Report

V for Verified

The Sophisticated Social Media Impersonation Campaigns Targeting Corporate Executives

BlueVoyant

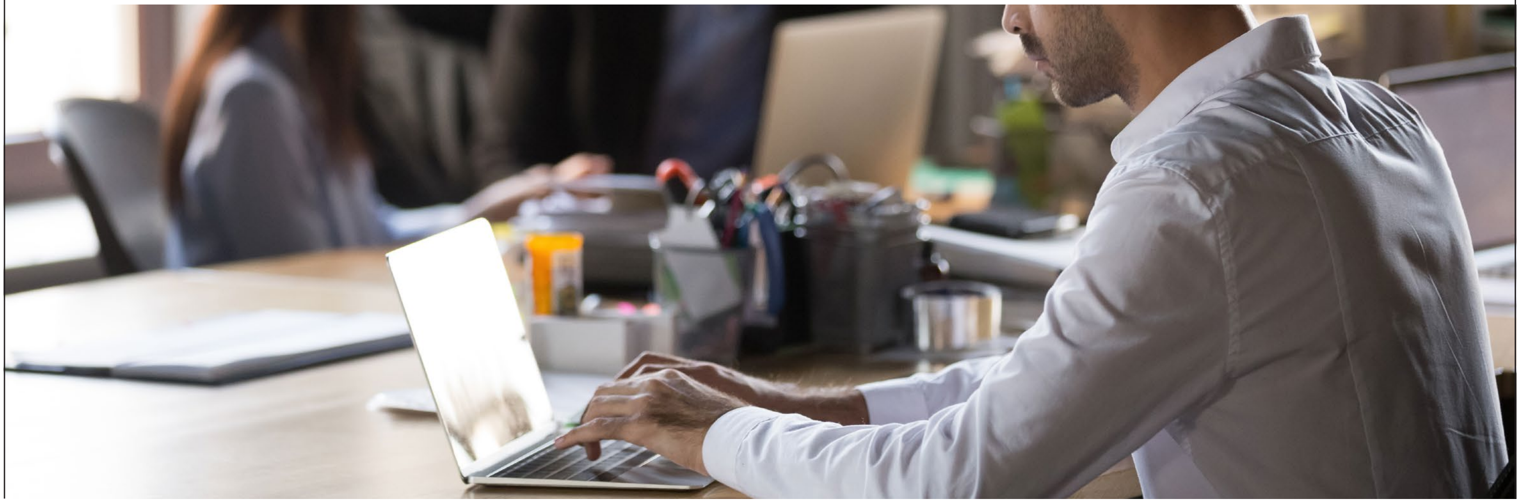
Executive Summary

In this report, BlueVoyant's cyber threat analysts delve into the rising trend of social media impersonation campaigns aimed at corporate executives and VIPs. These attacks exploit the likeness of high-profile individuals to deceive users into revealing sensitive data including payment card details. The report offers a comprehensive analysis of the attack methods, trends, and a case study of an impersonation campaign targeting an executive of a company involved in cryptocurrency investment.

