

Security Advisory (Mar 2024): A Surge in Sophisticated Job Scams

Singapore has witnessed an alarming rise in job scam incidents in recent months, with significant financial repercussions for victims.

According to a Police Advisory published by the Singapore Police Force on 20 February 2024s, there have been at least 3,066 individuals who lost over \$45.7 million to such scams between 1 October 2023 and 31 January 2024. Additionally, in a separate advisory published on 8 January 2024, at least 180 people were defrauded of about \$2.6 million in December 2023 alone, falling prey to fake job offers that led to substantial money transfers under the guise of securing easy profits.

In contrast to scam tactics that lure individuals with quick monies or free gifts, and are easier to identify, job scams may be more sophisticated, targeting both individuals who may be genuinely looking for legitimate job opportunities or additional income sources. Some scam cases may also involve impersonation of actual and reputable companies, baiting unsuspecting victims into falling for them.

Nonetheless, there are common traits and channels employed by scammers, and these are some of the more common characteristics of job scams:

Channels that Scammers Conduct Their Scams

1. Social Media and Texting Apps

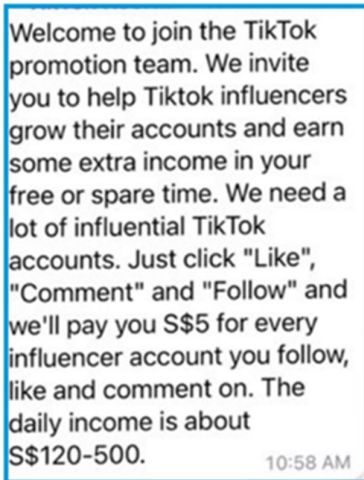
Scammers have been using social media and messaging apps such as WhatsApp and Telegram and even dating apps to target and reach out to potential victims, introducing paid online jobs.

The scammers may also claim they were representatives from social media companies, marketing companies, and online communication companies. One such example will be TikTok.

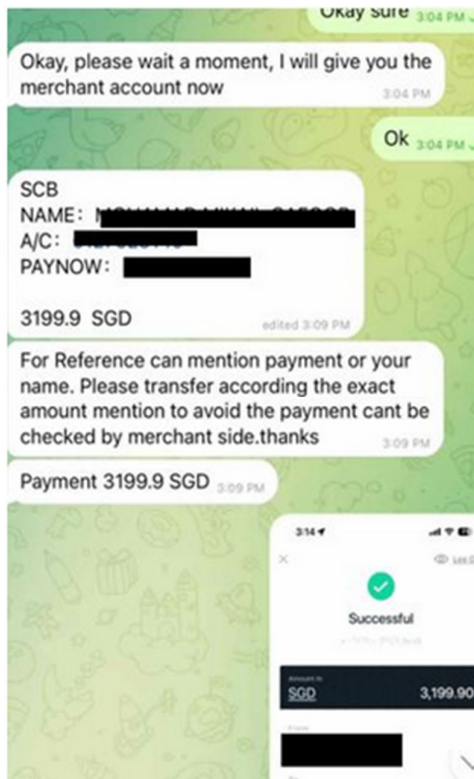
Individuals may be either added to chat groups or approached personally on messaging apps, where they are presented with lucrative commissions to help boost products on e-commerce platforms, or to help generate traction for specific social media accounts. This may include performing simple tasks, which may include:

- following specific TikTok or Instagram accounts, before liking and commenting on the respective posts
- subscribing to YouTube channels,
- liking Spotify songs
- liking posts on websites, eg. Trip.com
- completing surveys, before being persuaded to perform more “advanced” tasks, such as social media boosting, or opening actual accounts on fraudulent websites or mobile apps in order to transfer larger sums of monies to bank accounts or crypto wallets given by the scammers under the pretence of better investment returns
- visit actual e-commerce websites, taking screenshots of products, before making payment to bank accounts/PayNow numbers given by the scammers before seeking refunds and commissions

In some cases, victims may even receive employment contracts to convince them of the authenticity of the job offer. They may also receive real remuneration from the scammers for completing the first few “tasks”, in order to convince them to carry on with the jobs and tasks.



