F-Secure Scam Kill Chain

A definitive framework for scam tactics and techniques

Reconnaissance	Development	Contact	Persistence	Access	Exfiltrate	Lateral Movement	Monetization
1.1 Manual profiling ○ Personal interests ○ Online accounts	2.1 Acquire infrastructure ○ Email servers ▪ Bulk email service ○ Domains/website ○ Cloud resources ▪ Content delivery networks (CDNs) ▪ Tunneling ○ C2 server ○ Phone numbers ▪ VoIP ▪ SIM/eSIM cards ○ Infrastructure for malware	3.1 Email	4.1 Erase virtual presence	5.1 Victims share information on their own ○ Over the phone ○ Email ○ Messaging platforms ○ Phishing pages	6.1 C2 channel ○ Web server ○ Cloud-based ○ Messengers	7.1 Spread to victim's contacts ○ SMS ○ Social media ▪ Posts ▪ Comments ▪ Direct messages ○ Email	8.1 Direct transfer of funds ○ Bank transfers ○ Cryptocurrency ○ P2P payment
1.2 Automated scraping ○ Web scraping ○ Social media	2.2 Software development ○ Custom malware ○ Website development ○ Bots ○ Automated scripts ▪ Victim-side scripts ▪ Adversary-side scripts	3.2 Phone calls	4.2 Cultivating trust ○ Genuine small payments ○ Psychological manipulation	5.2 Victims' information stolen with malware ○ Mobile malware ○ Computer malware	6.2 Direct access to victim's device or account ○ Screen sharing software ○ Email forwarders	7.2 Compromise victim's other online accounts ○ Password reset ○ Linked accounts ○ Single Sign-On (SSO)	8.2 Investment scheme ○ Rug pull ○ Ponzi scheme
1.3 Phishing for information ○ Phone calls/vishing ○ Emails ○ Smishing ○ Social media and instant messaging ○ Websites	2.3 Acquire services ○ Human personnel ○ 'XYZ'-as-a-Service ▪ Phishing-as-a-Service ▪ Malware-as-a-Service	3.3 SMS	4.3 Change medium	5.3 Attacks with no interaction with the victim ○ Sim-swapping ○ Enterprise-level data breach		7.3 Leverage victim's access rights ○ Admin access on social media ○ Financial information	8.3 Sale of stolen data ○ General sale ○ Specific sale
1.4 Purchase from closed sources ○ Illegal marketplaces ○ People search databases ○ Insider help	2.4 Create accounts ○ Social media ○ Email accounts ○ Cryptocurrency wallets ○ Messengers ○ Fake legitimacy	3.4 Social media ○ Adversary-driven communication ○ Victim-driven discovery					8.4 Identity theft for further benefits ○ Taking a loan in victim's name ○ Purchase of non-liquid assets
	2.5 Develop the bait ○ SMS ○ Email ○ Content for websites ○ Human-language script • Direct messaging • Commenting • Phone call ○ Advertisements ○ Mobile apps ○ SEO poisoning ○ URL manipulation ▪ QR codes ▪ URL shortener	3.5 Search engines					8.5 Cryptocurrency mining
	2.6 Algorithmic manipulation ○ Advertisements ○ SEO poisoning ○ Misleading content	3.6 Online services					8.6 Gains (financial and non-financial) via virtual assets ○ legitimate online service or a game ○ Online gift cards
		3.7 Mimicking legitimate companies or services ○ Websites ○ Mobile apps ○ Fake online accounts					
		3.8 Messengers					

Stage 1: Reconnaissance

In the Reconnaissance tactic, the scammer gathers information about potential victims to use in later stages of the scam. This phase involves both identifying victims and collecting their personal data for future exploitation. The scammer's goal is to identify as many victims as possible – or a more targeted group – and gather extensive information about them. Techniques may include manually collecting details from social media (e.g. name, address, and interests), using automated data collection, phishing via SMS and phone calls, or purchasing personal data from illicit sources, such as illegal marketplaces on the internet.

