

Security Advisory: Beware of Impersonation Scams on Facebook and WhatsApp [March 2022]

Received any unexpected calls, emails or text messages claiming to represent iFAST? Before taking further actions, always verify the authenticity of such requests. [Updated on 4 March 2022]

iFAST Corp is committed to the prevention of scams and frauds to safeguard our investors' online privacy and safety.

It has come to the company's attention that there are scammers who may have impersonated as staff of iFAST and/or our subsidiary companies who have either tried to solicit personal information from unsuspecting victims, or to lure them with gifts to participate in promotions or chat groups, or to get them to sign up for investment schemes not offered by the company.

Common channels that scammers use include phone calls, text messages (including on SMSes and messaging applications such as WhatsApp), email, websites, and mobile applications, and some of them may also be fraudulently using the iFAST branding and logos.

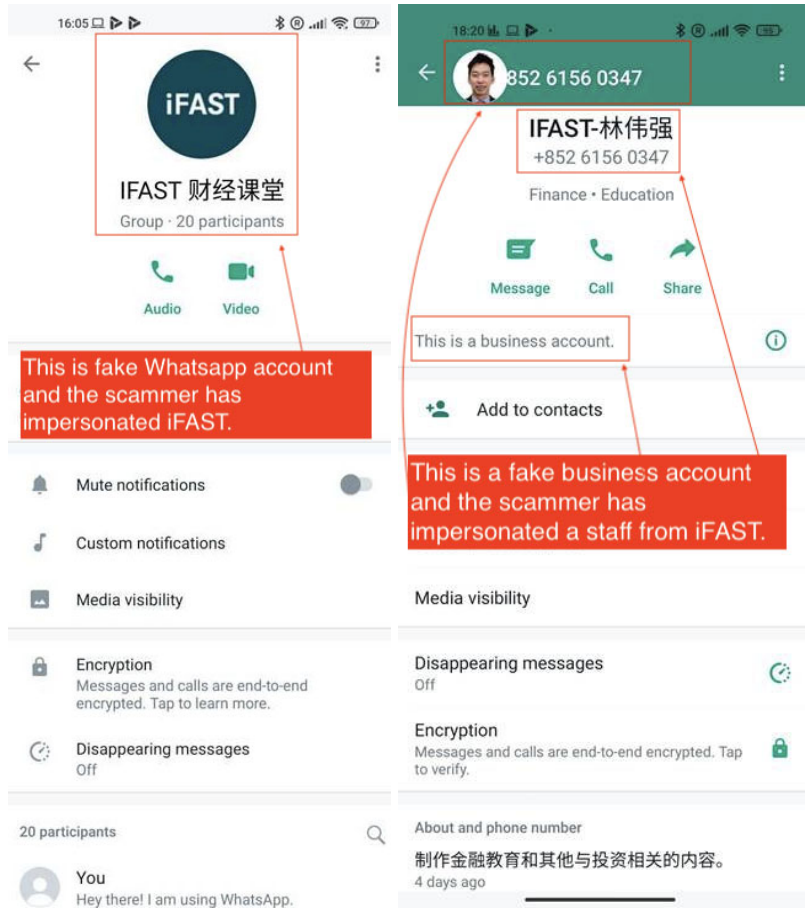
In one recent scam flagged out to us, SMSes in Chinese were sent with the sender's name showing as FACEBOOK or OPPO:

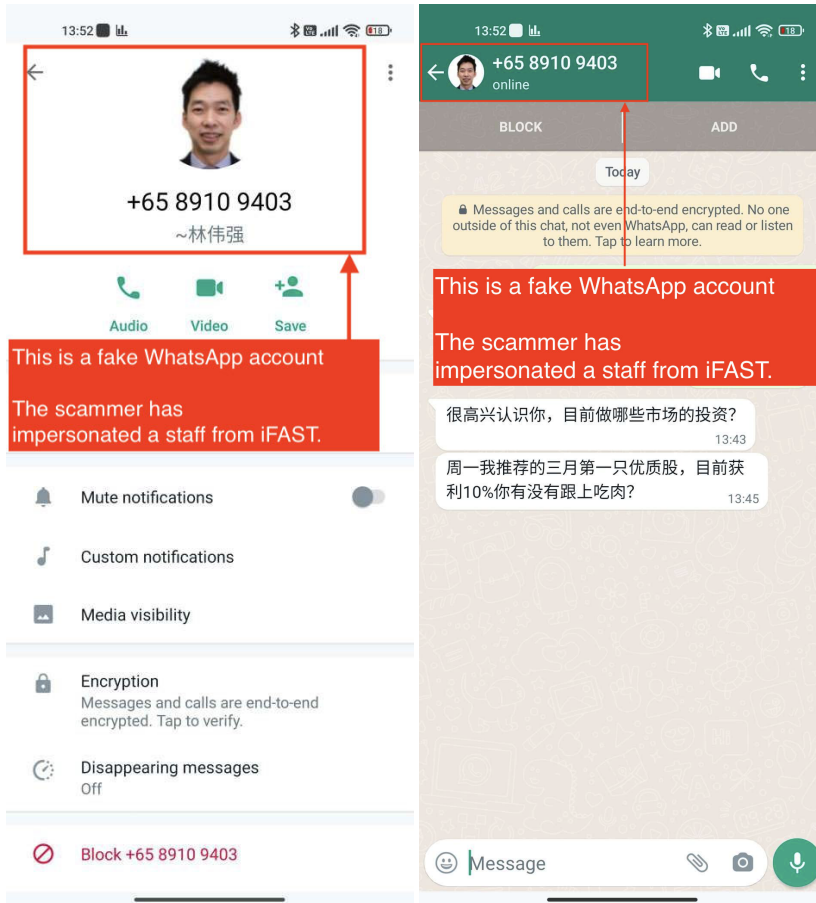


The text message attempted to lure to unsuspecting message recipients to click on an URL link to receive codes for two free stocks. After clicking on the link, the message recipients will be redirected to join a WhatsApp group named “iFAST 财经课堂” (English: “iFAST Financial Classroom”) which is not an official WhatsApp chat group under iFAST and has misused iFAST's logo as its profile photo.

Based on our investigations, the owner of the WhatsApp Group has set up a fake business account and has impersonated a staff from iFAST Singapore and misused his photograph as the profile picture. The scammer

will then initiate conversations to establish contact with the unsuspecting victims and eventually attempt to solicit more information while providing stock tips, encouraging the participant to open accounts with other brokers to follow their investment tips given to trade China A-shares and Hong Kong stocks. These are signs of a Pump and Dump scam.

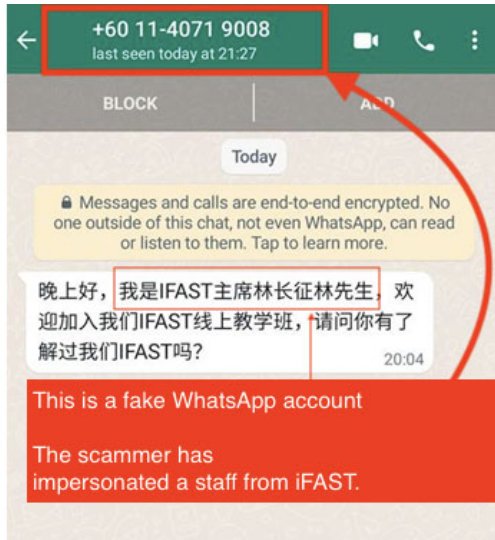




In a separate scam flagged out to us, the scammer impersonated another iFAST staff and sent out spam text messages in Chinese via WhatsApp, attempting to promote and sell online investment courses to unsuspecting victims.



SG_20220304



iFAST would like to reiterate the following points pertaining to impersonation scams:

- If you receive text messages from any individuals claiming to be from iFAST inviting you to participate in any promotions for free gifts, or to join any iFAST-named chat groups or social media groups to receive investment tips, or even to purchase online investment courses, **do not** respond or click on any such links as this could expose you to investment scams such as Pump and Dump scams, malware download, or phishing attacks where your account details could be at risk.
- If you have doubt over the authenticity of the messages that you have received, do not provide any personal details or sensitive information to the message sender, and reach out to iFAST immediately to verify its authenticity:
 - iFAST Corp
 - Official Website: <https://www.ifastcorp.com>
 - Hotline: +65 6535 8033
 - Email Address : ifastadmin@ifastfinancial.com
- If you believe that your investment account has been compromised, or if you have unknowingly provided your account details, passwords and/or other information on any dubious websites, change your account password immediately.