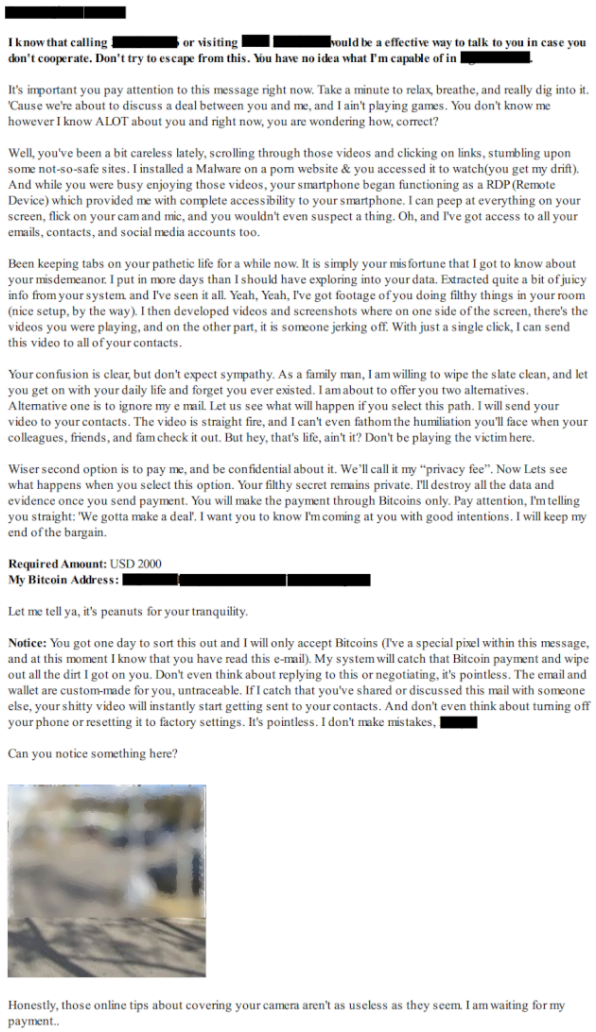
The Sextortion Scammers' Process

Sextortion scams exploit fear, not facts. While some involve actual compromising material, **many rely on the illusion of possession**. Scammers prey on victims' anxieties, convincing them that they have explicit photos or videos.

These scams are carefully constructed from bits of truth and tech. They combine publicly available data, information bought from data brokers, and even details gleaned from data breaches. Injecting the right type of personal data - **like a picture of your house** - can make it feel like the sender knows you personally.



[redacted]

I know that calling [redacted] or visiting [redacted] would be a effective way to talk to you in case you don't cooperate. Don't try to escape from this. You have no idea what I'm capable of in [redacted].

It's important you pay attention to this message right now. Take a minute to relax, breathe, and really dig into it. 'Cause we're about to discuss a deal between you and me, and I ain't playing games. You don't know me however I know ALOT about you and right now, you are wondering how, correct?

Well, you've been a bit careless lately, scrolling through those videos and clicking on links, stumbling upon some not-so-safe sites. I installed a Malware on a porn website & you accessed it to watch(you get my drift). And while you were busy enjoying those videos, your smartphone began functioning as a RDP (Remote Device) which provided me with complete accessibility to your smartphone. I can peep at everything on your screen, flick on your cam and mic, and you wouldn't even suspect a thing. Oh, and I've got access to all your emails, contacts, and social media accounts too.

Been keeping tabs on your pathetic life for a while now. It is simply your misfortune that I got to know about your misdemeanor. I put in more days than I should have exploring into your data. Extracted quite a bit of juicy info from your system. and I've seen it all. Yeah, Yeah, I've got footage of you doing filthy things in your room (nice setup, by the way). I then developed videos and screenshots where on one side of the screen, there's the videos you were playing, and on the other part, it is someone jerking off. With just a single click, I can send this video to all of your contacts.

Your confusion is clear, but don't expect sympathy. As a family man, I am willing to wipe the slate clean, and let you get on with your daily life and forget you ever existed. I am about to offer you two alternatives. Alternative one is to ignore my e mail. Let us see what will happen if you select this path. I will send your video to your contacts. The video is straight fire, and I can't even fathom the humiliation you'll face when your colleagues, friends, and fam check it out. But hey, that's life, ain't it? Don't be playing the victim here.