1.1 Manual profiling

An adversary may gather information about potential victims to build detailed profiles. These profiles can help identify individuals more likely to fall for scams and inform the scammers' choice of modus operandi.

- **Personal interests** – Adversaries may leverage victims' personal interests when building profiles. Factors such as contact networks, location, nationality, political inclinations, religious beliefs, hobbies, and sexual orientation are often used in profiling by adversaries to develop targeted scamming strategies.
- **Online accounts** – Adversaries may profile potential victims based on the websites where they hold accounts. Having accounts on specific platforms often reveals a victim's interest in the services those websites offer. For example, an account on a dating website suggests an interest in dating or browsing profiles.

1.2 Automated scraping

To acquire the personal details of victims, adversaries may pilfer online resources by scraping large volumes of raw data that can be filtered and refined to the desired level of detail. Scraping can target a variety of online platforms, each yielding different types of information.

- **Web scraping** – Adversaries may use web scraping to gather personal information about victims. This can involve targeting a predefined list of names to collect additional details or scraping data to generate a new list of potential victims. In either case, the goal is to obtain more information that can be misused in various ways, such as creating fake social media profiles or applying for loans in the victim's name.
- **Social media** – Adversaries may exploit social media to gather additional data about potential victims, including photos, videos, voice recordings, and personal information such as relationship status. This information can be used to create fake online identities.

1.3 Phishing for information

A highly popular technique used by adversaries to access victims' sensitive information is 'phishing for information', which involves contacting a large set of potential victims – similar to casting a wide fishing net – in the hope of obtaining personal information from a few individuals.

- **Phone calls (aka vishing)** – Adversaries may place fake calls to victims (or have the victims call them) to trick them into revealing sensitive information, such as their name, address, credentials, or credit card number.
- **Emails** – Adversaries may send direct links or email attachments containing fraudulent links to steal sensitive user information. They may also send emails that create a sense of urgency, tricking the user into calling a phone number and divulging sensitive details.
- **SMS (aka smishing)** – Adversaries may send phishing SMS messages to trick users into sharing personal or financial information, typically by clicking on malicious links.
- **Social media and instant messaging** – Adversaries may contact victims directly via social media or instant messaging platforms to gather information, such as phone numbers and email addresses, or to send malicious links that lead to sites designed to steal information or host malware.
- **Websites** – Adversaries may use fake links to trick victims into revealing sensitive information. Victims can be exposed to these malicious sites through ad popups, social media messages, and other means.

1.4 Purchase from closed sources

Adversaries may purchase victim data from closed sources for use in later targeting.

- **Illegal marketplaces** – Stolen or breached data may be obtained from illegal marketplaces, often referred to as 'dark web marketplaces', and used to target victims. Adversaries may purchase this data to access victim email addresses, phone numbers, credentials, demographics, and other personal information.
- **People search databases** – Adversaries may purchase victim data from people search websites. These databases – at least the authentic ones – offer accurate and detailed information about individuals.
- **Insider help** – Adversaries may attempt to lure insiders at organizations to disclose personal information about the organization's customers. Alternatively, the adversary may be an insider who abuses their position to illicitly acquire individuals' data, such as an employee committing insider fraud.

Stage 2: Development

For a scam to succeed, the scammer must follow several steps, each building on the last. In the Development tactic, the scammer establishes resources that form the foundation of the entire scam. These resources support later tactics in the Scam Kill Chain and may include creating, purchasing, or compromising resources to aid in targeting victims. Resources can be both physical (e.g. computing devices and human scammers) and virtual (e.g. websites, social media accounts, and malware) infrastructure used in the scam.

2.1 Acquire infrastructure

Adversaries may seek to purchase, steal, or compromise physical infrastructure resources to create their own servers or other assets for use in campaigns against victims. Such infrastructure may be built to facilitate specific scam attacks or designed to be reused for various scams.

