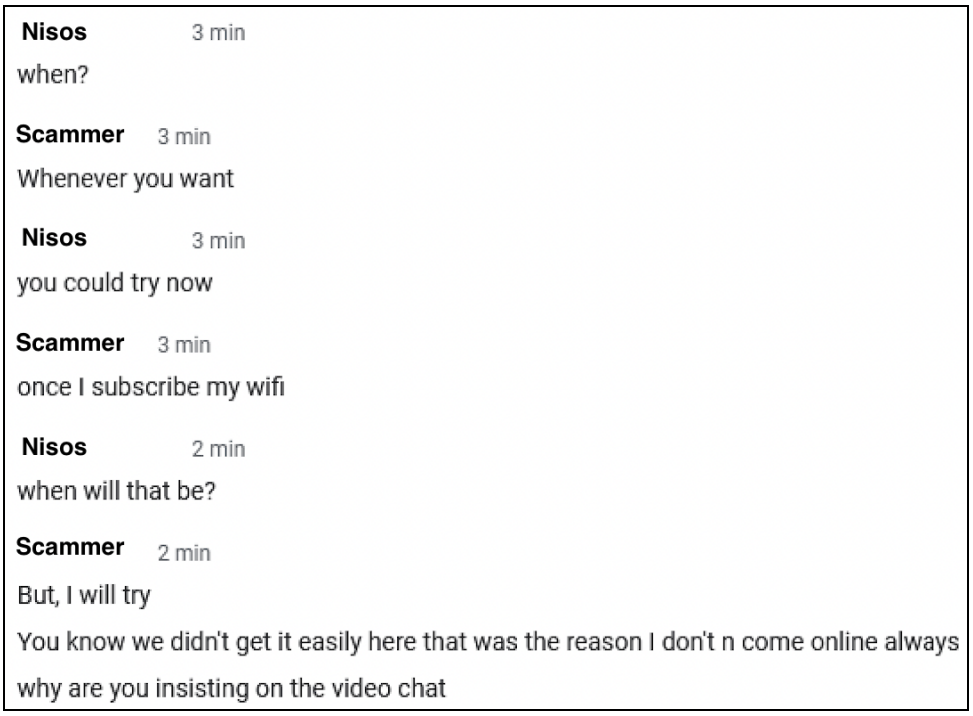
Some of the suitors also offered to send links to these alternative chat platforms. Although this was most likely to help non-technologically proficient victims find the correct platform, some scammers may have installed nefarious programs or malware into the links as well.

Graphic 31: Example of account offering to send a link to download an alternative chatting platform.

Inability to Video Chat

Often related to the scammer's story is that they are currently working out of the country and are reliant on unstable internet connections. Scammers will claim to be unable to video chat with their victims. This is, of course, because they look nothing like, or are located nowhere near, what they have claimed.

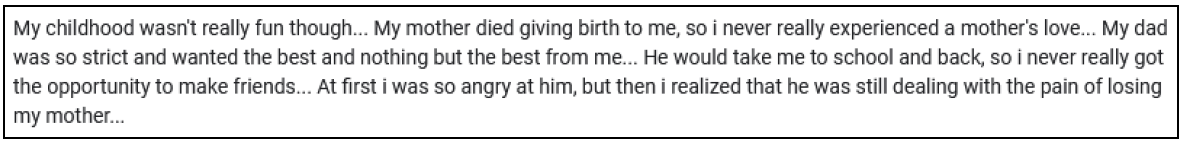




Graphics 32 and 33: Example of explaining why they are unable to video chat.

Attempts to Elicit Sympathy

The users of scam accounts regularly implement sad stories to gain the sympathy and trust of their victims. These stories are often used to gauge the sensibilities and susceptibilities of a victim, strengthen the relationship, and are frequently used in a scenario to directly solicit money to support the scammer in overcoming that difficulty.



Graphic 34: Example of sad story presented by scammer.

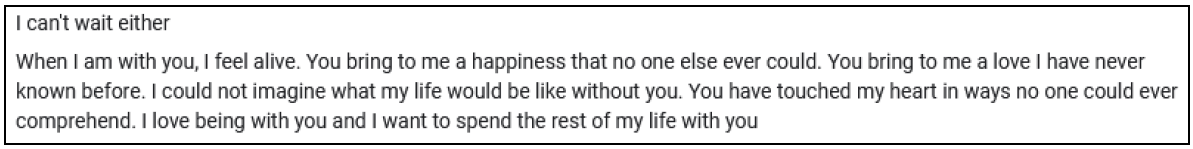
Copying and Pasting

One of the biggest red flags we observe in foreign-scammer messages are significant grammatical errors. Throughout our discussions with previous victims and through the course of our research, we identified that the majority of scammers implemented passable English but struggled to quickly type messages and often used poor grammar and spelling.