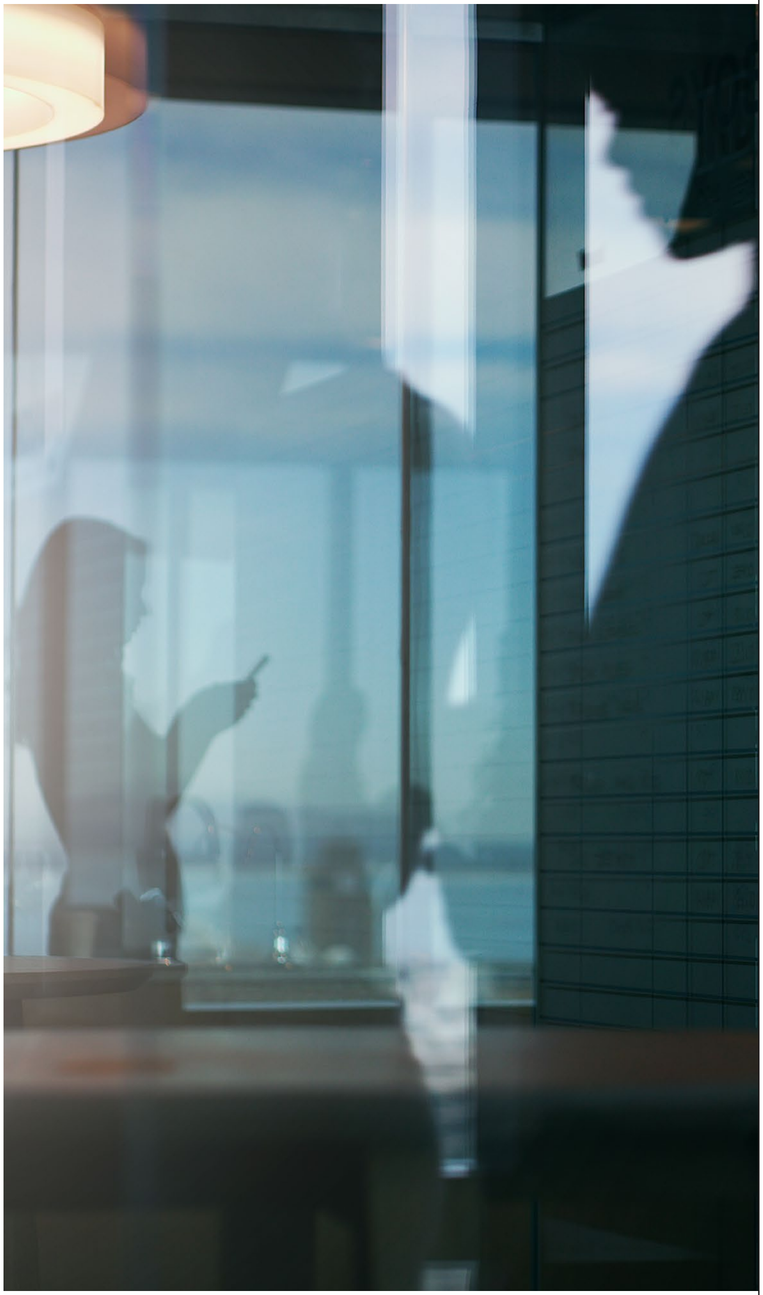
The impersonation process is relatively straightforward - attackers create social media profiles using the name, image, and other identifying features of the target. These campaigns are particularly profitable when targeting public figures, as the impersonators can reach out to potential business partners or employees, leveraging the executive's credibility to extract information or funds. They can also target ordinary users who wish to interact with the executive on social media. Key to a successful impersonation is reconnaissance and social engineering. Information is gathered through various means, including social media profiles of friends and family, breached databases, and public records websites. BlueVoyant determined that among all social media platforms, Facebook is often preferred by attackers for executive impersonation campaigns.

As a case study, BlueVoyant's analysts investigated profiles impersonating an American cryptocurrency executive and observed several characteristics. Many profiles were likely created by the same threat actor or group, they were often old and had been recently updated to impersonate the executive. Once activated, the profiles quickly gained followers, likely through bots, and began posting cryptocurrency-related content copied from the executives' official profiles, making them appear more trustworthy. The impersonators then targeted inexperienced crypto investors, and upon establishing contact with a potential victim, directed them to a fraudulent investment website promising high returns.

Despite social media platforms' best efforts at preventing impersonation attempts – using verification systems, bot detection, and other preventative measures – attackers continue to evade security protocols and successfully set up fraudulent executive profiles. Organizations should consider monitoring for threat activity specific to their executives to facilitate proactive takedowns of these profiles before they can victimize customers, business partners, employees, or even executives' personal connections. Recommendations also include increasing awareness among employees and customers, as well as protecting executives' data and monitoring for sensitive information found on the web.



Introduction



Threat actors consider corporate executives to be high-value targets. A successful attack can deliver lucrative rewards, such as the VIP's personally identifiable information (PII), login credentials for both personal and company accounts, and other sensitive data that could be used in an account takeover or fraud campaign. Executives are frequent targets of spear-phishing, doxing, and smishing attacks because they present an entry point to corporate systems and valuable confidential information. Successful attacks can cause financial and reputational damage not only to the executives themselves, but also to their organizations.

As social media influencer culture has become ubiquitous in today's society, many executives have begun to serve as thought leaders for their industries on popular social media platforms – namely LinkedIn and X/ Twitter. But this presents a new challenge: social media is a goldmine for cybercriminals due to the relative ease of executing successful social engineering attacks, scams, phishing attacks and more. Given the significant value corporate executives represent, it should come as no surprise that threat actors choose to impersonate them with great regularity.

Executives are highly sought-after targets, as hackers can take advantage of their notoriety to dupe unsuspecting users into interacting with an impersonating executive profile and providing PII, payment information, or otherwise falling victim to the scam and sharing personal data or transferring money to the threat actors.