Example of a job offer provided by a scammer impersonating as a team from TikTok (Image source: Singapore Police Force, [Trending Scams in the Past Week 2024-3 \(19 Jan 2024\)](#))



Example of a tasks given by a scammer to transfer payment to a fraudulent “merchant” (Image source: Singapore Police Force, [Trending Scams in the Past Week 2024-3 \(19 Jan 2024\)](#))

iFAST

WELCOME ON BOARD

HEAD OFFICE

Company Location

10 Collyer Quay
Financial Centre
Singapore 049315

February 15 2024

#26-01, Ocean

Fake logo that looks similar to iFAST Corp's logo

Fake onboarding job offer

Scammer impersonating a staff from iFAST Corp to sign off the fraudulent job offer document

I would like to extend a warm welcome to you on behalf of the **iFAST CORPORATION** and leadership team. We are thrilled to have you as part of our team here at **iFAST CORPORATION**, located in the heart **10 Collyer Quay #26-01, Ocean Financial Centre Singapore 049315**

At **iFAST**, we pride ourselves on being more than just a workplace. We are a family, and we hope that you will quickly feel at

home here. We believe that the key to success is creating a supportive and positive environment where our employees can thrive. As part of our team, we are committed to providing you with the tools, resources, and encouragement you need to succeed and grow both personally and professionally. As you start your journey with us, we want you to know that we place great import on the well-being of our employees. We offer a wide range of benefits to ensure that you feel supported and valued, including fair compensation, health and well-being initiatives, job security, career advancement opportunities, and feedback and recognition programs. We also believe in creating a culture of belonging and work-life balance, and we offer a flexible schedule to accommodate your personal and professional goals. In addition, we offer tuition reimbursement, internet reimbursement, and employee discounts, rewards, and bonuses to help you reach your full potential.

We take pride in the success of our employees, and we encourage you to take advantage of the many training and development opportunities that we offer, including career development and personal growth training, as well as 1:1 financial coaching.

As you settle in, you will find that **iFAST** is a dynamic and exciting place to work, full of new challenges and opportunities. Our team is made up of some of the most talented and passionate people in the industry, and we look forward to introducing you to them and helping you become an integral part of our team. Please remember that your success is our success. We expect all of our employees to be dependable, reliable, and committed to following our policies and procedures. We believe that with your openness, follow-through, attentiveness, and willingness to take responsibility, you will thrive in your role at **iFAST**.

In closing, I want to again welcome you to the **iFAST** family. We are delighted to have you on board and look forward to getting to know you better in the coming weeks and months.

Lim Kian Thong Jimmy
Chairman of the Board of Directors
Rep Director and Chairman & CFO
iFAST CORPORATION

Example of a fraudulent job offer letter using a fake logo that looks similar to iFAST Corp’s logo, with the scammers impersonating a staff from iFAST to sign off the fraudulent letter.

2. Job offers on legitimate job-seeking and/or professional portals

Scammers are also utilising legitimate job seeking platforms such as LinkedIn to run their scams as well. Scammers will impersonate companies from well-known companies and offer up fake jobs.

Unsuspecting individuals usually receive direct messages from a “recruiter”, saying that they have the requisite skills for a job position. Scammers may use a flattering or friendly tone, aiming to build trust and encourage individuals to share with them personal information. They may also ask individuals for a virtual interview with an official looking invitation. In other cases, individuals may be asked to undergo a “trial period”, where the individual will be asked to complete certain tasks to prove their competence for a role. After the interview or trial is over, individuals will get an “official” offer letter from the scammer, which usually includes the company’s logo and name to make them appear more authentic.

However, after presenting the job offer, scammers may ask victims for money or personal information, saying it is for equipment like a laptop or to fill out employment paperwork. Again, the scammers may provide “official” documents such as an invoice for equipment.

Victims may only find out they have been scammed after the scammers obtained the victim’s personal information or money and stopped responding to messages and disappearing completely.