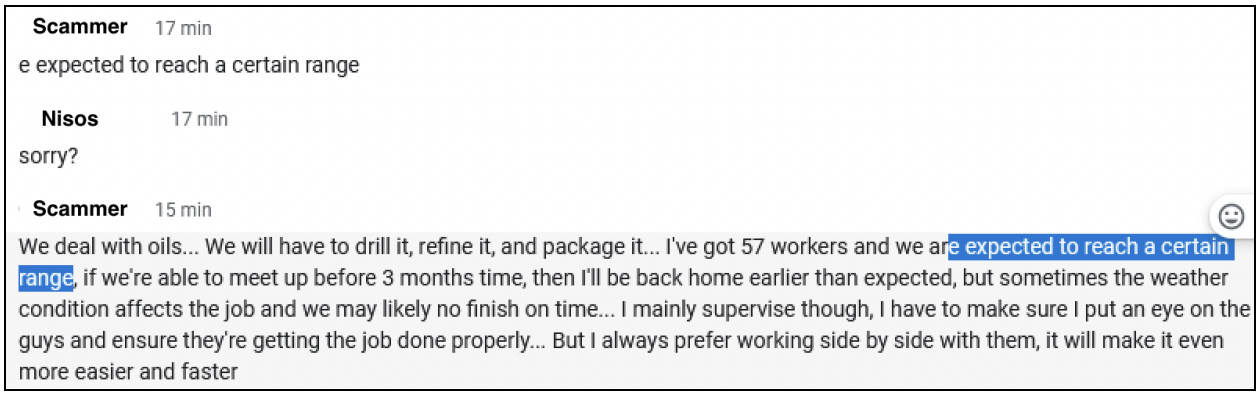
As scammers are regularly chatting with many potential victims at any time, they likely implement the same phrases, stories, and flattery across each to help standardize their work and increase their efficiency. As such, we identified multiple instances where scammers were clearly copying and pasting

text either from other chats or from some sort of master list of comments they use. Some of these comments included long sentences or paragraphs that were posted almost immediately following a previous comment and were usually general, affectionate language that they could use across many accounts.

We also identified an instance where a scammer accidentally only pasted a short middle snippet of one of its standardized messages, and quickly turned around to paste the full message shortly thereafter.



Graphic 35: Example of a long message posted almost immediately after the first line.



Graphic 36: Example of mistake in scammer's copying and pasting, which they corrected with the full message two minutes afterwards.

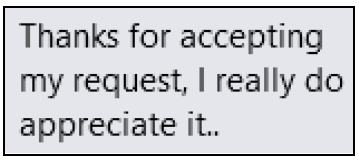
Inconsistent Stories

Many scammers adequately generate and sustain backstories for use with a specific victim. However, many others are attempting to make money as quickly as possible and are chatting with multiple potential victims. As such, details in their stories can change.

During our investigation, we sent an email to an address that we identified through our discussions with past victims. This email address has been involved in scamming for at least the past 18 months and likely even longer. From our newly created email address, we sent a message saying that we missed talking with the individual and that we should catch up again. Even though this email address and persona were accounts with which the scammer had not previously communicated, they immediately emailed back and jumped into the conversation as if we were old friends. This likely indicates that the scammers are contacting so many people that they are usually unable to keep track of all specifics and did not find it worthwhile to validate if we were a previous contact.

We also connected with multiple imposter accounts (identified by our interviewees) to reveal how the scammer would react when a potential victim initiated contact. After connecting with the imposter accounts, we waited for them to send the first message. In one instance, an account to which we had sent the connection request almost immediately messaged us back and thanked us for accepting their

request, suggesting that this account regularly sends out bulk requests and adds all individuals it can without validating the individual connections.



Graphic 37: Example of account we sent a connection request to thanking us for accepting their request.

Military Impersonation

Nisos researchers interacted with multiple social media profiles posing as US military personnel deployed overseas. Impersonating US military personnel is a popular scammer technique, as it can elicit immediate trust and respect from a potential victim. It also provides a satisfactory story as to why the victim is not able to video chat or meet in person with the scammer.

Nisos researchers connected with 10 accounts posing as deployed US military personnel who had all posted on social media within the last couple of weeks.[3] Almost immediately, five of those accounts accepted our request and began to carry out the similar scam methodologies we outlined above. We note that one military imposter account that requested we connect with them had a username that did not match the profile name, suggesting that this social media account likely previously portrayed a different individual and was repurposed to pose as a US soldier.

Actual Locations

Nisos researchers identified the locations of multiple scammers, all of whom claimed to be in other locations and were impersonating US citizens. Many of these scammers promised a lifetime of romance and financial protection at a mansion to entice the victim to send money and wait for the suitor to return from their work opportunities abroad. In reality, these scammers are most often located in foreign countries, particularly in Africa.