This report will provide an inside look into how threat actors carry out these attacks, how successful they are, and the implications for security teams that must grapple with social media impersonation of their organizations' executives and VIPs.

Social Media Impersonation

Who, How, and Why?

Social media impersonation of individuals is a type of identity theft, a technique used in social engineering. It typically involves creating an account, profile or page that uses the name, image, and other identification features of a person or company in order to carry out fraudulent activities. It only takes a few minutes to set up and the only real obstacle is the platform's validation process. Cybercriminals also know how to make an impersonating profile more believable by, for example, using bots to generate fake followers and comments. Even though social media platforms have improved recognition of fake or fraudulent accounts over the years, these profiles can still be found in abundance and present a challenge even to the most advanced automated mitigation mechanisms.

Social media impersonation is especially worthwhile for threat actors spoofing a high-profile persona, celebrity, or corporate executive. Obtaining photos of public figures is easy, and the potential reward for a successful attack could be very cost-effective. When impersonating an executive, threat actors can reach out to potential business partners or the executive's employees, attempting to use the executive's credibility to trick them into sharing sensitive information or transferring money.

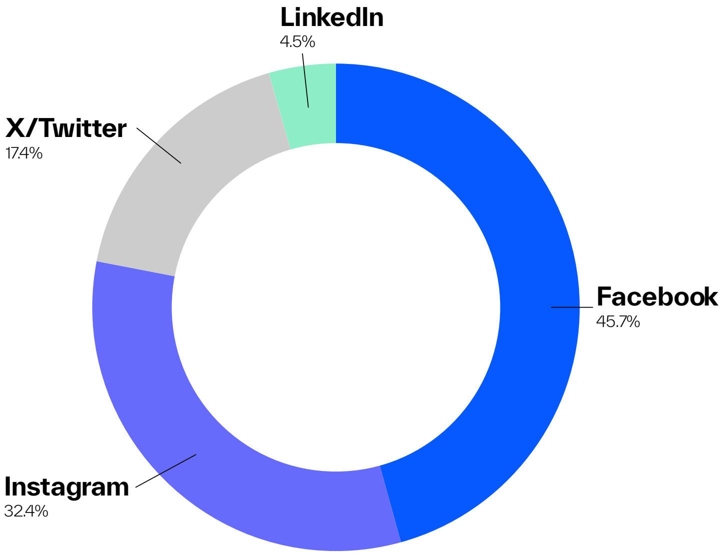
Threat actors are drawn to social media impersonation attacks because of the amount of exposure it gives them. Most users log onto social media multiple times a day and consume the content relevant to them quickly and without a discerning eye. Social media platforms are built to draw users in and coerce them to engage with other users and with brands. As it provides a distraction from the real world, most users often let their guard down while using social media and may overlook subtle warning signs when interacting with impersonating profiles.

Innocent users on social media may feel they can trust a profile of a well-known persona, even if they do not know them personally, and may be more inclined to respond positively if asked to do something for them. Furthermore, cybercriminals do not need to concern themselves with firewalls, spam filters, antiviruses and other computer security mechanisms while they are working their charm on an oblivious user.

In addition to the obvious financial pursuits, threat actors can use an impersonating profile to damage the target's credibility by performing catfishing, harassment, or spreading damaging disinformation. Threat actors may create an impersonating profile solely to tarnish that person's name and reputation. They may write things that may aggravate other users, clients, business opportunities or partners, who in turn will attribute those things to the actual person without realizing it's an impersonating profile.

The Scale of Social Media Impersonation Targeting Executives

BlueVoyant set out to determine which platforms are used the most by threat actors when impersonating executives. Our proprietary system has examined more than 1000 impersonated executive profiles on Facebook, Instagram, X/Twitter, and LinkedIn, as depicted in the chart below:



Facebook is dominating the impersonation arena, clocking in with 45.7% of all fraudulent executive profiles detected. **Facebook** was one of the pioneers of social media platforms, and as such many well-known individuals use the platform to connect with fans, business partners, or other people in their networks. The sheer volume of **Facebook** users across the globe likely influences this large percentage.

Instagram appears to be the runner-up, accounting for 32.4% of all fraudulent executive profiles detected. Instagram is the primary platform companies and individuals use to promote themselves, especially for consumer-facing businesses. However, the majority of users on Instagram are those who consume content from business and individuals' accounts. As a result the potential reach of an impersonation attack on **Instagram** is massive.

