Heartfelt Hoaxes: Avoiding Relationship Scams

What are they exactly, and why are they relevant?

Relationship scams happen when scammers impersonate people we trust, such as friends, family members, or romantic partners. They create believable stories to gain our trust, and once they establish an emotional bond, they manipulate us into giving away money or sensitive information. The consequences of falling victim to these scams can include:

- Stolen money
- Compromised identity credentials
- Involvement in other crimes, such as money laundering and investment fraud

It's common to encounter scams that begin when someone befriends you online or through social media platforms like Facebook. Once you become emotionally invested in the relationship and feel comfortable, they typically make a request for money. Spotting these scams can be challenging because they rely on emotional manipulation. When you develop feelings for someone or feel attached to someone, it becomes easier to overlook warning signs, which is why these scams continue to be successful.

★ ***Social media platforms*** are online tools that let users create, share, and interact with content. Popular platforms include Facebook, X, Instagram, TikTok, and LinkedIn.

We will be discussing two types of relationship scams:

- Romance Scam
- Grandparent Scam

Romance Scam

Romance scams occur when fraudsters create fake personas or digital profiles to target victims, pretending to develop a romantic interest in individuals who are genuinely seeking a real connection.

- The majority of romance scams originate online, though in-person meetings can also happen.
- Scammers often target individuals in vulnerable situations, such as older widowers and divorcees.

How can you avoid a Romance Scam?

1. Make decisions without letting emotions influence you, even if a friend or potential partner seems caring and persistent.

2. Use tools like **TinEye** to reverse image search their profile photos to check if they appear on other sites with different names or locations.

★ ***TinEye i****s a reverse image search engine. You can submit an image to TinEye to find out where it came from, how it is being used if modified versions of the image exist, or to find higher-resolution versions.*

★ ***A reverse image search*** *is a tool that lets you upload an image to find out where else that same image appears online. This can help you trace the origin of a picture. If you suspect a romance scam, it's a good idea to use this tool to check if the profile picture of your potential partner is being used by someone else online. This could indicate a fake identity and a scam.*

3. Be careful about sharing personal pictures or videos, especially if you haven't met someone in person. Scammers sometimes use compromising material to blackmail their targets after a relationship ends.

4. Limit the personal information you share on social media. Scammers can use your information and photos to create fake identities or target you.

5. Discuss your online friendships with people you know in real life.

How can you identify a Romance Scam?

It is quickly labeled as "love"

Individuals enticed into a virtual connection are ***"love bombed"*** and encouraged to leave the dating app to communicate through messaging apps like Snapchat, WhatsApp, and Telegram.

- ★ ***Love bombing*** is a way to control someone using intense attention, affection, and gifts. This often happens at the start of a relationship. The person receiving this affection may feel overwhelmed and believe they owe something to the love bomber.

Requests for gifts or financial assistance

Scammers often create convincing scenarios that tug at your heartstrings to solicit gifts or financial assistance, claiming they are in trouble. They may even encourage you to invest in schemes linked to cryptocurrency.

- ★ ***Cryptocurrency*** is a type of digital money that uses cryptography for security.
- ★ ***Cryptography*** is the study of ways to keep communication and data safe from unauthorized access or changes.

Excuses for not meeting in person or appearing on video chat become a recurrent pattern

A typical tactic used by scammers is to propose an initial in-person meeting. However, shortly before the meeting is set to occur, they often create an excuse to cancel, making the victim feel sympathetic toward their situation. This manipulation causes the victim to overlook the importance of upholding commitments.

The primary goal of online dating or romance scams can differ

- Scammers sometimes seek personal information from their victims, leading to identity theft.
- In other instances, they may persist with the scam for months or even years, attempting to defraud you of as much money as possible.

Romance Scammers Favorite Lies

- *"I or someone close to me is sick, hurt or in jail."*
- *"I can teach you how to invest."*
- *"I'm in the military far away."*
- *"I need help with an important delivery."*
- *"We've never met, but let's talk about marriage."*
- *"I've come into some money or gold."*
- *"I am on an oil rig or ship."*
- *"You can trust me with your private pictures."*

Quick Facts

- Romance scams typically unfold over a period of time, lasting weeks, months, or years.
- Anyone, regardless of age, gender, cultural background, education, or income level, can fall victim to these scams.
- Many romance scammers begin by offering to do a favor for their targets.

What to Do If You Suspect a Romance Scam

You can approach these schemes from two perspectives. *As a victim* or *by looking out for someone you suspect is a victim.*

If you are the victim of a Romance Scam

➔ First and foremost, the same principle applies to any online scam: **"Cease communication immediately."**

➔ If unsure whether something is a scam, consult someone you really trust. Don't feel embarrassed to ask for help; as mentioned earlier, these scams can affect anyone. Remember, you are not alone—having the support of friends and family can make it easier to navigate the situation.

➔ Make sure to document everything. For example, if the communication took place on Facebook, take screenshots to have supporting evidence for your case if you need to report it.

➔ Report the incident. This allows involved institutions to develop better practices and implement policies to prevent and combat cybercrime.

If a person you know is the victim of a romance scam

➔ **Take action before it happens**

- ◆ Check-in on your loved ones who may feel lonely or isolated.
- ◆ Discuss with vulnerable loved ones how they can protect themselves online.
- ◆ Talk to them about monitoring their personal and financial accounts.

➔ **If you suspect they are being scammed, approach the topic gently and discuss your concerns with them.**

- ◆ Avoid shaming or embarrassing the victim. When dealing with a romance scam, the victim may have formed an emotional attachment to the scammer. If you scold them, you risk pushing them away from you and further towards the scammer.