- **Email servers** – Adversaries may set up email servers to send phishing emails. These servers can be purchased, rented, or abused. Additionally, regular web servers with email services may be utilized, and adversaries may also subscribe to SMTP relay services and bulk email services to support their operations.
- **Domains** – Adversaries may purchase domains or utilize free-to-use domain names. They may also compromise existing website domains to hijack their legitimacy. Additionally, adversaries might use domain generation algorithms to create and register hundreds of domains for their campaigns.
- **Cloud resources** – Adversaries may acquire cloud resources to host malicious content by purchasing them or exploiting publicly available services. Furthermore, adversaries can use Content Delivery Networks (CDNs) to hide the original IP address of malicious sites or network tunneling tools like Cloudflare to expose privately hosted websites to the public internet.
- **C2 server** – Adversaries may build a command-and-control (C2) server from scratch or leverage publicly available resources for malicious purposes. In scams, C2 servers are primarily used to exfiltrate victims' personal information. These servers can take various forms, including centralized servers under the attacker's control, bulletproof hosting, social networks, messengers, or cloud services.
- **Phone numbers** – Adversaries may create a set of fake phone numbers for their campaigns, such as making fraudulent calls to potential victims. They may achieve this using VoIP tools or by purchasing multiple SIM or eSIM cards, which can later be used to contact victims.
- **Infrastructure for malware** – Adversaries may create their own malware payload to exploit victims, or they may rent or purchase malware from a malware-as-a-service provider or simply download free-to-use malware.

2.2 Software development

Software development is a key aspect of resource development. Adversaries may develop, purchase, or steal various types of software to manage different stages of a scam. Below are the types of software they might create.

- **Custom malware** – Adversaries may write custom malware as part of a scam payload. This malware is typically designed to perform malicious activities, such as stealing information or ransoming files, on the victim's device.
- **Website developments** – A scam often involves redirecting a victim to a phishing or scam website. In this technique, the adversary creates a malicious website designed to deceive victims. The site may be entirely new or a replica of an existing brand, intended to steal personal information from the victims.
- **Bots** – After creating new or replica websites, adversaries may add chatbots to enhance the appearance of legitimacy. These bots, whether functional or not, are designed to lure victims into the scam. Their applications can range from stealing credentials to obtaining credit card data through fake transactions, such as fake pizza orders.
- **Automated scripts** – In addition to programming websites, adversaries may create computer scripts to carry out malicious activities as part of the scam. Victim-side scripts are typically activated on websites that deceive victims, displaying fake login pages to capture keystrokes or redirecting users to fraudulent sites. Adversary-side scripts, on the other hand, are typically hosted on the server the victim connects to and can store stolen data.

2.3 Acquire services

Instead of building their own infrastructure, adversaries may attempt to purchase, rent, or hijack existing services.

- **Human personnel** – Adversaries may trick, hire, or coerce individuals to work on their behalf in the scam. Human involvement is common in scams like tech support, romance, and investment frauds. In some cases, individuals may also be used for more specific tasks, such as intimidating victims or building relationships to manipulate them.
- **XYZ-as-a-Service** – Adversaries may acquire various malicious services by subscribing to or purchasing them. These services, referred to as 'XYZ', enable the adversary to carry out their scam and can include offerings like Phishing-as-a-Service or Malware-as-a-Service. While some services may be developed by the adversary from scratch, they are often available for hire on illegal marketplaces. In some cases, adversaries may be directed to these services by other cyber criminals.

2.4 Create accounts

Adversaries may create new accounts on existing online services, which differs from compromising existing accounts. In some cases, adversaries steal data, such as images, names, or other personal details to steal the identities of the original account holders. Furthermore, they may use the photos and information of high-profile accounts to create fake or imposter accounts, aiming to deceive victims.