In third place is **X** (formerly **Twitter**), with 17.4% of our findings. **X/Twitter** is the platform where most executives have public profiles, where they can express their opinions, highlight their achievements and interact with their communities. Since **X/Twitter** has changed its verification system, it has become much easier to create a "verified" account impersonating a high-profile executive.

Finally, there's **LinkedIn** in fourth place, with 4.5% of the detected accounts. Since **LinkedIn** is a networking platform designed for the business community, it is the main platform for job searches, recruiting employees, and business interactions. For those reasons, BlueVoyant has observed a phenomenon unique to **LinkedIn** – profiles impersonating not only the CEO or other C-suite executives, but other high-level employees from departments such as HR or IT as well. Therefore, any person with a key position in a company may be in danger of being impersonated on LinkedIn.

The Tactics, Techniques, and Procedures (TTPs) Being Used

When establishing a profile, the threat actor also needs to make sure it looks believable so users will feel comfortable interacting with the profile. That interaction is key for the scam to work. Reconnaissance and social engineering are the prime methods for accomplishing a convincing impersonation attempt. The threat actor will need to take action, dedicate time and possibly even money to gather the necessary information if they wish to profit from the impersonating profile.

Obtain information → **Build reliable entity** → **Initiate contact**

The first and easiest way to start is by copying information from a legitimate executive's profile, including pictures, bios, posts, and their writing style. Furthermore, a public profile may also contain information such as date of birth, contact information, work and life information and updates, location data, personal interests and beliefs, and so much more.

On some occasions, threat actors also copy the profile's naming convention, creating a username that appears similar to the executive's real profile. For example, if the X/Twitter handle of a legitimate executive profile is "@ Sonia_1", creating an impersonating X/Twitter handle such as "@s0nia_1" or "Sonia__1" can be useful in making the profile look believable as it may trick other users.

However, if the executive does not have a legitimate social media profile on any platform or they have one on only one of them, the threat actors may have to devise other techniques in order to make it look believable. The actors will need information about the executive in order to establish a believable profile, and fortunately for them private information is not that hard to come by nowadays. The threat actor is presented with a few options:

1. Gather information regarding the executive from friends and family's social media profiles. Many users post events and information not only regarding their own life, but also shared experiences with other family members or friends. It may seem harmless, but if the profile is public, information such as location data, relationship status and other people's photos can be used to the threat actor's benefit.
2. Acquire exposed private information from databases or documents. Breached databases and documents containing private information often find their way onto the open web. In many cases, the leaked information does not only include the person's email, but other private information, such as an individual's signature, address, phone number, social media profiles, ID number, credit card details, and so on. Moreover, some breached information may contain data such as a whole work and education history.
3. Leverage public records websites to gain access to private information. These websites collect and sell information that they gather from a variety of publicly available federal, state, and local government databases, including property records, birth, marriage, divorce, and death records, business listings, phone directories, surveys, and voter registration information. Furthermore, these websites also gather private information from other sources, including public social media profiles, mailing lists, documents, blogs, and some may also buy private information from other data brokers.

   Such websites often require a paid subscription in order to view the information, but many don't. A user might be willing to pay for a subscription if they are looking to reconnect with an old friend or to check on a potential love interest, and of course it is also a tool often used by private investigators, law enforcement and cyber security companies. However, with just a few clicks a threat actor can also, with a high probability, find their victim's email, phone number, address and more.

Once the reconnaissance phase is completed, the threat actors use the information they have gathered and implement it into the impersonating profile they created, making it look more convincing by generating activity and gaining followers. Unsuspecting eyes might miss the additional features that will expose it for the fake it is, such as posts or a profile bio with a malicious link, and/or fake contact information.

With so much personal information available online, executives are at risk of a variety of threats besides social media impersonation, ranging from doxing, harassment, identity theft, swatting and more. However, impersonation, specifically, isn't exclusive to social media. Impersonating a person can be done by text, email and or even by phone.

Therefore, for an impersonation scam to work, it is not enough to know the basic information that can be found on an executive's Wikipedia page. Rather, cybercriminals will look for the missing piece of information on an executive, the "crown jewel". That "crown jewel" is the detail on the executive that won't trigger warning signs from their victims who may know the executive personally, whether it's a family member or a coworker, and that key detail can only be found with a comprehensive search of the executive's private information online.

