

China-Born "Romance Scam" Spread Overseas: Cyber-Forensics.net Alerts Dating App Users

MELBOURN, VICTORIA, AUSTRALIA, November 14, 2021 /EINPresswire.com/ -- China-Born "[Romance Scam](#)" Spread Overseas: [Cyber-Forensics.net](#) Alerts Dating App Users



Codenamed "Romance Scam," the massive global "pig butchering strategy" in China is now spreading to Japan, the United States, Malaysia, Singapore, and Hong Kong. As reported by FTC, the faulty investment schemes cost a record-breaking \$304 million financial loss in 2020.

Cyber-Forensics.net, an industry leader in providing cyber-forensics services for victims of online scams, recently unveiled how offenders assume fake online identities to trick victims.

Fewer opportunities to go out amid the pandemic wave forced people to look for partners online through applications like Tinder, Bumble, OkCupid, Hinge, and Happn.

The reports highlight unidentified scammers creating fake profiles to gain the trust of the potential victims and lure them into investing millions.

In the past year, China created apps like Study Xi, Strong Nation, and similar apps to profess the teachings of their Chinese president and Communist Party leader Xi Jinping. The app converted the teachings of the Chinese president into a game and allowed awarding points to frequent log-ins, time spent reading and watching videos. The Study Xi app soon became the most downloaded app in China.

In what seemed like Chinese government officials chatting on apps, the imposters had other intentions. The app users began targeting women to dupe them of millions of renminbi (the official currency of China) by claiming their official positions. The scammers claimed that their higher positions prevented them from using other social media apps or dating apps.

Later around April, a security audit by the Open Technology Fund discovered that the app contained a code amounting to a digital backdoor which allowed complete administrator-level

access to a user's phone.

The matter attracted global attention and initiated worldwide investigations showcasing worrying implications towards the increasing cases.

In October, Hong Kong Police arrested 32 people for selling their bank accounts to fraudsters who later used them to launder more than HK\$9 million (the US \$1.2 million) in 2021. The police charged five men and 27 women with cyber deception and ensured further probing.

The details revealed that approximately HK\$35 million came from 26 romance scams and 29 investment frauds, all taking place between February 2020 to January 2021.

In June 2021, Singapore and Malaysian police simultaneously joined the operations to dismantle Malaysia's transnational internet love scam syndicate.

The large-scale operations brought arrests in connection with an international financial fraud unveiling of victims in Singapore, losing S\$64,000 and eight other victims in Malaysia, losing RM3.7 million (S\$1.2 million) in total.

Cyber-Forensics.net released new insights into international trading scams, which have already cost nations heavily, and the most impacted countries might be Japan and the United States.

National Consumer Affairs of the Center of Japan uncovered the figure of surging romance scam cases reaching new levels in the first four months of 2021.

The suspects used social media websites and online dating websites to find and connect with the potential victims based on incident reports.

Other modus operandi criminals use are cryptocurrencies and business email compromises where email accounts are manipulated to change bank details. The suspects concoct their sob stories and berate their victims.

The attackers target middle-aged women, tech-savvy young professionals, and other vulnerable individuals who start looking for partners after feeling lonely in the pandemic only to plow them of hundreds of dollars.

With the functionality of sophisticated trading apps, the offenders persuade the target to install [fake cryptocurrency trading](#) apps and collect personal data, install managing apps for malicious purposes, and add or remove accounts.

Cyber-Forensics.net warns budding investors to avoid falling victims to these types of scams. Users should only install apps from authentic stores. The golden rule is to step back from sending any amount to anyone you barely know or haven't met in person.

There are additional news reports from the UK of such scams where one victim learned that he lost \$87000 to a scammer who contacted them through Facebook.

The reports suggest that scammers plan months building their trust to feel genuine before convincing you to make fraudulent get-rich-quick schemes investments. A classic part of the routine includes posting attractive pictures, quickly striking a friendship, and beginning to message every day.

The scammers go to extreme lengths to hook you into the idea by showing positive returns in the beginning. And once the victim can see profit, they typically continue to encourage victims to invest more money only to find out that the money's gone.

Cyber-Forensics.net has always insisted that victims report the scams to the police to help others identify tricks such as obtaining bank account details. And if it has already happened, they need to check their computers for viruses and ensure to change passwords.

A cyber forensic scan on the computer can help mitigate risks that hostile anti-viruses may overlook. In addition to this, victims should gather sufficient knowledge of fund recovery scams that promise or guarantee money return. There is a possibility that criminals may re-target their victims in different ways.

If you believe the statistics, nearly one-third of the deceived people learn about the scam after already losing their amount.

It is important to consult experienced investigators before you send any amount to people you hardly know. Cyber Criminals often manipulate victims to keep their relationships private. This should be a red flag for anyone meeting people online that they do not know.

If you have already lost your money, you can contact experienced investigators like Cyber-Forensics.net to analyze your situation and guide you through the process to recover your money.

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams..Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. For more information, please visit <https://cyber-forensics.net>.

Peter Thompson

Cyber-Forensics.net

+1 917-920-6613

[email us here](#)

Visit us on social media:

[Twitter](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/555989873>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.