After accepting friend requests from these potential suitors who claimed to be US citizens, friends recommended by social media platforms were subsequently almost exclusively Nigeria-based individuals. This suggests that these accounts were likely repurposed into fraudulent profiles. We suspect that the underlying metadata available to these social media platforms — including IP addresses or other locational information — predetermined that the user was based in Nigeria. This likely prompted the social media platforms to suggest additional Nigeria-based accounts to us following our direct connection with these scammers.

[3] Nisos reported these accounts to the appropriate administrators and authorities, in line with these findings.

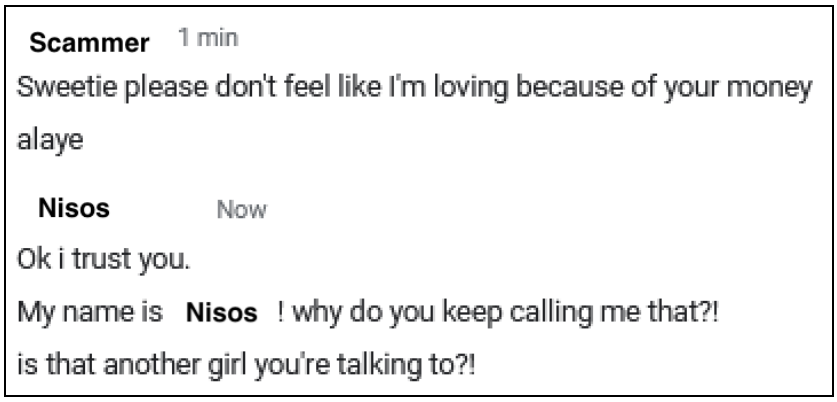
Nigeria

Case Study 1

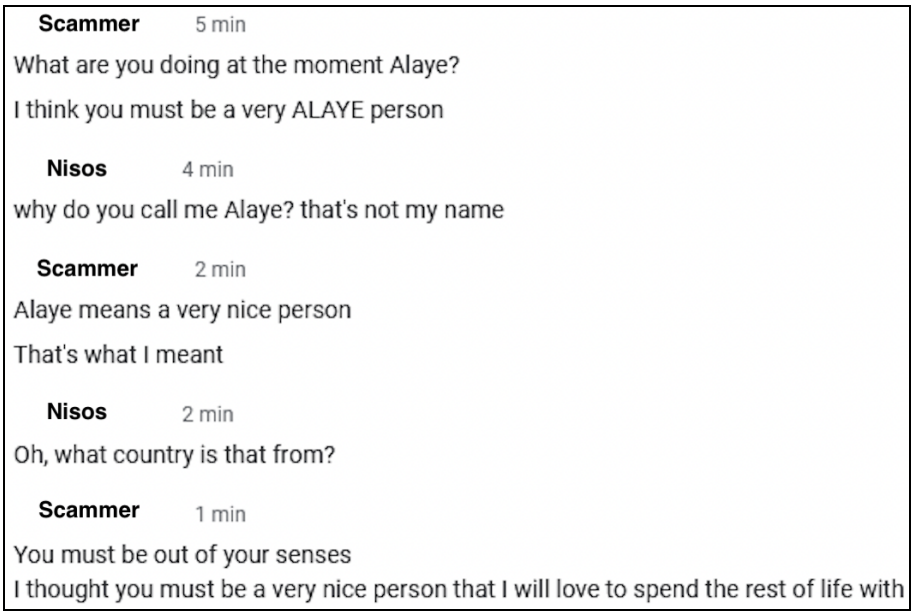
A scammer who initiated conversation with our account within 24 hours of its creation promised eternal romance after just a few messages back and forth. The scammer claimed that they were a logger originally from California who was currently working in Mexico. Their contract was allegedly ending in two months, but because they were so excited to meet us, they wanted us to send them money so that they could pay another worker $2,500 to take the rest of their shifts. Nisos tradecraft identified that the user's IP address was associated with a service provider in Nigeria.

Case Study 2

We identified the user of an account posing as a US military member stationed in South Korea actually located in Nigeria using an IP address associated with another service provider. Throughout our conversation, the scammer used multiple terms that also helped to confirm that they were located in Nigeria. At least three times they referred to us as 'Alaye'. This is a Yoruba language term meaning "younger brother" adopted by Nigerian scammers to identify their own kind to know if they have been speaking to another scammer.[4] When this word was used by the scammer, we accused them of having another girlfriend named Alaye who they were also messaging. This caused the scammer to go on the defensive, convincing them that we did not recognize this term, which allowed for our conversations and their solicitations for money to continue.