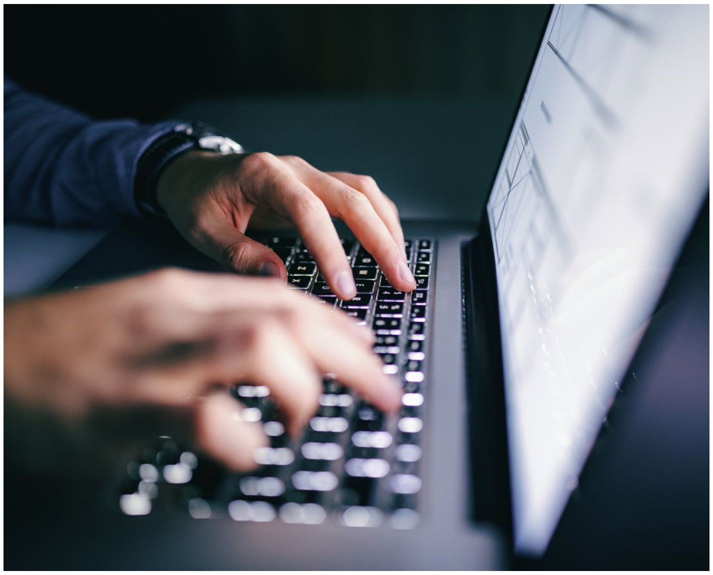
Case Study

For the purposes of this report, BlueVoyant focused on social media profiles impersonating an executive of an American company involved in cryptocurrency investment. As part of an ongoing impersonation campaign, the executive has hundreds of impersonating profiles on the most popular social media platforms.

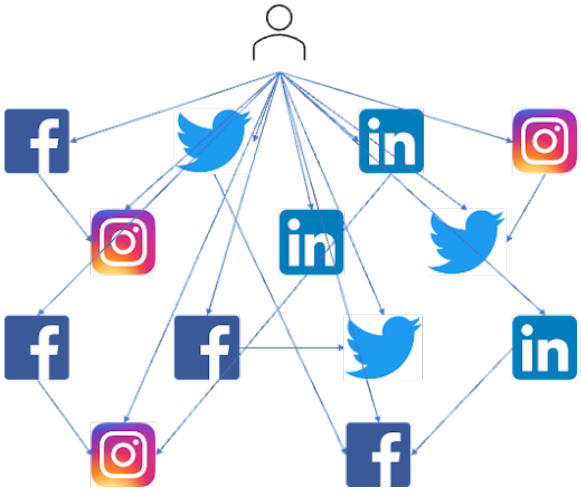
When investigating the campaign, BlueVoyant began with several leading questions:

- Is there one threat actor behind the campaign, or more?
- Is there a connection between the different profiles on the same platform?
- Is there a connection between the profiles on all four platforms?
- Are there similar patterns in the profiles' behavior/ characteristics?
- Are the profiles active and do they engage with other users?
- What is the end goal of those accounts?
- Can we gain insights into their TTPs and IOCs?

BlueVoyant's analysts first mapped out all the profiles and noted the active ones and those with similar patterns of appearance. Then, BlueVoyant searched to see if any of them were following other fake profiles or tagging/ reposting each other's posts.



At first glance, it appeared that other than reposting the executive's official, legitimate posts, there was no visible connection between the impersonating profiles. However, by using BlueVoyant's systems we did uncover that many, with high probability, were created by the same threat actor or group, as many of the fake profiles across the different platforms were linked to each other, as can be seen demonstrated below:

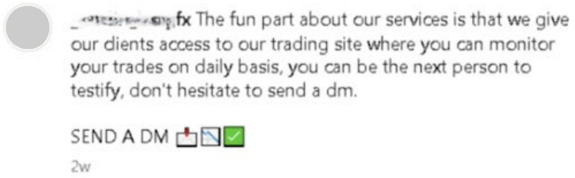


BlueVoyant's analysts also observed a pattern in the creation of the fake profiles. Many of the profiles were old and unused, created initially with a different name and picture, and were recently changed to impersonate the executive. By looking at the profile name as appears in the URL, and at the posts and pictures, BlueVoyant's analysts could trace it back to its original appearance. It is possible that these profiles might have been compromised, potentially by using leaked credentials that were found or purchased on the black market.

After gaining control of the profile, the threat actor begins with subtle changes to reset it: name change, profile picture change, handle change, URL name change, and sometimes unfriending or unfollowing other profiles. After the resetting process is done, the profiles lay dormant until the threat actor decides to start generating activity. BlueVoyant assesses that when the threat actor operating these profiles decides to activate them, the profiles suddenly gain dozens of followers, potentially by using bots or purchasing followers, which makes it look more trustworthy.