- **Social media** – Adversaries may create accounts on popular social media platforms such as Facebook, Instagram, LinkedIn, TikTok, YouTube, and similar. These accounts are used to spread false information, solicit monetary favors from friends, send lures (such as URLs), or even intimidate others. Adversaries may also impersonate well-known brands to promote fake information or fraudulent shopping sites.
- **Email accounts** – Adversaries may create many fake accounts on existing email service providers which can then be used to carry out phishing campaigns.
- **Cryptocurrency wallets** – Adversaries may create their own cryptocurrency wallets to deceive victims into sending cryptocurrency to these fraudulent accounts.
- **Messengers** – To target potential victims, adversaries may use popular messaging platforms such as Telegram, WhatsApp, and Discord. They may create accounts, channels, groups, or communities on these platforms to attract and lure victims. Additionally, scammers can leverage automated services to assist in their efforts.
- **Fake legitimacy** – Adversaries may purchase or create fake reviews, ratings, subscriptions, likes, and other forms of engagement to create seemingly legitimate profiles, pages, or applications. Another technique includes generating fake tracking codes for deliveries.

2.5 Develop the bait

Building infrastructure is just one step for the adversary toward the end goal of scamming potential victims. In addition to this, the adversary may develop capabilities to generate content for the scam in various ways. A key part of the scam is creating a 'bait' that encourages victims to act. This bait must be carefully crafted to appear credible and compel the victim to engage with the scam. To achieve this, the adversary may, for example, tailor the content to reflect current news, use threats to create urgency, or lure victims with tempting offers. Once the bait is crafted, the adversary will use a variety of techniques to deliver it to unsuspecting victims.

- **SMS** – Adversaries may use mobile phones to send scam SMS messages to victims.
- **Emails** – Adversaries may use emails to send scam messages, as emails give scammers more freedom to be creative compared to the brevity required in SMS messages.
- **Website content** – Adversaries can create more elaborate schemes by building fake websites designed to illicitly extract users' personal or financial information. They may either create these websites manually, which requires more effort, or use phishing kits to automate the process.
- **Human-language scripts** – These differ from automated computer-language scripts. Human-language scripts are playbooks and instructions that humans can follow. They are used by adversaries when interacting with victims over the phone, through direct messaging, or by commenting on social media posts, employing specific language or a systematic, easily replicable script.
- **Advertisements** – Adversaries may purchase online advertisements specifically designed to scam victims, often through Scam-as-a-Service or Fraud-as-a-Service offerings, or they may create their own ads. These ads are strategically placed in high-visibility locations online, such as search engine results, websites, or social media ads.
- **Mobile apps** – Adversaries may create fake apps for popular operating systems like Android or iOS. These apps can perform various malicious tasks, such as providing fake functionality or stealing personal information. As part of scam campaigns, adversaries may target victims through their smartphones, enticing them to install these fraudulent apps and continue with the scam. A common technique is to replicate legitimate apps and inject malicious code.
- **SEO poisoning** – Adversaries may manipulate content to influence search engine rankings, thereby promoting their own malicious or scam-related content among the top search results.
- **URL manipulation** – Adversaries may manipulate or create fake links for phishing attacks to conceal the real URL from victims. This can be done using QR codes, also known as 'quishing', where adversaries use QR codes to direct users to fake websites designed to steal sensitive information. Alternatively, adversaries may employ URL shortening services to obscure phishing URLs.

2.6 Algorithmic manipulation

Adversaries may take a more passive approach by directing victims to websites, hoping they will click on scam lures.

- **Advertisements** – Adversaries may post scam advertisements across various platforms, including websites, social media, and YouTube.
- **SEO poisoning** – Adversaries may manipulate search engine results to promote scams at the top, hoping that victims will trust these results without question and click on them.
- **Misleading content** – Adversaries can create content, such as videos or posts, on social media to lure victims to malicious sites or encourage engagement with the content, such as resharing it.