From: ROSA hill <rosahillme@gmail.com>
Date: Thu, Feb 8, 2024, 1:52 PM
Subject: WELCOME TO IFAST CORPORATION
To: [REDACTED]

Email sent from non-corporate email domains

Hello [REDACTED]

It was with great pleasure that I learned of your new position **IFAST CORPORATION**. Having known and worked with you, I believe you are ready for such a challenge. You have the necessary skills and experience and will make a terrific Team Leader.

Best of luck as you advance in your career, and please keep me updated as to how things are going!

Sincerely,
Ms. Rosa Hills

Example of a fraudulent job offer email sent from a Gmail account, and not from an official corporate email account.

What can job scams lead to?

Monetary Loss:

Initially offering small commissions, the scammers gradually entice victims with the promise of increased earnings through more complex tasks, ultimately leading victims to transfer large sums to bank or cryptocurrency accounts controlled by the scammers.

The scam often only comes to light when victims find their accounts in deficit, confronted with demands for additional funds to "upgrade" their accounts or when they are unable to withdraw supposed earnings.

In other cases, scammers may ask for cash or digital transfers (PayNow/PayLah) to pay for "equipment" such as laptops or shipping fees

Leak of Personal Information:

Under the guise of "employment papers", Scammers may take their victims personal information like your IC Number, bank account number etc. They will usually ask for these **before** answering any questions about the role. This may lead to scammers using this information to impersonate victims (identity theft).

Tips when encountering these type of scams:

- **Verify:** Always verify the authenticity of job offers provided by strangers, either by contacting the Company through official channels, or by verifying the identity of those approaching you. Never give out any personal information before verifying through legitimate channels and be **wary of any offer that seem too good to be true.**

- **Avoid:** Do not engage with claims made in unsolicited group chats and refraining from clicking on suspicious links or downloading applications from unknown sources.

Check if the email address comes from a work email or a personal one. If it is a personal one, it may

be a scam. **Never pay upfront fees for any job or equipment to be delivered to you, legitimate employers will not ask you to do so.**

- **Prevent:** Set up the privacy function on messaging apps, to prevent getting added by strangers into scam chatgroups.

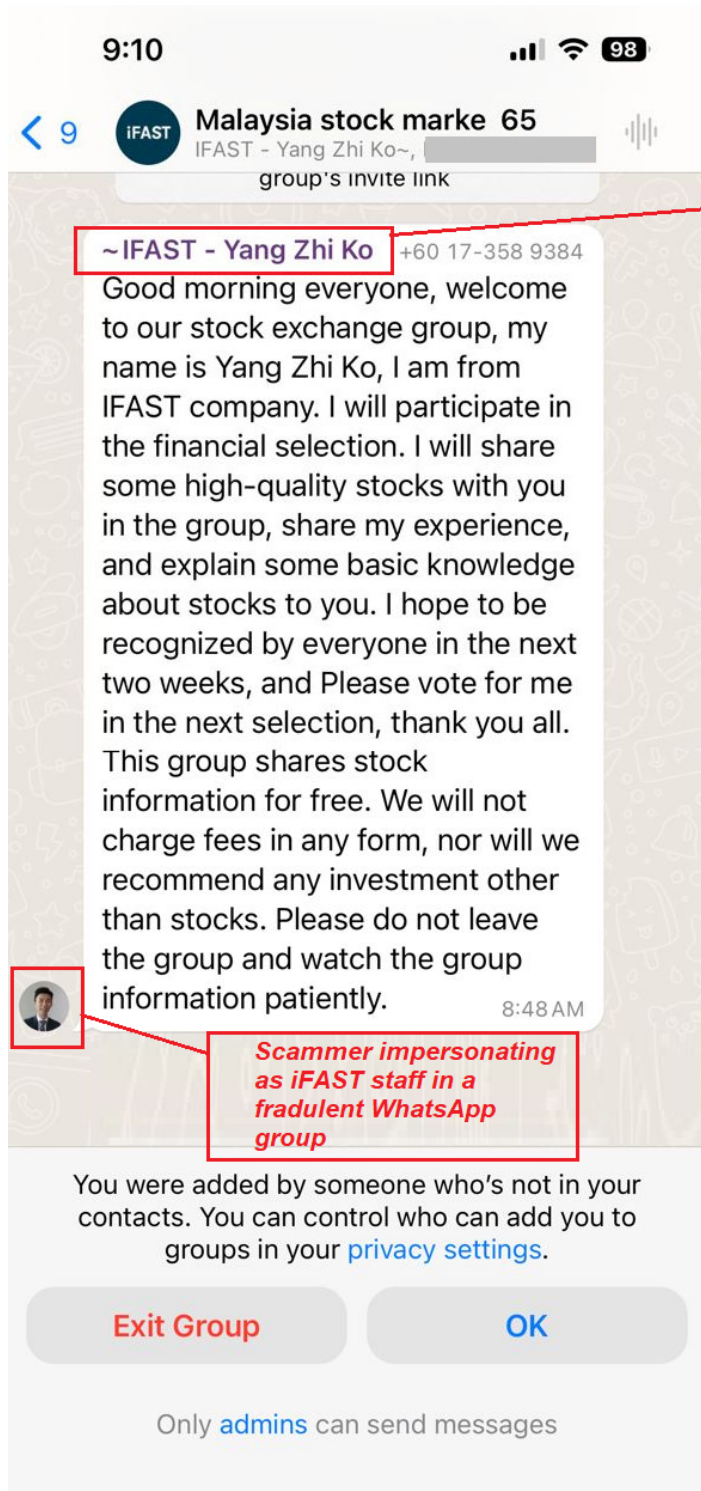
Conclusion:

The frequency of scam cases in Singapore reached an all-time high in 2023, with 9,914 cases (\$135.7 million lost in total) being job scams, making it the most common type of scam in 2023. This disturbing trend emphasizes the need for proactive measures to combat the growing threat of online fraud.

By recognizing the warning signs, protecting personal and financial information, and verifying the legitimacy of job opportunities, individuals can navigate the digital job market more securely.

Singaporeans with details on scams or have doubts about the veracity of messages can call the police hotline on 1800-255-0000, the Anti-Scam Telephone Hotline on 1800-772-6688, or go to www.police.gov.sg/iwitness or www.scamalert.sg

Other Recent Scam Incidents:



Scammer impersonating iFAST staff to share stock tips, while stating that no fees will be charged.

This is likely to be a Pump and Dump scam.

Scammer impersonating as iFAST staff in a fraudulent WhatsApp group

References:

1. Singapore Police Force website, Police Advisory On Job Scams (20 February 2024): https://www.police.gov.sg/media-room/news/20240220_police_advisory_on_job_scams
2. Singapore Police Force website, Police Advisory On Job Scam Involving Social Media Tasks (10 Jan 2024): https://www.police.gov.sg/media-room/news/20240108_police_advisory_on_job_scam_involving_social_media_tasks
3. At least 180 victims lost \$2.6m in December to social media job offer scams (Updated Jan 08, 2024): <https://www.straitstimes.com/singapore/180-victims-lose-26m-in-december-after-falling-for-ruse-involving-social-media-job-offers>
4. 3,066 victims lose over \$45m in job scams between Oct 2023 and Jan 2024 (Updated Feb 27, 2024) : <https://www.straitstimes.com/singapore/3066-victims-lose-over-45m-in-job-scams-between-oct-2023-and-jan-2024>
5. Scammers impersonate well-known companies, recruit for fake jobs on LinkedIn and other job platforms (August 8, 2023) : <https://consumer.ftc.gov/consumer-alerts/2023/08/scammers-impersonate-well-known-companies-recruit-fake-jobs-linkedin-and-other-job-platforms>
6. Exposed: The Dark Side of LinkedIn Job Scammers (April 1, 2023) : <https://www.linkedin.com/pulse/exposed-dark-side-linkedin-job-scammers-sagar-neupane/>
7. Scam Alert Website: www.scamalert.sg.