Once the profile looks believable, the threat actors begin posting news and information about cryptocurrency. Most of the posts are either informative or general updates regarding the life of the executive, copied from their official profile. However, out of the four platforms, the only posts that encouraged users to contact the fake profile were found on Instagram. On those Instagram profiles, the threat actors deployed the next phase in the impersonating scam - establishing contact with potential victims and luring them into fraudulent cryptocurrency investments.

Please see the example below:



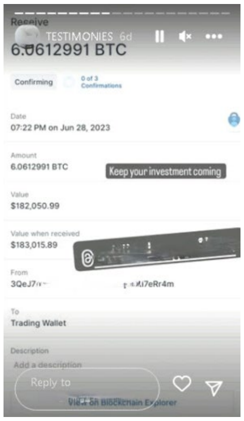
[redacted]fx The fun part about our services is that we give our dients access to our trading site where you can monitor your trades on daily basis, you can be the next person to testify, don't hesitate to send a dm.

SEND A DM 📤🔄✅

2w

Cryptocurrency scams are very common, typically advertising a new cryptocurrency platform that is allegedly supported by a high-profile executive. The purpose of this scam is to encourage innocent users to sign up to the fraudulent trading platform, convincing them that it is advisable since a high-profile executive is endorsing and profiting off of it.

Apart from posting messages like the one above, the threat actors post other content in order to encourage users to approach them and increase their trust in them. An abundance of screenshots can be found on the fake executive profiles, containing conversations with other users who allegedly sought their help, displaying their gratitude and marking their achievements. On top of that, many of the posts include screenshots of investment apps, portraying the amounts gained by investing in crypto currency with the help of the fake profiles' guidance. Such as: Looking to gain more insight into the fake profiles and take on the part of the victim in the scam, BlueVoyant analysts conducted an active engagement operation and reached out to two Instagram profiles impersonating the executive.



Receive

TESTIMONIES 6d

6.0612991 BTC

Confirming

0 of 3 Confirmations

Date
07:22 PM on Jun 28, 2023

Amount
6.0612991 BTC

Keep your investment coming

Value
$182,050.99

Value when received
$183,015.89

From
3QeJ7[redacted]Ki7eRr4m

To
Trading Wallet

Description
Add a description

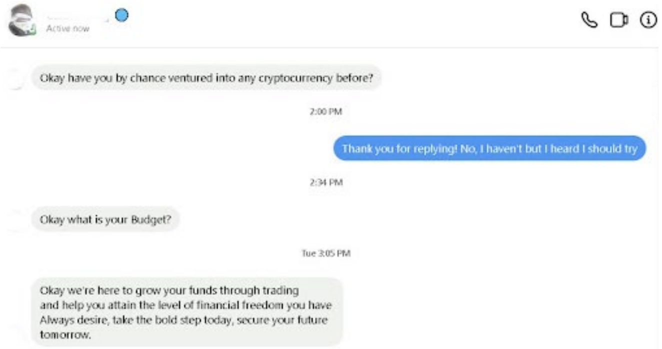
Reply to

View on Blockchain Explorer

Both profiles were active, posting regularly and interacting with users through their posts. Both used the executive's name and picture, and had thousands of followers. When scrolling through both profiles, it is clear that the threat actors have done their homework and continue to do so: both profiles demonstrated knowledge not only in crypto, but also regarding the executive's habits and current activities, personal or work related.

When BlueVoyant's analysts began a conversation with the fake profiles, both threat actors first made sure that their new potential victim had no experience in crypto investing. It may be that the fake profiles prefer targeting inexperienced victims who would be easier to trick and defraud.

After the threat actors' concerns were eased with the knowledge that their new potential victim is a novice, BlueVoyant's analysts were requested to download a legitimate online exchange cryptocurrency app. The fake profiles then instructed BlueVoyant's analysts on how to install the app and create an account. Following the creation of an account on the app, the threat actors encouraged BlueVoyant's analysts to invest more than the minimum capital required by the app in order to "make more profit".



[redacted] Active now

Okay have you by chance ventured into any cryptocurrency before?