Stage 3: Contact

Once potential victims are identified and their information is gathered, the scammer must use this data to make contact. In the Contact tactic, the scammer may employ various manipulative techniques, including interactive contact (e.g. phone calls), non-interactive contact (e.g. online ads), or a mix of both. Common channels include email, SMS, social media direct messages, and more. In some cases, victims may even contact scammers unintentionally, such as by searching for pirated software. The goal of the Contact tactic is to provoke a response, either by directing the victim to a malicious site or getting them to reveal sensitive information.

3.1 Emails

Adversaries may attempt to make initial contact with victims by sending emails containing a lure, such as offering a free product. Alternatively, emails may be used to scare victims with threats of disastrous consequences, such as deportation for failure to pay taxes. Typically, these emails include a link to download or access something malicious.

3.2 Phone calls

Adversaries may make direct contact with victims by calling and initiating a conversation. They often impersonate trusted figures (such as government authorities or family members) to gain the victim's trust, setting the stage for further malicious actions. The phone call technique aims to create a sense of trust, urgency, or threat – elements that may be harder to convey through other methods.

3.3 SMS

Adversaries may contact victims by sending fake text messages, using bait sourced from the Development tactic. Phishing SMS messages employ the same techniques as phishing emails, with the key difference being that they are typically more concise.

3.4 Social media

Adversaries may contact victims through messages or advertisements on social media platforms like Facebook, LinkedIn, and others. Common lures on these platforms include fake product offers, fake job interview calls, and fake lottery winnings. Adversaries may also use social media messengers to initiate contact. Additionally, this communication can be driven in one of two ways. In adversary-driven communication, the adversary takes the lead in contacting and luring victims through various methods, primarily aiming to deceive them. In contrast, victim-driven discovery involves victims actively searching for dubious products or services, such as pirated content, and visiting malicious websites. Here, the adversary creates the scam resources but waits for victims to find them.

3.5 Search engines

In the Development tactic (2.6 Algorithmic manipulation), the adversary manipulates search engine results to deceive victims. In this technique, the goal is for the victim to search for terms with manipulated results (e.g., pirated movies or free software) and fall into the trap by clicking on altered links.

3.6 Online services

Adversaries may exploit existing online services to search for and contact victims. For example, they might abuse platforms like Tinder, a dating app, to target individuals. These online services provide adversaries with a tailored opportunity to find and reach victims.

3.7 Mimicking legitimate companies or services

In this technique, adversaries exploit the reputation and trust of popular services to their advantage. They create a service similar to an established one on the same platform, such as a website, mobile app, or fake online account mimicking famous personalities, using the brand's name to lull potential victims into a false sense of security.

3.8 Messengers

Adversaries may contact victims using popular messaging platforms such as WhatsApp, Facebook Messenger, Telegram, etc.

Stage 4: Persistence

As a scam progresses, the likelihood of discovery increases. At this stage, the scammer has already invested time and effort into building and launching the scam. Now, they must prolong it by any means necessary to reach the Monetization tactic. This is known as the Persistence tactic. The scammer may use several techniques, but the focus remains on building trust. This could involve misleading the victim about the scam's intent, convincing them to make small payments under the false belief of earning rewards, or shifting conversations to different platforms to avoid detection.

4.1 Erase virtual presence

Adversaries may choose to minimize their virtual presence as much as possible through two key actions:

- Implementing malware that deletes itself after stealing data from the victim's device.
- Deleting social media profiles, removing online comments and advertisements, and taking down malicious websites. For example, they may keep phishing websites active for only a short duration to make detection and prevention more difficult.

4.2 Cultivating trust

The adversary's goal is to build trust so the victim stays engaged in the scam. To achieve this, they may use several techniques to maintain the victim's interest for as long as possible. For example, they might make real small payments to the victim to establish trust and alleviate any suspicions. In scams involving ongoing communication, the adversary may also use emotional manipulation to keep the victim engaged.

4.3 Change medium

Adversaries may persuade victims to move conversations to a different messaging platform, claiming it offers greater safety and security. This is done to bypass evasion techniques employed by different platforms.