Wiser second option is to pay me, and be confidential about it. We'll call it my "privacy fee". Now Lets see what happens when you select this option. Your filthy secret remains private. I'll destroy all the data and evidence once you send payment. You will make the payment through Bitcoins only. Pay attention, I'm telling you straight: 'We gotta make a deal'. I want you to know I'm coming at you with good intentions. I will keep my end of the bargain.

Required Amount: USD 2000
My Bitcoin Address: [redacted]

Let me tell ya, it's peanuts for your tranquility.

Notice: You got one day to sort this out and I will only accept Bitcoins (I've a special pixel within this message, and at this moment I know that you have read this e-mail). My system will catch that Bitcoin payment and wipe out all the dirt I got on you. Don't even think about replying to this or negotiating, it's pointless. The email and wallet are custom-made for you, untraceable. If I catch that you've shared or discussed this mail with someone else, your shitty video will instantly start getting sent to your contacts. And don't even think about turning off your phone or resetting it to factory settings. It's pointless. I don't make mistakes, [redacted]

Can you notice something here?

Honestly, those online tips about covering your camera aren't as useless as they seem. I am waiting for my payment..

If you receive an email demanding payment or someone will expose your secrets, chances are, you are simply one of hundreds of thousands on a spam list. There is no "or else."

Let's break down the typical process these scammers follow:

Sextortion Scammer Process Summary

Step	Time	Skills Needed	Tools/Sources	Criticality
Data Collection	Hours to Days	Basic cybersecurity, database handling	Dark web, public databases	High
Scripting and Crawlers	Hours, ongoing	Programming, API exploitation	Web scrapers, Google Maps API	Medium to High
Assembly of Threats	Minutes to Hours	Social engineering, script writing	Pre-written templates, text customization tools	High
Spoofing and Masking	Minutes to Hours	Email spoofing, anonymization	Spoofing tools, VPNs, Tor	High
Automation and Bulk Sending	Minutes to Hours	Botnet management, email filtering bypass	Bulk email services, botnets, scripts	High
Social Engineering	Ongoing	Psychological manipulation	Case studies, updated scam tactics	Very High
Monetization	Minutes to Hours	Cryptocurrency knowledge, anonymization	Bitcoin wallets, tumblers/mixers, QR code generators	Very High

Data Collection from Breaches

Scammers acquire personal details like email addresses, passwords, and other sensitive information primarily from large data breaches.

Breached Databases

Scammers obtain your personal information like email addresses, passwords, and other details through large-scale data breaches. These breaches can happen when websites get hacked, public databases are exposed, or services like LinkedIn, Facebook, or even government databases are compromised. **Major breaches** like those at Equifax, Yahoo, **National Public Data**, First American, LinkedIn, and Facebook have unfortunately given scammers access to a vast amount of personal data.

DeHashed, **Scylla** and similar tools can be used to find breached data.

Dark Web Markets

Breached data is often sold on dark web markets like **RaidForums** or **BlackMarket**. Scammers purchase datasets containing millions of email addresses and other details.Password cracking tools like **Hashcat** or **John the Ripper** can be used to crack weak or commonly reused passwords, which makes the scam more convincing.

Public Records and Search Engines

Once a target is identified, scammers enrich the data by using services like **Whitepages**, **BeenVerified**, or tools like **Google Maps** to obtain additional information, such as home addresses or images of the victim's house.

Time Required

- Can take **hours to days** depending on the volume of data and tools used.

Skills Required

- **Basic cybersecurity skills** to navigate the dark web.
- **Database handling** skills to sort and analyze relevant data.

Tools/Sources

- Dark web marketplaces, breach databases (e.g., **Have I Been Pwned**).
- Password cracking tools (e.g., **Hashcat**, **John the Ripper**).
- People search engines and APIs like **Google Maps**.

Process Criticality

- **High** – Access to compromised data is critical for the scam's success. It provides the core information needed to personalize emails.

Automated Scripting and Crawlers

Scammers rely on automation to gather information from various public sources to personalize their sextortion threats and increase credibility.