2:00 PM

Thank you for replying! No, I haven't but I heard I should try

2:34 PM

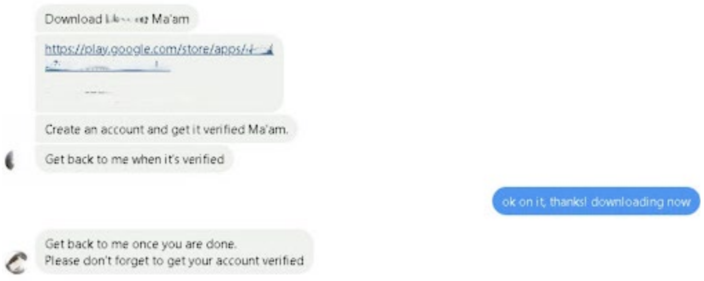
Okay what is your Budget?

Tue 3:05 PM

Okay we're here to grow your funds through trading and help you attain the level of financial freedom you have Always desire, take the bold step today, secure your future tomorrow.

Throughout the conversation, both profiles also encouraged BlueVoyant's analysts to send them screenshots of the app. As mentioned above, this is a method the fake actors use to gain trust since they can post those screenshots on their profile to show how helpful they have been to other users. However, in this case, it appears the fake profiles were hoping that by sending them screenshots, the victim might accidentally also share private information.

In both conversations, the fake profiles were generally very attentive and polite, eager to help, and responsive. Both requested a confirmation after each instruction was carried out, and maintained a sense of urgency. Up to this point, the correspondence seemed relatively legitimate.



Download [redacted] Ma'am

https://play.google.com/store/apps/[redacted]

Create an account and get it verified Ma'am.

Get back to me when it's verified

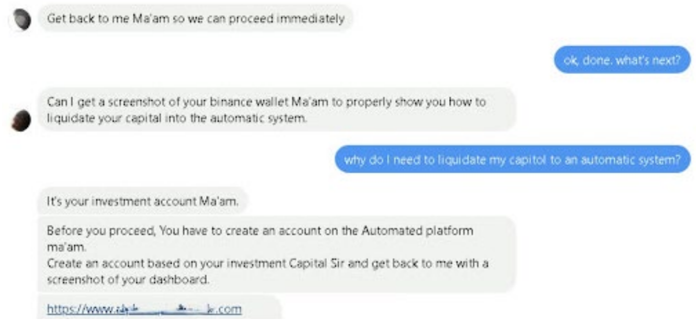
ok on it, thanks! downloading now

Get back to me once you are done.
Please don't forget to get your account verified

Once BlueVoyant's analysts followed the fake profiles' instructions on how to install the app, register and purchase bitcoin, the threat actors moved on to the final stage of the scam: investing.

The first fake profile shared a link to an investment website, instructing BlueVoyant's analysts to sign up and invest the money they had converted to cryptocurrency. At first glance the website seemed to be legitimate. However, upon further investigation, BlueVoyant analysts determined the website was malicious. In addition, several accounts were warning users against using the platform, and it was reported as a scam by an official financial authority.

If a user had indeed followed through with the scam and signed up to this fraudulent platform, they would have been required to disclose private information, which would have been collected by the threat actor.



Get back to me Ma'am so we can proceed immediately

ok, done. what's next?

Can I get a screenshot of your binance wallet Ma'am to properly show you how to liquidate your capital into the automatic system.

why do I need to liquidate my capitol to an automatic system?

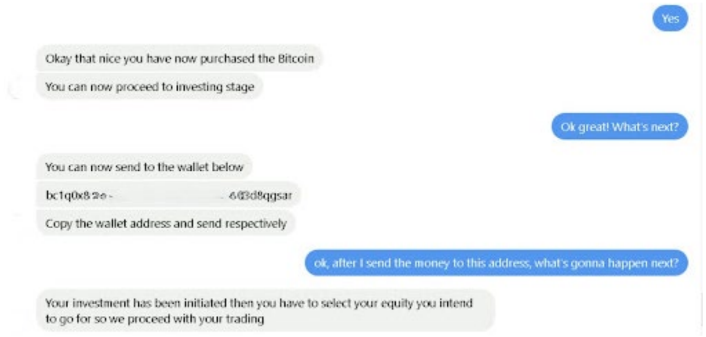
It's your investment account Ma'am.

Before you proceed, You have to create an account on the Automated platform ma'am.
Create an account based on your investment Capital Sir and get back to me with a screenshot of your dashboard.

https://www.[redacted].com

This specific website is currently down, however, it may pop up again or may be replaced by a new website set up by the threat actor, if a new opportunity arises.

The initial engagement with the second fake profile played out largely the same, until the final stage where the threat actor sent BlueVoyant's analysts a Bitcoin address to transfer funds for investment.