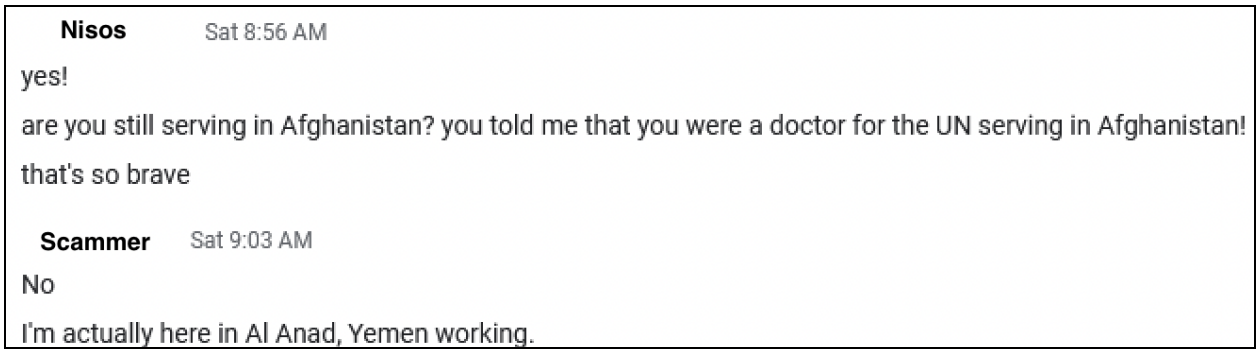
[4] https://www.dailymail.co[.]uk/femail/real-life/article-10979137/Alaye-word-Nigerian-scammers-use-you.html



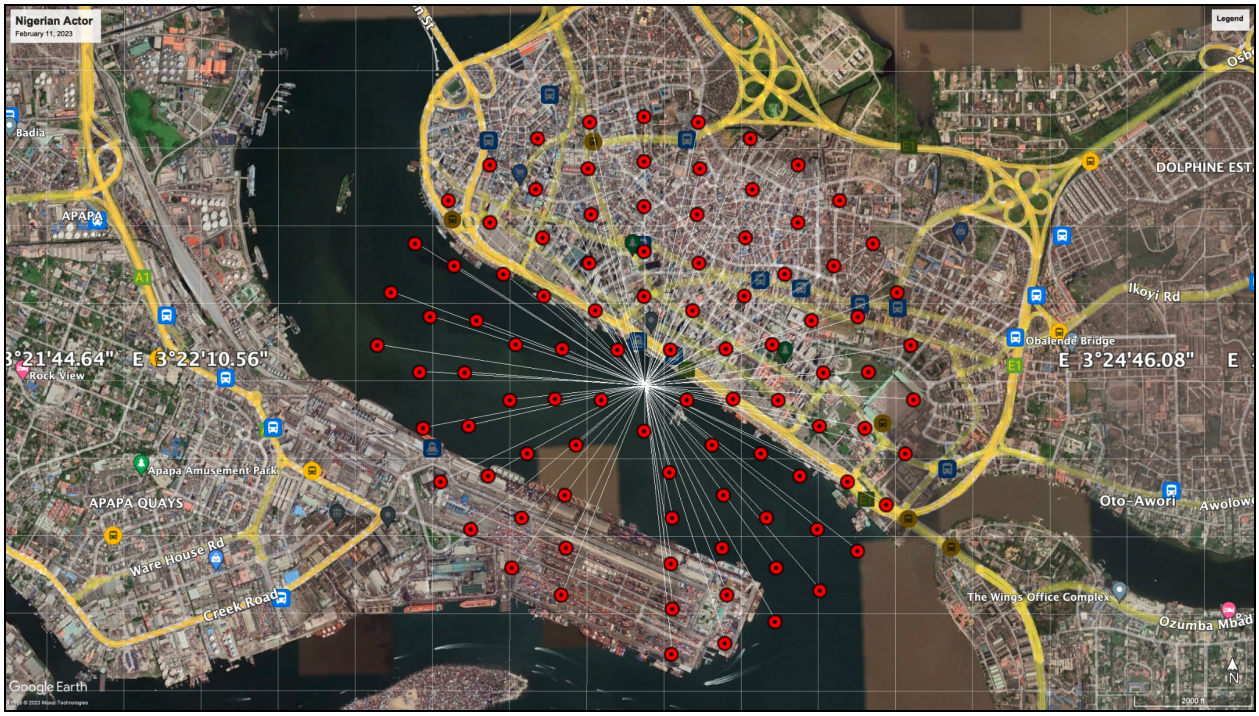
Graphics 38 and 39: Example of scammer referring to us as 'alaye'.