Data Scraping Bots

Web scraping tools (**BeautifulSoup**, **Selenium**, **Scrapy** etc.) are used to automatically collect details like names, locations, and browsing habits from social media, forums, and public directories. According to Akamai, **bots now represent 42%** of overall web traffic, with 65% of those bots being malicious. Headless browsers (**Puppeteer, Playwright**, **PhantomJS**) allow bots to mimic real user interactions, making their activity harder to detect.

API Exploitation

Some scammers exploit APIs (e.g., **Google Maps API**) to retrieve images of a victim's home, adding a personalized and invasive element to the scam. Open-source intelligence (OSINT) tools like **Maltego** or **Shodan** can also be used to gather additional data on victims from publicly available sources.

Data Augmentation

Scammers enhance the data they buy by cross-referencing it with publicly available information from social media or other platforms. There are hundreds of options available, many with easy access.

- **Clearbit**: An enrichment API that can provide detailed information about people based on their email addresses or company domains. While designed for marketing, it can be used by scammers to gather additional personal details about a target.
- **Pipl**: A people search engine designed to gather in-depth information on individuals, such as social media profiles and professional data. Scammers can use it to cross-reference data from multiple sources and enhance the credibility of their scam.
- **Hunter.io**: A tool that allows users to find and verify email addresses from domain names, which could be used to enrich existing datasets or identify additional targets.

Time Required

- **Hours** to create scripts; **ongoing** for data collection.

Skills Required

- **Intermediate programming** skills in **Python**, **JavaScript**, or other languages to develop scrapers.
- Knowledge of **API usage** for extracting personalized information.

Tools/Sources

- Web scraping tools (e.g., **BeautifulSoup**, **Selenium**).
- **Google Maps API** for retrieving home images.
- **Maltego**, **Shodan** for additional OSINT data collection.
- Data augmentation: **Clearbit** , **Pipl**, **Hunter.io**, and many many more,
- Data cleansing, organization, contextualization (**OpenRefine**, **FOCA**)

Process Criticality

- **Medium to High** – Personalized information like home addresses adds credibility, but the scam can still succeed without it. Automation dramatically increases efficiency.

Assembly of Threats

Scammers craft the emails using pre-made templates and personalize them by inserting victim-specific details.

Pre-Formatted Email Templates

These templates typically include threats, Bitcoin wallet addresses, and short deadlines. Scammers insert personalized details such as the victim's name, email, and compromised password (from breaches).

Inserting Personalization

Adding old passwords or home addresses to the message makes the scam more believable. Email spoofing techniques are also used to make it appear as though the email is sent from the victim's own account.

Time Required

- **Minutes** to assemble using templates; longer for more customized emails.

Skills Required:

- **Basic editing** and **script writing** skills.
- Knowledge of **social engineering tactics** to craft persuasive language.

Tools/Sources:

- Pre-written sextortion templates from scammer forums.
- Text customization tools to insert personal details automatically. (Mail Merge Scripts, **Spintax**)

Process Criticality:

- **High** – Effective personalization and fear-inducing language increase the scam's success rate.

Spoofing and Masking Techniques

Scammers use spoofing techniques to make their emails seem more credible and anonymous.

Email Spoofing

Tools like **Emkei's Fake Mailer** or **SpoofBox** are used to spoof the victim's email address, making it appear as if the email is coming from their own account. By manipulating email headers, scammers create the illusion that they have hacked the victim's email system.

Encrypted Cryptocurrency Wallets

Scammers provide QR codes or wallet addresses (usually for **Bitcoin**) to avoid traceability.

Time Required

- **Minutes to hours** depending on sophistication.

Skills Required

- **Basic to Intermediate** email spoofing and anonymization skills.
- Knowledge of **SMTP manipulation** or email header tampering.

Tools/Sources

- Tools used in spoofing (e.g., **Emkei's Fake Mailer**, **SpoofBox**, **SendGrid**, **Gophish**)
- VPNs and **Tor** for IP masking and anonymity.
- Cryptocurrency wallets for anonymous payments.

Process Criticality

- **High** – Spoofing and anonymity are essential to convincing victims that the scammer controls their email and can follow through on threats.