Stage 5: Access

In this tactic, the scammer attempts to access the victim's devices, such as online accounts, laptops or mobiles, with the goal of stealing private information, either with or without gaining a foothold on the device. Scammers are typically interested in data they can use directly or sell, rent, or ransom later. This includes personally identifiable information, credit card details, cryptocurrency wallets, and more. The victim's information may be accessed in several ways, such as directly from the victim or through phishing or malware. While similar to the Contact tactic, the Access tactic differs in that its goal is to actively access and gain control of the victim's information.

5.1 Victims share information on their own

In this technique, adversaries lure victims into willingly sharing their information. After establishing initial contact, they rely on the victim falling for the bait and responding in one of the following ways:

1. **Over the phone:** The victim calls the adversary using the phone number provided in the lure. During the call, the adversary uses persuasive tactics to extract private and sensitive information.
2. **On messaging platforms:** The victim provides sensitive details, such as personal information, access credentials, or banking details, through direct messages or messaging platforms.
3. **Via phishing pages:** The victim clicks on links provided by the adversary, often via email or advertisements. These links lead to phishing pages designed to mimic legitimate login or payment forms. The victim enters sensitive information, such as credit card details, which is then captured by the adversary.

5.2 Victims' information stolen with malware

In this technique, adversaries stealthily steal victim information, often without the victim's awareness. They may trick victims into installing fake smartphone apps that exfiltrate sensitive data to a command-and-control (C2) server or deploy malware on computers to steal information, hijack resources for cryptocurrency mining, or launch denial-of-service (DoS) attacks. A common malware type, infostealers, infects victims via email attachments, malvertisements, and similar methods, targeting credentials for online banking, social media accounts, and other sensitive information.

5.3 Attacks with no interaction with the victim

In this technique, adversaries steal victim information without the victim's knowledge or direct interaction.

- **SIM swapping:** Adversaries contact the victim's telecom operator using stolen details to request a new SIM card, gaining control of the victim's phone number. This allows them to reset online accounts linked to the number and gain access to sensitive information.
- **Enterprise-level data breach:** Adversaries compromise an online service or company's IT system that the victim uses, gaining access to sensitive information.

Stage 6: Exfiltrate

Accessing the data alone isn't enough as access to it could be denied or revoked at any time. The scammer must now take possession of it. This occurs in the Exfiltrate tactic, where the scammer transfers the stolen data from the victim's device or saves the information entered by the victim on the scammer's hosted service. Some exfiltration techniques may require interaction with the victim, while others can be carried out without their knowledge. These techniques can be either automated or manual.

6.1 C2 channel

In this technique, adversaries establish a command-and-control (C2) server by either leveraging existing resources or creating their own, offering greater flexibility and control over data exfiltration. Data obtained from the victim is sent to the C2 server in plaintext, archived, or encrypted and archived form. Adversaries may use publicly available services like Google Drive or Amazon, gaining the advantage of 'hiding in plain sight'. Platforms such as Telegram and Discord, with their user-friendly bot APIs, are also frequently misused as C2 servers for exfiltrating and storing sensitive data.

6.2 Direct access to victim's device or account

In this technique, adversaries exfiltrate data using non-traditional methods outside of command-and-control (C2) channels. This can involve direct interaction with the victim or other passive means. For instance, adversaries may exploit a legitimate and non-malicious screen-sharing software like TeamViewer to remotely access and steal victim information and transfer it elsewhere. Alternatively, they might set up email forwarding rules to monitor victim activities, steal sensitive data, and maintain persistence, even if account passwords are changed.

Stage 7: Lateral Movement

Typically, the success of a scam grows with the number of victims, and scammers exploit this to increase their profits. In the Lateral Movement tactic, the scammer spreads the scam to as many people as possible using the initial victims' environments. This can occur in several ways, such as by abusing the victims' social media accounts to reach their contacts, posting scam messages in victim-related groups or forums, or using one social media account to access others. This proliferation also helps the scammer cover their tracks, making it harder for new victims to identify the true perpetrator.