Case Study 3

Nisos researchers initiated conversation with an email account that had solicited information and money from victims roughly 18 months ago. At that time, the email account claimed to be a UN medical doctor from the United States who was serving in Kabul, Afghanistan. In their response to our outreach, the user stated that they were now serving in al-Anad, Yemen. Nisos researchers identified that the account was using an IP address from a service provider in Nigeria. As this email address had been used in scams since at least mid-2021, the user demonstrated increased wariness when conversing with our email address, suggesting that the lack of previous communication with our new email address caused them at least minor concern. However, this did not stop them from communicating with our account.



Graphic 40: Example of email user claiming a new location as a fraudulent UN doctor.



Graphic 41: The scammer was likely located within the Lagos Harbor area at the time of our communication.

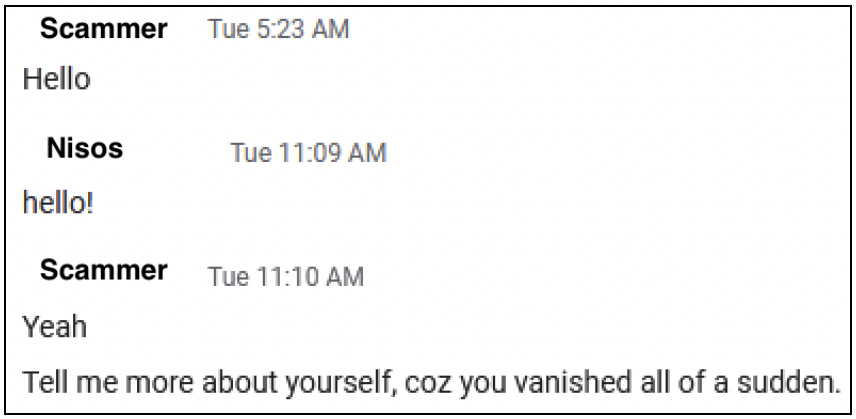
Ghana

Case Study 4

Nisos researchers initiated contact with an email address used to conduct romance scams since at least August 2021. Although we had never had any contact with this individual under our persona's email address and associated social media account, our initial email indicated we had missed chatting with them and hoped to hear from them again soon. Nisos conducted this experiment to determine what level of research rigor or records these scammers kept between their many contacts. Almost immediately, the email address responded indicating that they were happy to hear from us again. The user quickly dove into their usual process for flattering and acquiring a potential victim.

The user of this account claimed to be from Copenhagen, Denmark, but said that he primarily lived in Wichita Falls, TX. During our chats, the user claimed to be working at an oil rig in Romania. Nisos was able to identify that the user was actually located in Ghana and using an IP associated with a provider there.

As this scammer had been using this same email for scams for at least 18 months, the user's practices and successful techniques were well-established. Nisos researchers found that sites accessed by the scammer's IP address within the hour that their IP was identified portrayed the scammer as experienced in their craft. Multiple sites were associated with crafting fake images and videos as well as chatting applications that the user likely sends to their victims to request additional engagement .



Graphic 42: Initial response by the scammer after falsely telling them we had previously chatted before.

