Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-010324-PSA
January 03, 2024

Chinese Police Imposters Incorporate Aggressive Tactics to Target U.S.-Based Chinese Community

The FBI is warning the public about criminal actors impersonating Chinese police officers to defraud the US-based Chinese community, in particular Chinese students attending universities in the United States. The criminal actors tell victims they are being investigated for an alleged financial crime in China and need to pay to avoid arrest. The criminal actors then direct victims to consent to 24/7 video and audio monitoring. The scheme consists of four phases.

Phase 1 - Initial Contact: US business or Chinese Embassy/Consulate Imposter

Criminal actors typically use technology to mask or "spoof" their true telephone numbers, calling victims from phone numbers that appear to be coming from a mobile telephone service provider, a large retailer, a delivery service, or the Chinese Embassy/Consulate. The criminal actors inform victims that their personal identifiable information is linked to either a subject or a victim of a financial fraud investigation.

Phase 2 - Scare Tactics: Chinese Police Imposter

Criminal actors then allegedly transfer the call to a Chinese provincial police department that is investigating them. A criminal actor posing as a Chinese police officer informs victims of the details of the alleged crime and provides fraudulent documentation, such as purported law enforcement credentials, the victim's Chinese national identification photo, and other documents outlining the alleged charges. Criminal actors may pressure victims to return to China to face trial or threaten them with arrest.

Phase 3 - Surveillance of Victims

Criminal actors direct victims to consent to 24/7 video and audio monitoring due to the alleged sensitivity of the investigation and/or to demonstrate the victims' innocence. Victims are instructed not to discuss the details of the case, not to conduct internet searches, and to report all their daily activities.

Phase 4 - Final Act: Extortion of Victims

Criminal actors instruct victims to wire a large sum of money to a Chinese bank account to prove their innocence or to post bail to avoid having to return to China. In some instances, criminal actors direct victims to lie to friends and family to secure additional money, to serve as a money mule, or to facilitate similar criminal schemes against other Chinese students in the United States.

TIPS TO PROTECT YOURSELF

- If an unknown individual contacts you to accuse you of a crime, do not release any personal identifiable or financial information and do not send any money. Cease any further contact with the individual.
- Contact from a seemingly official phone number is not proof of official action. Criminal actors may use technology to disguise or "spoof" the actual number they are calling from to appear as a trusted number.
- If you are contacted by any government agency for an allegedly official purpose, you may verify the contact is official by (1) using public sources (phone book, internet, etc.) to identify the government agency's contact information then (2) directly contacting the agency to confirm the legitimacy of the interaction.
- Do not consent to 24/7 video or audio monitoring.
- If you believe you have been contacted by an individual claiming to be a Chinese authority, contact your local FBI field office. Foreign government officials conducting legitimate law enforcement activity in the United States must act in coordination with US federal authorities.

REPORT IT

The FBI requests victims report these fraudulent or suspicious activities to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov as quickly as possible. Be sure to include as much transaction information as possible, such as wire instructions, wallet addresses, telephone numbers, and text or email communications.

In addition, the FBI recommends taking the following actions:

- Report the activity to the payment service provider used for the financial transaction.
- Contact your financial institution immediately to stop or reverse the transaction. Ask the financial institution to contact the corresponding financial institution where the funds were sent.
- Report activity to your campus security or public safety office to elevate awareness within the student population.

Criminal actors may use similar tactics to target other members of the Chinese community, not necessarily Chinese students in the United States.

For additional information on similar scams or fraudulent activity, please see the previous Public Service Announcements:

IC3 | Criminals Pose as Chinese Authorities to Target US-based Chinese Community
IC3 | 繁體中文版 (in Chinese - Traditional Written)

IC3 | 简体中文版 (in Chinese - Simplified Written)