Automation and Bulk Sending

Sextortion scammers use automation to send emails to large numbers of recipients quickly and efficiently.

Mass Email Sending Tools

Tools like **Sendblaster** or **MailChimp** are used to send emails in bulk, often to thousands of victims at once. **MIT Tech Review**: “Various researchers have shown that spammers pay botnet owners between $100 and $500 to send a million spam emails.”

Customization via Macros or Scripts

Automation scripts modify each email slightly, inserting unique details like the victim’s name, password, or home address to make it feel personalized.

Time Required:

- **Minutes to hours** depending on the number of targets.

Skills Required:

- **Intermediate knowledge** of bulk emailing software.
- **Email filtering bypass** techniques to avoid spam folders.

Tools/Sources:

- Bulk email services (e.g., **Sendblaster**, **MailChimp**).
- **Postfix** or **Exim** can be set up on compromised servers to send massive volumes of emails. These tools allow scammers to control their own email infrastructure, reducing reliance on third-party email services.
- **Storm Proxies** could be used to route email traffic through various IPs to avoid detection, prevent blocking, and evade spam filters.
- Botnets or zombie networks for mass email sending.

Process Criticality:

- **High** – Automation allows scammers to reach a large number of victims, dramatically increasing their chances of success.

Social Engineering and Fear Amplification

The success of the scam hinges on effective psychological manipulation.

Psychological Manipulation

Emails are crafted to evoke fear and panic by referencing private information, such as passwords or home addresses, and threatening to release fabricated videos unless a ransom is paid. By referencing sensitive or private information (like a password or street address), the email creates the illusion that the scammer truly has compromising information. This technique

plays on fear and guilt, encouraging the victim to comply quickly. Studies show that **fear-based appeals can be up to 50%** more effective in influencing behavior than positive messages.

Short Deadlines and Threats

Scammers often give victims **24-48 hours** to pay, creating urgency and preventing victims from thinking rationally or seeking advice.

Time Required:

- **Ongoing refinement** based on victim responses.

Skills Required:

- **Advanced social engineering** skills to exploit fear, guilt, and panic.
- Crafting convincing narratives using old passwords or other personal details.

Tools/Sources:

- Case studies from forums on effective sextortion methods. (PsyOps Playbooks)
- Regularly updated **psychological tactics**.
- Dark chatbots like **FraudGPT** and **DarkBERT**

Process Criticality:

- **Very High** – Manipulating the victim's emotions is key to ensuring quick payment.

Monetization

Scammers rely on cryptocurrency payments to maintain anonymity.

Cryptocurrency Payments

Payments are usually demanded in **Bitcoin**, which is perceived to be difficult to trace. Scammers often use **cryptocurrency mixers** or tumblers to launder the money after receiving it.

QR Codes for Easy Payment

To make payment easier, scammers include QR codes linked to their Bitcoin wallets, allowing victims to pay with minimal technical knowledge.

Time Required

- **Minutes to hours** to set up cryptocurrency wallets and payment systems.

Skills Required

- Knowledge of **cryptocurrency transactions**.
- Skills in **anonymizing financial transactions** through cryptocurrency mixers.

Tools/Sources

- Cryptocurrency wallets (e.g., **Bitcoin**, **Exodus**, **Monero**, **Samourai**).
- Cryptocurrency tumblers/mixers (e.g., **Wasabi**, **Mixero**, **ChipMixer** and **Blender.io**).
- QR code generators for payments.

Process Criticality

- **Very High** – Monetization is the ultimate goal of the scam, and cryptocurrency provides a way for scammers to remain anonymous.

Conclusion

The process of assembling sextortion emails is highly automated, leveraging data breaches, publicly available information, and social engineering. Scammers attempt to instill fear through personalization and mass targeting, leading victims to pay ransoms even though the threats are empty. Through automation and fear amplification, these scams generate profits for scammers despite their low success.

A seasoned scammer, using automation and pre-existing tools, **could potentially develop and launch a sextortion campaign targeting one million recipients within a single day**. The most time-intensive steps, such as data collection and personalization, can be streamlined if the scammer has access to existing resources, allowing for rapid deployment.

If you need advice about a specific situation, ObscureIQ can help. Visit us at **ObscureIQ.com**.