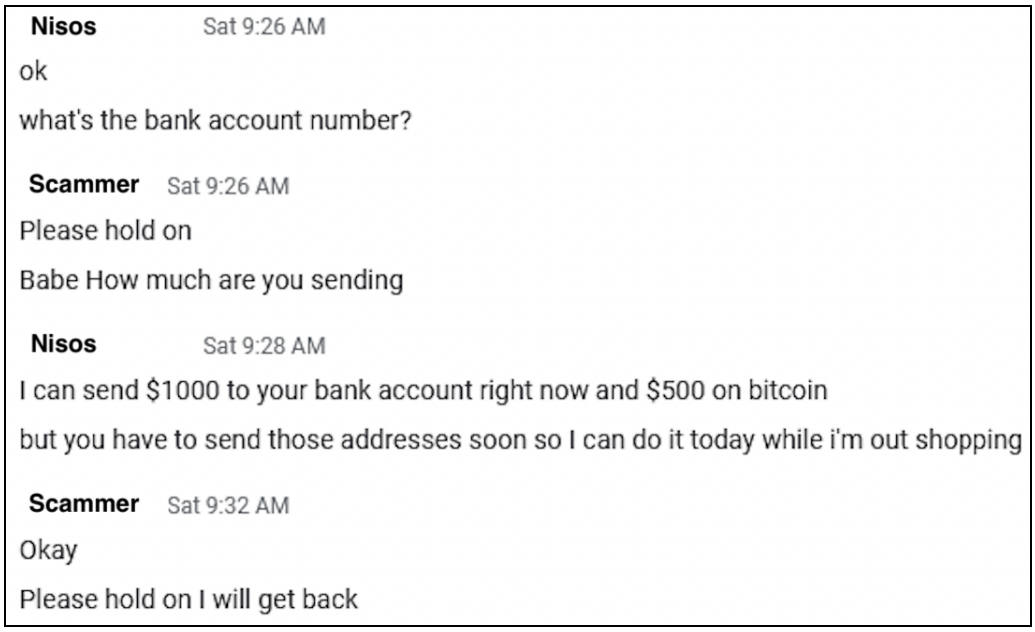
Wider Scamming Network

Many scammers work within larger networks when conducting a scheme. By utilizing a wide range of fraudulent social media profiles and accounts, scammers are able to work together to establish a network of social media accounts and money moving vehicles that support one another. Through the course of our interactions with the first fraudulent account that reached out in less than 24 hours, we solicited significant information that offered insight into the larger network and organization involved in its scamming operations.

Working in Teams

Nisos identified indicators that multiple individuals were simultaneously running a single account conversing with our profile. Nisos tradecraft revealed that at least two separate operating systems accessed a specific URL provided only to this contact within moments of each other. This suggests that multiple individuals involved in some sort of delegation of responsibilities took an interest in the page, likely in order to craft the appropriate response back to our persona.

Multiple times throughout our conversation with the scammer — who ultimately provided multiple physical addresses, a bitcoin address, and two bank accounts — we were told to wait as they obtained that information. These were likely moments when the scammer was conversing with other members of their network to obtain additional account information that could be passed to us.



Graphic 43: Example of scammer likely conferring with others in their network for usable contact information.

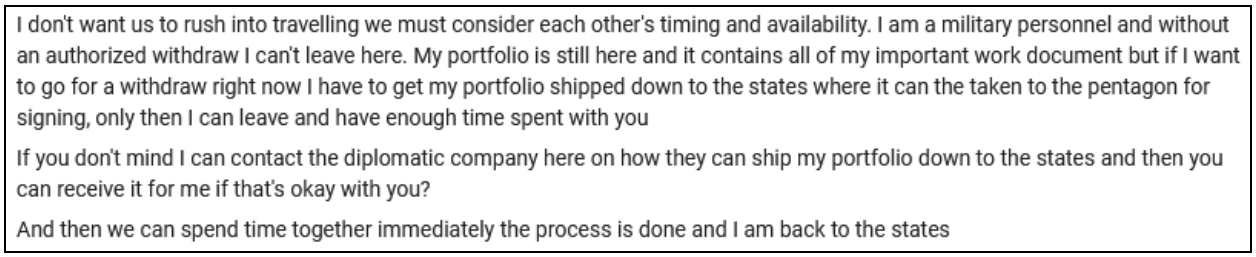
Victims as Money Mules

After an account quickly established itself as our romantic partner and they expressed a desire to end their working contract early and join us, the scammer requested $2,500 be sent to a P.O. Box in Iowa. According to the scammer, this money would be used to pay the worker who was going to finish out the scammer's contract. Nisos researched the P.O. Box and confirmed it to be associated with the name the scammer provided.

However, the person's name and the P.O. Box belonged to a woman in her seventies whom we assess to be a separate victim of the scammer or the wider scamming network. When Nisos researchers pretended to have issues at the post office sending money to that address, the scammer provided an alternate physical mailing address in California, which is likely also attributable to another victim. Nisos made multiple attempts to contact the victims but did not receive a response as of the time of publishing. While the scammer requested that we send $2,500 to this account to pay off an alleged work replacement, the woman who owned the P.O. Box likely was provided a different story to explain a pending shipment of cash. For example, a possible scenario would be the scammer telling the woman that they were having issues with their bank and would send cash to her so that she could use it to purchase gift cards. These gift card codes could then be sent to the scammer for them to redeem. While the victim would see themselves as being helpful to someone they trust, these additional steps ensnare innocent victims as unwitting money mules in this process.

Nisos researchers likely experienced being on the receiving end of this scheme when an account requested that we receive their "diplomatic portfolio" because they needed to have it shipped to the United States and taken to the Pentagon. In this instance, we possibly were intended as a recipient

address for another victim to send money while also being tasked to send $5,000 to the scammer to facilitate the shipment.



Graphics 44 and 45: Request by scam account for us to pay for and receive a package.

Bitcoin and Bank Addresses

While our fraudulent suitors preferred to launder their money through means that would be less traceable and detectable to fraud monitoring — such as sending payments of cash through the mail for other victims to exchange for gift cards — scamming networks also implement other methods to maximize potential profits. Through the course of our investigation, Nisos researchers were able to gain the trust of a scammer enough to receive additional contact information from them.

