Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-042624-PSA
April 26, 2024

New Verification Schemes Target Users of Online Dating Platforms

The FBI warns of "free" online verification service schemes in which fraudsters target users of dating websites and applications (apps) to defraud victims into signing up for recurring payments. Unlike romance scams involving investment-confidence schemes, commonly referred to as pig-butchering[1], where victims are convinced to transfer large amounts of money over time, the so called "free" verification schemes involve recurring and costly monthly subscription fees. Additionally, fraudsters collect the information entered by victims at registrations (e.g., emails, phone numbers, and credit card information) and use it to commit further fraudulent activity such as identity theft or selling the information on the dark web.

HOW THE SCHEME WORKS

Fraudsters meet victims on a dating website or app. Fraudsters express an interest in establishing a relationship and quickly move the conversation off the dating app or website to an encrypted platform. Under the guise of safety, the fraudster provides a link that directs the victim to a website advertising a "free" verification process to protect against establishing a relationship with predators, such as sex offenders or serial killers. The website displays fake articles alluding to the legitimacy of the website. The verification website prompts the victim to provide information such as their name, phone number, email address, and credit card number to complete the process. Once the victim submits the information, they are unwittingly redirected to a private, low-quality dating site charging costly monthly subscription fees. Eventually, the victim's monthly credit card statement displays a charge to an unknown business.

Verification Scheme	
	Meets on an online dating website or app; Expresses interest in establishing a relationship
	Quickly directs communications off the dating website to an encrypted platform
	Sends a “verification link” promoting protection from predators such as sex offenders or serial killers; directs you to register
	Articles on the link appear to be from trusted media logos using scare tactics to coerce you to register
	Link prompts you to enter sensitive information: name, phone number, email address, credit card information
	Monthly credit card statement displays a costly subscription charge to an unknown company

TIPS TO PROTECT YOURSELF

- Avoid clicking on links, downloading files, or opening attachments from someone you only met online. Only open attachments from known senders and scan all attachments for viruses, if possible.
- Avoid moving the conversation from a reputable dating site's messaging service, since many of these offer some safety features.
- Report suspicious user profiles to the dating site administrator and cease all contact with suspicious users.
- Be cautious of someone you only met online professing their love quickly, expressing a need for help, and/or enticing you with provocative pictures and text topics. Fraudsters use social behavior to deceive you and separate you from your hard-earned money.
- Do not provide sensitive information to someone you only met online. Regularly monitor your personal financial accounts for irregularities, such as recurring charges to unknown businesses.
- Contact your credit card issuer/bank as soon as possible if you discover what appears to be a fraudulent transaction. Explore the possibility of closing that credit card.
- Use one credit card with a limited balance or consider using virtual credit cards when subscribing to new online services.
- Avoid websites that use scare tactics to coerce you to register for a service. Search the source of all information to determine its legitimacy.
- Stay updated about the latest fraud schemes by following the FBI IC3 website or other financial government websites.

The FBI requests victims report fraudulent, suspicious, or online criminal activity to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov.

[1] *PSA, Alert Number I-100322-PSA, dated 3 October 2022, "Cryptocurrency Investment Schemes."* ↩