# Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

**August 05, 2019**

Alert Number
**I-080519-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

## Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules

### WHAT IS CONFIDENCE/ROMANCE FRAUD?

Confidence/romance fraud occurs when an actor deceives a victim into believing they have a trust relationship—whether family, friendly, or romantic—and leverages the relationship to persuade the victim to send money, provide personal and financial information, or purchase items of value for the actor. In some cases, the victim is persuaded to launder money on behalf of the actor.

Actors often use online dating sites to pose as U.S. citizens located in a foreign country, U.S. military members deployed overseas, or U.S. business owners seeking assistance with lucrative investments.

### THREAT

In 2017, more than 15,000 people filed complaints with the FBI's Internet Crime Complaint Center (IC3) alleging they were victims of confidence/romance fraud and reporting losses of more than $211 million. In 2018, the number of victims filing these complaints increased to more than 18,000, with more than $362 million in losses—an increase of more than 70 percent over the previous year.

In 2018, confidence/romance fraud was the seventh most commonly reported scam to the IC3 based on the number of complaints received, and the second costliest scam in terms of victim loss.

IC3 receives victim reports from all age, education, and income brackets. However, the elderly, women, and those who have lost a spouse are often targeted.

### METHODS

After establishing their victims' trust, scammers try to convince them to send money for airfare to visit, or claim they are in trouble and need money. Victims often send money because they believe they are in a romantic relationship.

For example, an actor claims to be a U.S. citizen living abroad. After a few months of building a relationship with the victim, the actor asks the victim to send gifts or electronics to a foreign address. After a few more months, the actor expresses a desire to return to the U.S. to meet the victim. The actor claims not to have the money to pay for travel and asks the victim to wire funds. In some cases, the actor claims the wired funds did not arrive and asks the victim to resend the money.

Some actors provide a fake travel itinerary. When they don't arrive as scheduled, they claim they were arrested, and ask for more money to post bail. They may also request more money for travel or to recover assets seized during their "arrest." Requests for money may continue until the victim is unable—or unwilling—to provide more.

### TRENDS

In some situations the victim may be unknowingly recruited as a "money mule": someone who transfers money illegally on behalf of others. Actors groom their victims over time and convince them to open bank accounts under the guise of sending or receiving funds. Grooming is defined as preparing a victim to conduct fraudulent activity on their behalf through communications intended to develop a trust relationship. These accounts are used to facilitate criminal activities for a short period of time. If the account is flagged by the financial institution, it may be closed and the actor will either direct the victim to open a new account or begin grooming a new victim.

In other situations, the actor claims to be a European citizen or an American living abroad. After a few months of developing trust, the actor will tell the victim about a lucrative business opportunity. The actor will inform the victim there are investors willing to fund the project, but they need a U.S. bank account to receive funds. The victim is asked to open a bank account or register a limited liability company in the victim's name and then to receive and send money from that account to other accounts controlled by the actor.

### TIPS TO PROTECT YOURSELF

Most cyber criminals do not use their own photographs; they use an image from another social media account as their own. A reverse image search can determine if a profile picture is being used elsewhere on the internet, and on which websites it was used. A search sometimes provides information that links the image with other scams or victims.

To perform a reverse image search on profile photos:

- Right click on the image and select "Search for image."
- Right click again and select "Save image as" to save the photo to your device.
- Using a search engine, choose the small camera icon to upload the saved image into the search engine.

Always use your best judgment. While most dating sites routinely monitor account activity and investigate all complaints of falsified accounts, most dating site administrators do not conduct criminal background checks when an account is registered. Keep in mind it is always possible for people to misrepresent themselves. Do not ignore any facts which seem inconsistent and be aware of the following common techniques used by romance scammers:

- Immediate requests to talk or chat on an email or messaging service outside of the dating site.
- Claims that your introduction was "destiny" or "fate," especially early in communication.
- Claims to be from the U.S. but is currently living, working, or traveling abroad.
- Asks for money, goods, or any similar type of financial assistance, especially if you have never met in person.
- Asks for assistance with personal transactions (opening new bank accounts, depositing or transferring funds, shipping merchandise, etc.).
- Reports a sudden personal crisis and pressures you to provide financial assistance. Be especially wary if the demands become increasingly aggressive.
- Tells inconsistent or grandiose stories.
- Gives vague answers to specific questions.
- Claims to be recently widowed or claims to be a U.S. service member serving overseas.
- Disappears suddenly from the site then reappears under a different name using the same profile information.

The FBI advises:

- Never send money to someone you meet online, especially by wire transfer.
- Never provide credit card numbers or bank account information without verifying the recipient's identity.
- Never share your Social Security number or other personally identifiable information that can be used to access your accounts with someone who does not need to know this information.

### WHAT TO DO IF YOU ARE A VICTIM

If you are a victim of a confidence/romance scam, the FBI recommends taking the following actions:

- Report the activity to the Internet Crime Complaint Center, your local FBI field office, or both. Contact IC3 at www.ic3.gov. Local FBI field offices can be found online at www.fbi.gov/contact-us/field.
- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.
- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.
- Report the activity to the website where the contact was first initiated.