Nisos researchers obtained a bitcoin address, a partial bank account, as well as the complete information for an additional bank account from the scammer as alternative means for us to send money. The scammer's bitcoin address received funds from multiple accounts, including a transaction worth over $3,500 in December 2022. That same month, the bitcoin address sent nearly the same monetary value to other bitcoin addresses, likely indicating it is only a link in a chain of associated accounts used to obscure these transactions.

Although the scammer was located in Nigeria, the bank information provided belonged to what were most likely an Ethiopian name and Russian-Caucasus name with accounts located in Turkey. We were unable to verify if the accounts provided belonged to the scammers themselves or if they belonged to additional victims who would be provided alternative stories and used to eventually send funds to the scammer.

Scammer 4 min

My agent said you should send the money through machine

Bitcoin machine

Nisos 3 min

ok i can do that!

Scammer 3 min

That will be better

Definitely you will add more money to the flight tickets so that I can get my internet

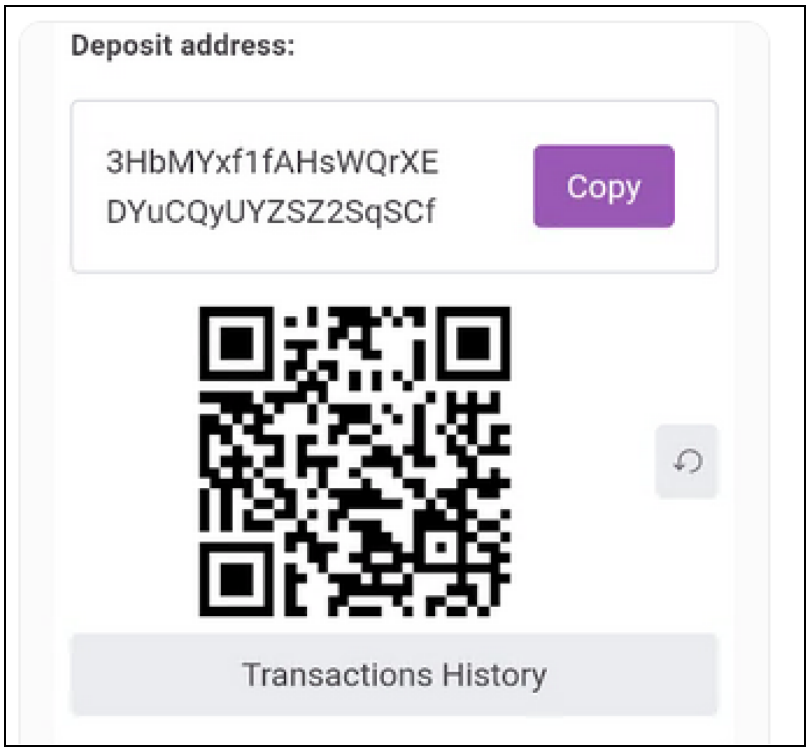
Nisos 1 min

yes!

UNREAD

Scammer Now

He said the money for the flight tickets is $1100

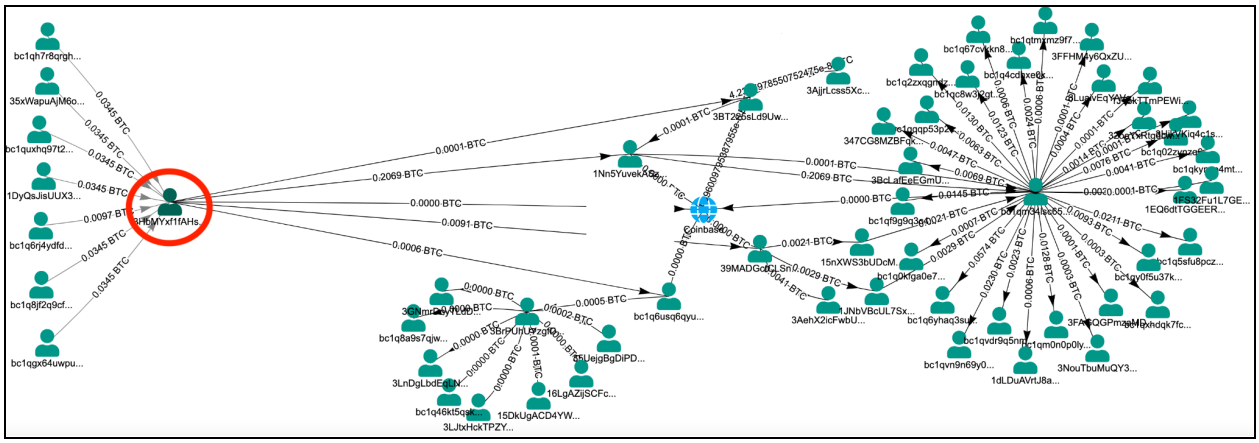


Graphics 46 and 47: Bitcoin address provided by scammer following our "failed" attempt to send gift card codes.

