

# LA BEOC

LOUISIANA BUSINESS EMERGENCY OPERATIONS CENTER

February 15, 2023

*Supporting business during a disaster*



In the last few weeks, there has been much talk about **ChatGPT** and how it is changing online interaction. One area that has not been discussed is its effect on online dating and romance scams.

Romance scams are some of the lucrative for those with bad intentions. The main reason these scams are successful is pride. No one wants to admit that someone has scammed them. They are even less likely to admit to the scam if it was through an “online” relationship.

Chatbots or programs that can mimic human conversation and interaction are making these romance scams harder to detect. AI programs can even use pictures that appear like selfies to lure unsuspecting people.

According to Robert Falzon, head of engineering at cybersecurity provider Checkpoint Canada, “Hackers in the old days used to be really terrible at grammar and spelling. He said, Now using the assistance of artificial intelligence and automating tools, they’re getting much better... and these emails are much harder to discern from real emails that you might receive.”

Please be wary that the person you’re talking to online may not be what they appear.

#### REFERENCES

Lavery, I. (2023, February 12). Is your valentine a chatbot? Experts urge caution amid rising AI scams. Retrieved from Global News: <https://globalnews.ca/news/9475788/romance-scams-artificial-intelligence-valentines-day/>

Be Safe,  
Jim

#### **James 'Jim' Williams**

Public-Private Partnership Operations Officer  
Informatics Research Institute  
University of Louisiana at Lafayette  
[james.williams@louisiana.edu](mailto:james.williams@louisiana.edu)  
337.482.0633

Greetings from NIMSAT!

This month, I want to talk about the risk of romance scammers – those looking for love on Valentine’s Day or any other day of the year.

According to the FBI, “Romance scams occur when a criminal adopts a fake online identity to gain a victim’s affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.”

In a [Forbes](#) article, the Federal Trade Commission reported “in 2022, nearly 70,000 people reported a romance scam, resulting in \$1.3 billion in losses, with a median loss of \$4,400 with the vast majority of frauds not disclosed to the government.” They suggest that less than 3% of victims submit a complaint to the government, such as the police, FBI, or any other law enforcement entity.

Forbes continues that the method of contact may vary, but there are some common themes in the relationship’s development. They report the scammers will claim to be stationed on a faraway military base, working on an offshore oil rig, or overseas. They may also claim to be sick, disabled, or in jail, and let you know from the initial contact that meeting in real life could be a challenge.

Likewise, they recommend looking for the following in identifying a scammer:

- ***They often seem too good to be true.***
- ***They fall in love or want to engage in first contact.***
- ***They use poor grammar or syntax.***
- ***They mix romance or business opportunities for investment advice or requests.***

“What can I do to protect myself and my loved ones from scammers?” Next, here is a list of steps from Forbes you can take to protect yourself:

- ***Be wary – don’t jump in with both feet.***
- ***Be stingy – never provide your bank account or routing number to someone you meet online.***
- ***Be smart – never send money or agree to invest with anyone you meet online.***
- ***Be curious- if something doesn’t add up, ask questions.***
- ***Be patient – take your time to learn about the person and their intentions.***

Remember, as with all cybersecurity, prevention is key. Learn how to identify a scammer and what you can do to protect yourself, your business, and your loved ones. By employing these useful tips, you can ensure that you do not fall prey to an online scammer.

For more information, I encourage you to visit:

<https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes>.

Stay Safe and Stay Aware!

Shannon



**Shannon Strother, PhD**  
Director, NIMSAT  
Informatics Research Institute  
University of Louisiana at Lafayette  
[shannon.strother@louisiana.edu](mailto:shannon.strother@louisiana.edu)  
337.482.0609

Latest News

Helpful Links

Follow @LABEOC



The LABEOC is managed by the [National Incident Management Systems and Advanced Technologies Institute](#) at the University of Louisiana at Lafayette, in partnership with the [Governor's Office of Homeland Security & Emergency Preparedness](#) and [Louisiana Economic Development](#).

[Join our Email List](#)

[Preference Center](#)