7.1 Spread to victim's contacts

After exploiting a victim, adversaries may abuse the victim's contacts to expand the reach of their scam. This often involves targeted phishing attacks, where the victim's contacts receive messages that appear to come from the victim, reducing suspicion and increasing the likelihood of success. The ultimate goal is to exploit additional victims, obtaining more data and, consequently, more money.

- **SMS** – Adversaries may spread the scam to a victim's contacts through SMS.
- **Social media** – Adversaries may exploit the first victim's social media accounts in various ways to spread scam messages, such as ironically posting in groups about scam awareness advertising 'scam recovery' services, leaving comments on social media posts about scams, and sending direct messages that appear to be from a friend to the victim's contacts or friends.
- **Email** – Adversaries may send emails to a victim's contacts.

7.2 Compromise victim's other online accounts

After the initial compromise, adversaries may attempt to take over other online accounts of the affected individuals, broadening the scope of the attack and increasing their potential rewards.

- **Password reset** – If adversaries gain access to the victim's email or phone number, they may attempt to reset passwords for other online services, assuming the victim reuses the same password across multiple accounts.
- **Linked accounts** – Adversaries can take over linked social media accounts such as Instagram or Facebook, or sub-pages on social media where the victim is an admin.
- **Single sign-on (SSO)** – If the victim uses the compromised account for SSO to access other online services, the adversary can exploit this to gain further access to the victim's information.

7.3 Leverage victim's access rights

In this technique, the adversary targets specific employees within an organization who have access to valuable resources. These resources may include admin rights to social media groups or elevated responsibilities in areas like gift card or credit card divisions. Once the victim's account with normal privileges is compromised, the adversary can move laterally to abuse the victim's corporate access. For example, if a victim has admin access to the company's Facebook page, that page may be compromised. Similarly, if the victim's account is compromised, sensitive corporate details such as credit card or banking information could be exposed.

Stage 8: Monetization

The final and most crucial step in the F-Secure Scam Kill Chain is the Monetization tactic. Scamming is a business, and profit is at the core of nearly every scammer's motive. All previous tactics lead to this point, but the scammer must take steps to avoid detection. For example, direct money transfers can be traceable, and cash transactions may be impractical or attract unwanted attention, especially if the scammer and victims are in different locations. As a result, scammers often use multiple forms of monetization, including actual money, cryptocurrency (fueling various investment schemes), selling valuable data, assuming another person's identity, or taking advantage of premium memberships to services such as Steam without paying.

8.1 Direct transfer of funds

Adversaries may trick victims into directly transferring money from their bank accounts to the adversaries' account. Alternatively, they may steal the victim's bank credentials to make transfers without the victim's knowledge. Other methods of transferring funds include:

- **Cryptocurrency transfers** – In this technique, adversaries may trick or blackmail victims into transferring cryptocurrency to the adversary's wallet. Several scams are associated with this approach, and the primary advantage for the adversary is the anonymity provided by cryptocurrencies. This anonymity allows the adversary to remain hidden from the victim and beyond the reach of law enforcement. As cryptocurrency usage continues to grow, so do the deceptive tactics employed by adversaries.
- **P2P payments** – P2P apps make it easy to send money to friends and businesses, often without fees and without the need for checks, cash, or debit cards. Adversaries may exploit this by tricking victims into transferring money through a mobile payment app. The reason behind using this technique is that adversaries know once money is sent via a mobile app, it's difficult for the victim to recover it.