Yes

Okay that nice you have now purchased the Bitcoin

You can now proceed to investing stage

Ok great! What's next?

You can now send to the wallet below

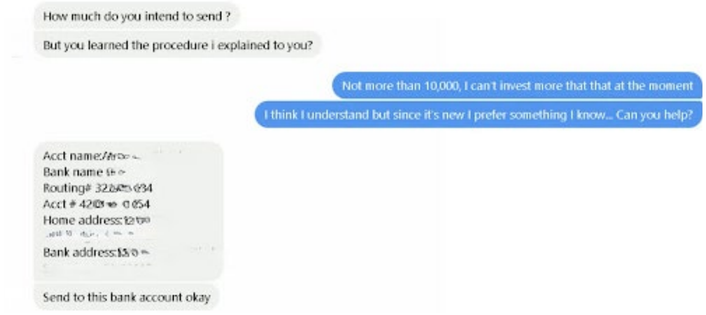
bc1q0x8[redacted]d8qgsar

Copy the wallet address and send respectively

ok, after I send the money to this address, what's gonna happen next?

Your investment has been initiated then you have to select your equity you intend to go for so we proceed with your trading

At this point in the conversation, BlueVoyant's analysts had established trust with the threat actor and claimed that the investment app was too complicated. In turn, the threat actor shared bank account details to transfer the money directly into.



How much do you intend to send ?

But you learned the procedure i explained to you?

Not more than 10,000, I can't invest more that that at the moment

I think I understand but since it's new I prefer something I know... Can you help?

Acct name:[redacted]
Bank name [redacted]
Routing# [redacted]
Acct # [redacted]
Home address:[redacted]
Bank address:[redacted]

Send to this bank account okay

In both cases, innocent users may have been fooled and invested their money via one of the options provided by the threat actors, believing that they made the right choice by contacting and trusting a high-profile executive on a legitimate social media platform, only to discover soon after that they were scammed out of their money.

On the other hand, the threat actors made a well-planned and conscious decision when they chose Instagram as their hub. They built a believable, active and informative profile of a well-known persona. They gained multiple followers, including some verified profiles. They instilled trust in their stories and posts. They were polite, approachable, and eager to help and share their expertise with anyone. It is little surprise that they can follow through with the scam and fool innocent users.

Mitigation Recommendations

It can be challenging to figure out who can be trusted online. Despite all the efforts made by social media platforms to eradicate fraudulent activities, many fall through the cracks, especially since most of the criminals' actions are carried out in private conversations and not in plain sight. However, cybersecurity awareness makes it harder for criminals to fool users . The following are recommendations for both companies and users to combat the threat of executive social media impersonation:

- **Increase cyber awareness on social media:** Companies should provide regular training to employees and clients on how to identify and prevent online impersonation. Verified accounts are generally more trustworthy, but users must be discerning – even verified accounts can be spoofed or hacked. For example, Twitter accounts belonging to Elon Musk, Bill Gates, Jeff Bezos and other incredibly powerful people were all hacked in 2020 as part of a cryptocurrency scam.
- **Protect your privacy:** Users should try to minimize the private information shared on social media to a minimum. Make it harder for an attacker to impersonate you by setting the privacy setting to private on all platforms (if possible), and do not approve any unknown contacts. For executives, instruct your organizations to remove any personal information from executive biographies on company websites.
- **Engage in general preventative actions:** If a user or a company suspects an account to be an impersonating account, report it and ask your friends and family to report the account as well. Furthermore, if a user or a company believes someone is impersonating them on social media, they can also consider filing a complaint with the local law enforcement agency.
- **Continue monitoring and mitigating:** Companies should regularly monitor their online presences to identify any instances of online impersonation of their executives. BlueVoyant's Executive Cyber Guard (ECG) service offers a tailor-made, white glove executive security service. Our ECG services provide detection of executives' digital footprint online, including social media monitoring and remediation of impersonating profiles, which addresses the threats detailed in this report and other non-legitimate threats related to executives.

BlueVoyant cyber defense.

BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native solution by continuously monitoring your network, endpoints, attack surface, and supply chain, as well as the clear, deep, and dark web for threats. The full-spectrum cyber defense solution illuminates, validates, and quickly remediates threats to protect your enterprise. BlueVoyant leverages both machine-learning-driven automation and human-led expertise to deliver industry-leading cybersecurity to more than 900 clients across the globe.

To learn more about BlueVoyant, please visit our website at www.bluevoyant.com or email us at contact@bluevoyant.com

BlueVoyant