Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

18 July 2022

PIN Number

20220718-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Cyber Criminals Create Fraudulent Cryptocurrency Investment Applications to Defraud US Investors

Summary

The FBI is warning financial institutions and investors about cyber criminals creating fraudulent cryptocurrency investment applications (apps) to defraud cryptocurrency investors. The FBI has observed cyber criminals contacting US investors, fraudulently claiming to offer legitimate cryptocurrency investment services, and convincing investors to download fraudulent mobile apps, which the cyber criminals have used with increasing success over time to defraud the investors of their cryptocurrency. The FBI has identified 244 victims and estimates the approximate loss associated with this activity to be $42.7 million. The FBI encourages financial institutions and their customers who suspect they have been defrauded through fake cryptocurrency investment apps to contact the FBI via the Internet Crime Complaint Center or their local FBI field office.

Threat

Cyber criminals are creating fraudulent cryptocurrency investment apps to exploit legitimate cryptocurrency investments, defrauding US investors and causing reputational harm to US investment firms. Innovative financial institutions offer mobile apps to enhance user experience and increase legitimate investment. Cyber criminals seek to take advantage of the increased interest in mobile banking and cryptocurrency investing. The FBI has observed cyber criminals using the names, logos, and other identifying information of legitimate USBUSs, including creating fake websites with this information, as part of their ruse to gain investors. Financial institutions should warn their customers about this activity and inform customers as to whether they offer cryptocurrency services.

- Between 22 December 2021 and 7 May 2022, unidentified cyber criminals purporting to be a legitimate US financial institution defrauded at least 28 victims of approximately $3.7 million. The cyber criminals convinced victims to download an app that used the name and logo of an actual US financial institution and deposit cryptocurrency into wallets associated with the victims' accounts on the app. When 13 of the 28 victims attempted to withdraw funds from the app, they received an email stating they had to pay taxes on their investments before making withdrawals. After paying the supposed tax, the victims remained unable to withdraw funds.

- Between 4 October 2021 and 13 May 2022, cyber criminals operating under the company name YiBit[1] defrauded at least four victims of approximately $5.5 million. The cyber criminals convinced the victims to download the YiBit app and deposit cryptocurrency into wallets associated with the victims' YiBit accounts. Following these deposits, 17 victims received an email stating they had to pay taxes on their investments before withdrawing funds; all 4 victims could not withdraw funds through the app.

- Between 1 November and 26 November 2021, cyber criminals operating under the company name Supayos, AKA Supay[2], defrauded two victims by instructing them to download the Supay app and make multiple cryptocurrency deposits into wallets associated with their Supay accounts. In November 2021, the cyber criminals told one victim he was enrolled in a program requiring a minimum balance of $900,000 without his consent; upon trying to cancel the subscription, the victim was instructed to deposit the requested funds or have all assets frozen.

[1] YiBit was a former legitimate cryptocurrency exchange that appeared to close in 2018.
[2] Supay is a fraudulent company using the same name as a currency exchange provider in Australia. The FBI believes the cyber criminals are using this name to appear more legitimate.

Recommendations

The FBI recommends financial institutions take the following precautions:

- Proactively warn customers about this activity and provide steps customers can take to report it.
- Inform customers as to whether the financial institution offers cryptocurrency investment services or other related services and methods to identify legitimate communications from the institution to customers.
- Inform customers whether the financial institution has a mobile application.
- Periodically conduct online searches for your company's name, logo, or other information to determine if they are associated with fraudulent or unauthorized activity.

The FBI recommends investors take the following precautions:

- Be wary of unsolicited requests to download investment applications, especially from individuals you have not met in person or whose identity you have not verified. Take steps to verify an individual's identity before providing them with personal information or relying on their investment advice.
- Verify an app is legitimate before downloading it by confirming the company offering the app actually exists, identifying whether the company or app has a website, and ensuring any financial disclosures or documents are tailored to the app's purpose and the proposed financial activity.
- Treat applications with limited and/or broken functionality with skepticism.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.