8.2 Investment scheme

Adversaries may trick victims into investing in fraudulent schemes, causing them to lose money. This deceptive practice, which has existed for centuries, involves offering tempting opportunities to lure victims into various investments. A modern variation is fraudulent crypto schemes, where adversaries entice victims to invest in fake cryptocurrencies, counterfeit exchanges, or fraudulent NFTs. They may also exploit legitimate exchanges' investment or liquidity pools to promote fake opportunities. While this resembles the 'Direct transfer of funds' technique, the key difference is that 'Direct transfer' focuses on tricking victims into sending cryptocurrency directly to the adversary, while this technique deceives victims into investing in fake crypto opportunities.

- **Rug pull** – In this technique, the adversary tricks one or more victims into investing in a cryptocurrency scheme before 'pulling the rug'. This means the adversary waits until the collected funds reach a desirable threshold and then runs off with the victims' investments. A fake mining pool is an example of this 'rug pull' scam. Cryptocurrency mining pools combine efforts from individual miners or smaller groups to compete with large mining operations. However, all pool wallets are at risk if the pool operator breaks the contract and runs off with the pool's cryptocurrency.
- **Ponzi scheme** – A Ponzi scheme is an investment scam in which returns are paid to existing investors using funds from new investors. Organizers of Ponzi schemes typically attract new investors by promising high returns with little or no risk. In reality, the scheme relies on receiving money from new investors and using it to pay earlier backers, all while pretending that these payments are profits from legitimate investments. Eventually, the system collapses when the influx of new investments slows down.

8.3 Sale of stolen data

Adversaries may choose not to use stolen data for their own purposes but instead sell it, often for various reasons, including selling it back to the original owner (ransom). For instance, stolen personal data such as names and addresses may not be directly useful to the adversary, but stolen credit card details can attract a significant audience on the dark web. Selling stolen data often fits into a larger scam, where it is resold to other adversaries for use in their own fraudulent activities.

- **General sale** – Adversaries may sell stolen data on illegal online marketplaces. Another method of sale includes using Telegram or Discord messenger channels, for example, where transactions occur with anyone who joins the channel.
- **Specific sale** – Adversaries may choose not to make the stolen data public but instead aim to achieve higher returns by auctioning it to the highest bidder. In specific cases, such as with spyware or stalkerware, the stolen data may only be sold to a relevant purchaser. Additionally, in ransomware attacks, the adversary may sell the data back to its rightful owner, demanding a ransom for its release.

8.4 Identity theft for further benefits

An adversary may steal or assume the victim's identity to gain benefits in their name, such as money or other assets, which can then be sold for profit. They may approach a bank or financial institution to take out a loan in the victim's name or use the victim's identity to purchase non-liquid assets, such as property, cars, or electronics.

8.5 Cryptocurrency mining

This technique focuses on using the victim's resources to mine cryptocurrency, which the adversary later sells for monetary gain. This technique can be further categorized into a couple of types:

1. The victim inadvertently downloads cryptocurrency malware, for example, by clicking on a link in a phishing email or through malvertising on a social media website.
2. Visitors to a legitimate website unknowingly have their CPU resources stolen. This is also known as 'cryptojacking', where the visits of thousands of people to a website are exploited for cryptocurrency mining.

8.6 Gains (financial and non-financial) via virtual assets

The typical benefit of scams is that the adversary directly earns money or cryptocurrency. However, in this technique, the adversary gains benefits indirectly by using various online services at the victim's expense. These benefits are considered indirect because the adversary enjoys services or premium subscriptions that belong to the victim. For example, accessing YouTube Premium accounts is one way an adversary may gain indirect benefits. In some cases, the adversary may 'enjoy' these services, while in others, they may sell stolen services, such as online game assets.

- **Legitimate online service or game** – The adversary may use stolen financial data (such as credit card, debit card, or bank account details) to register for premium accounts with legitimate online services, thereby gaining access to those services. In effect, the adversary may launder stolen money through these legitimate services.
- **Online gift cards** – Adversaries may intimidate victims into paying money through gift cards as a way to remain anonymous. One example of this scenario is in 'sex-for-money' scams, where the victim is coerced into visiting a specific location to claim the offered 'services' and is first pressured into making payments via gift cards.