Timestamp	Block	Amount
2022-12-23 21:35:04	768679	0.20696021 BTC $3478.22
2022-12-01 15:28:11	765483	0.00969469 BTC $165.72

Timestamp	Block	Amount
2022-12-29 17:05:39	769441	0.0097 BTC $161.23
2022-12-24 02:22:14	768697	0.2070 BTC $3480.63

Graphics 48 and 49: Examples of inflow (top) and outflow (bottom) of currency to the bitcoin address in December 2022. [5] [6]



Graphic 50: Graph demonstrating the flow of cryptocurrency received by the scammer-provided address to other central accounts that then further distribute the money. [7]

Conclusion

Online scammers target seemingly vulnerable individuals to steal money and information. Scammers move quickly to identify, vet, and make requests from their targets as evidenced by our research. It is critical for vulnerable people and their caregivers to remain vigilant when new connections are made online. Nisos' methodology and research from victim interviews points to the prevalence and acceleration of this type of fraud. As discovered in this research, scammers may be working in concert with a network of other scammers to increase their profits and to reduce the costs of engaging authentically or in a bespoke manner with individual targets. The inclusion of AI tools in image and text generation is also a point of note to be considered as language barriers are reduced and ways to obfuscate true identities becomes easier. Regrettably, the damages to victims aren't limited to finances, but can cause further emotional duress and loneliness.

[5] https://explorer.bitquery[.]io/bitcoin/address/3HbMYxf1fAHsWQrXEDYuCQyUYZSZ2SqSCf/inflow?from=2022-10-01&till=2023-02-13
[6] https://explorer.bitquery[.]io/bitcoin/address/3HbMYxf1fAHsWQrXEDYuCQyUYZSZ2SqSCf/outflow?from=2022-10-01&till=2023-02-13
[7] https://explorer.bitquery[.]io/bitcoin/address/3HbMYxf1fAHsWQrXEDYuCQyUYZSZ2SqSCf/graph?from=2022-10-01&till=2023-02-13

Appendix A: Commonly Used Phrases

Nisos provides the following examples of commonly used tactics and questions by scammers that have been used during their vetting process but also throughout their interactions with a victim. While not comprehensive, this list provides a sampling of questions that individuals may use to help determine whether the person they are engaging with online is who they claim to be or if they may be interacting with a scammer.

Remember, scammers find value in almost all information they can glean from their victims, even if it appears mundane. This information can give them insight into possible usernames or passwords for accounts. If you supply them with photographs, they may use them for blackmail or extortion or as a tool to engage others you may be connected to, such as friends or family. They may also be used to hurt other victims by providing these unique photos of a "real" person to that new victim. All information provided to scammers helps them identify specific ways to manipulate a victim and will help inform the types of stories or claims you might be susceptible to.

Be on the lookout for:
Urgency in obtaining personal information
Impatience or guilt-inducing tactics if you are delayed in responding
Requests to email or message additional accounts with personal information
Requests to send money to their company to fund a leave trip
Demands for receipts alongside sending money
Requests for gift cards
Requests to change social media or chat platforms
Inability to video chat
Attempts to elicit sympathy
Text that appears generic, particularly of a flattering nature or of a background story, that could indicate copying and pasting
Inconsistent details in someone's story
Military impersonators or other individuals claiming to be US citizens working in a foreign country
Use of unfamiliar terms or inconsistent grammar
The presence of images on additional social media accounts with different names - do a reverse Google Image search
Seemingly random questions, such as whether or not you know how to drive or have access to a vehicle

Information valuable to scammers that may not seem risky to provide:	
Family member names, nicknames, and ages	Common valuable assets (i.e. if you own a car)
Names of pets	Income/net worth
Personal images (including explicit or compromising photos)	Technological capabilities (i.e. a bitcoin wallet)
Images of family members	Living status (i.e. proximity to children, roommates)
Any physical address	Information related to your age (i.e. favorite artists)
Email address	Employment status and work experience
Phone number	Former schools and mascots

Appendix B: Additional Unsolicited Contact

Our social media account was involuntarily added to multiple pornographic chat groups throughout our week of activity. Within two days of conducting activities on our profile, it was added to two separate chat groups where links alleged to be associated with pornographic sites were shared. Although we did not engage in these channels, it demonstrates how quickly an unsuspecting account can be involuntarily added to ancillary groups where potentially problematic behavior takes place. At the very least, users may be subject to images and discussions that they are not specifically seeking out. While these specific chat groups did not lead to additional scamming attempts, it shows how easily unsuspecting social media users can be added to groups and chats where scammers can select and interact with potential targets outside of public view. Our account was selected for these chats most likely because of its presence in dating groups.

