Hearts of Darkness: How Romance Scams Have Swept

SOCIAL MEDIA

Alliance to Counter Crime Online

“If it’s illegal IRL, it should be illegal to host it online.”

THE PROBLEM

The Internet has become Ground Zero for romance scammers who lurk in chat rooms and on social media sites and dating apps hunting for victims.

FAKE

Romance scammers steal images from real, innocent people to create fake profiles. People whose identities have been stolen and used in romance scams often struggle to get social media platforms to remove them.

Victims of romance scams often lose tens of thousands of dollars, and many end up experiencing severe emotional consequences.

Many perpetrators of online romance scams can be easily identified by their pattern of online behavior. But social media platforms like Facebook and Instagram have been reluctant to take action against them.

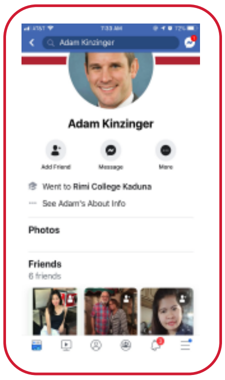
THE SPECIFICS

In romance scams there are generally two types of victim — the person whose identity is exploited and the person who is financially manipulated.

Identity theft victims tend to be people who hold positions of trust, such as military service members, veterans and doctors. Some victims have had their images used in hundreds of scams.

The Purported location of the scammer is always far from where the real person actually resides. The scammer may or may not use the identify theft victim's real name.

Scam victims tend to be elderly and/or people who have recently lost spouses or children. Scammers look for people they identify to be lonely and vulnerable.



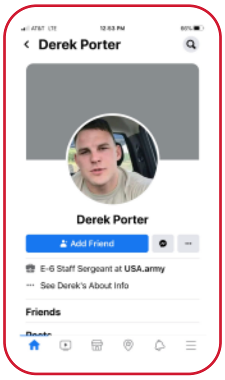
Adam Kinzinger

Went to Rimi College Kaduna

See Adam's About Info

Photos

Friends
6 friends

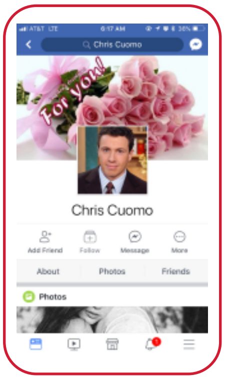


Derek Porter

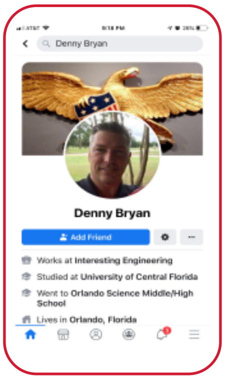
E-6 Staff Sergeant at USA.army

See Derek's About Info

Friends



Chris Cuomo



Denny Bryan

Works at Interesting Engineering

Studied at University of Central Florida

Went to Orlando Science Middle/High School

Lives in Orlando, Florida

Authorities are tracking multiple romance scam gangs operating out of West Africa, particularly Nigeria, a country where computer savvy criminals have cooked up a wide range of Internet scams.

West Africa is not the only source of romance scams. There have also been cases emanating from Canada, Ghana, India, Turkey and the United Kingdom.

In some situations the victim may be unknowingly recruited as a “money mule,” someone who transfers funds illegally. Money from romance scams has also been diverted to extremist groups like Boko Haram.

Outdated or non-existent laws and lax enforcement mean tech firms can profit off romance scams and face scant liability.

LEARN MORE

Find ACCO research and media coverage at www.counteringcrime.org.

Alliance to Counter Crime Online

KEYS FACTS AND FIGURES

The New York Times estimates that the number of fake online profiles has steadily risen to about 120 million accounts across Facebook's family of platforms, which includes Instagram and WhatsApp.

$475 million

The FBI's Internet Crime Complaint Center calculates that online romance scams cost American victims more than $475 million in losses in 2019 alone. This number is likely just the tip of the iceberg, as many fraud victims are too ashamed to report this type of crime.

Two ACCO experts, Kathy Waters and Bryan Denny, are leading the fight against the romance scam problem. Together they founded Advocating Against Romance Scammers (AARS), which raises awareness and pushes for legal reform to counter romance scams and identity theft.

HOW IT WORKS

A romance scammer downloads images of an upstanding citizen, such as a doctor, first responder, or member of the military. These images are stolen from publicly available online sources.

After establishing a fake profile on social media or a dating site, the scammer reaches out to innocent people, liking their images or sending flattering messages.

The scammer's intention is to establish a relationship as quickly as possible, endear themselves to the victim, and gain trust.

Scammers may propose marriage and make plans to meet in person. Eventually, they will ask for money.

Scammers rarely ask victims to send bank wire transfers or funds through Western Union or PayPal. Instead, they ask for hard-to-trace gift cards that can be turned into cash.

CURRENT LAW

Creating fake profiles to scam people for money violates community standards set by major Internet platforms including Facebook, Instagram and Google. Tech firms have implemented procedures to ensure people use their real identities, but criminals have found loopholes they can be exploited. There's currently no law forcing tech firms to remove false profiles.

Section 230 of the 1996 Communications Decency Act (CDA230) grants immunity to any provider of an "interactive computer service" for user-generated content. This means that social media platforms and dating apps can host romance scams with zero liability for the harm they have facilitated.

PROPOSED LEGAL REFORM

It's time for Congress to reform CDA230 and explicitly strip out immunity for identity theft. Two bills introduced in Congress, H.R. 6586 "Social Media Accountability and Account Verification Act," and H.R. 6587 "Social Media Fraud Mitigation Act," aim to do just that.

ACCO'S MISSION

The Alliance to Counter Crime Online is a team of security experts, academics, NGO leaders, and citizen investigators who have come together to push organized crime and terror activity off Internet platforms.

What to do if you think you are being scammed:

If things are not adding up in an online relationship, here are some things you can do:

- Perform a reverse image search in Google Images to see if a suitor's profile picture is being used elsewhere or by others.
- Copy and paste a section of the personal profile language into the Google search bar to see if it's being used by people with different profile pictures.
- If the suitor claims to be far away, in Syria, for instance, have them photograph themselves in front of a famous Syrian monument or holding an edition of that day's local newspaper.
- Ask them to take a selfie holding up a toothbrush or standing on one leg within an alloted timeframe. The scammer won't be able to do so because the photo they'd provide would not match their profile picture.

LEARN MORE Find ACCO research and media coverage at www.counteringcrime.org.

Alliance to Counter Crime Online