➔ **Suggest stepping back and slowing down communication with the person in question or cutting off contact entirely**

- ◆ Observe their reactions and let empathy guide the conversation. This type of scam can lead victims to feel shame and guilt. Be an active listener and try to understand their perspective.

Grandparent Scam

This type of fraud involves someone impersonating a family member, such as a grandchild, niece, or nephew. Scammers typically contact elderly victims over the phone, posing as these relatives. They may use the family member's name, which can often be found online or on social media, or they might begin the conversation with phrases like, **"Hi Grandpa, it's me."** The goal is for the victim to mention the grandchild's name, reinforcing the scammer's deception. By exploiting this familial relationship, scammers create a false sense of security that can cloud the victim's judgment, leading them to take actions they usually wouldn't.

- The grandparent scam is based on **"Social Engineering"** techniques. The scammer often pressures victims to take immediate action regarding their claims, involving the urgent transfer of a large sum of money to *"save"* a family member.
- Scammers often target older adults because they are generally more trusting. Scammers may also believe that this age group is more likely to have significant savings, own homes, and maintain good credit, making them attractive targets.
- To deceive their victims, scammers might impersonate police officers, hospital staff, or government officials.

Narratives Behind the Grandparent Scam

Scammers can be persuasive because they often have specific information about the grandchild or family member. They may use spoofed phone numbers that appear to belong to the grandchild, and sometimes, they even use voice software to imitate the grandchild's voice.

1. **Legal Trouble:** The scammer, posing as the grandchild, claims to need financial assistance to cover legal fees or fines urgently.
2. **Medical Trouble:** The individual impersonating the grandchild alleges that they have been seriously injured in an accident and describes an emergency that requires immediate funds for medical treatment, hospital bills, or transportation back home.
3. **International Trouble:** The scammer claims that the grandchild is stranded in a foreign country and facing unexpected challenges, such as being arrested or dealing with a travel-related emergency.

At the heart of these false claims are unclear details intended to instill fear and urgency. Scammers work hard to prevent you from hanging up the phone, insisting that if you do, you won't be able to ***"post bail"*** for your family member or ***"confirm that the money has been received."*** Their goal is to ensure you do not hang up and verify the accuracy of the information they have provided.

What To Do If a Scammer Calls You Pretending To Be a Family Member

Slow down and trust your gut

Consider these facts: *Is this person truly your grandchild? What evidence do you have? Are there any red flags?* Look out for these phrases:

"Don't tell Mom and Dad." Scammers want to keep you from discussing this with anyone who might reveal their scheme.

"A lawyer will contact you." Scammers try to gain credibility by mentioning authority figures. Avoid sharing any information until you can verify their identity.

Verify the Caller's Identity

Don't let your guard down just because the number or caller ID looks familiar.

Ask Specific Questions: Inquire about personal details that only your grandchild would know. If they can't answer, hang up and call your family member directly.

Contact Relevant Agencies: If the caller claims to be a police officer or lawyer, verify their identity by contacting their organization. If they have no record of the person or situation, it's likely a scam.

Protect Yourself from Scammers

If someone calls and says, ***"Hi Grandma, it's me,"*** do not share your grandchild's name. Wait for them to provide it, or ask directly. If they cannot, it is likely a scam.

Don't give your address or personal information to anyone who calls you. Scammers are always on the lookout for information they can use against you. Don't let them have it.

Check your social media privacy settings. Make sure your social media settings are private and that you share as little personal information publicly as possible. This will prevent fraudsters from using this information to scam you.

Contact a trustworthy family member or friend

If you receive a call from someone claiming to be a distressed family member, it's important to verify the situation:

Contact someone else in the family to get more information about the alleged emergency.

Share your concerns. Explain the call to this trusted person, who can help confirm or deny the situation. In most cases, your grandchild or family member is safe.

Be Cautious of Specific Payment Requests

Scammers often ask for payments through methods that are difficult to trace, such as wiring money, sending gift cards, or using payment apps. These methods can significantly hinder your chances of recovering funds. If someone requests payment in this way, it's likely a scam. *Always confirm the recipient's identity 100% before sending any money.*

Here are some payment methods that should raise red flags:

- **Gift Cards:** Scammers frequently request payment via gift cards (like Amazon) because they are untraceable. No legitimate agency or authority will ever ask for payment in gift cards.
- **Wire Transfers or Payment Apps:** Sending money through wire transfers is like giving away cash. Once you send it, you cannot get it back. This applies to payment apps like Zelle and Cash App as well.
- **Cash Pick-Up:** No legitimate organization will send a courier to pick up cash payments from you.

Did You Send Money To a Scammer? Here's What To Do

If you or someone you know has conducted a financial transaction with a scammer—whether through a gift card, wire transfer, credit card, debit card, or cryptocurrency—while your money might be considered lost for good, there is still hope.

- ➔ Contact the company that issued your gift card. Tell them it was used in a scam and ask for a refund. Keep the gift card and the receipt.
- ➔ Call the wire transfer company and explain that the transfer was fraudulent.
- ➔ Contact the bank or company that issued your credit or debit card and let them know it was a fraudulent charge.
- ➔ Inform your bank about the unauthorized debit or withdrawal.
- ➔ Remember that cryptocurrency payments usually cannot be reversed. Once you send cryptocurrency, you can only get your money back if the person you paid returns it. Still, contact the company you used to send the cryptocurrency and report it as fraudulent.

Report Fraud to the FTC and Local Authorities

It is crucial to report all scams to the appropriate authorities. Doing so can help stop cybercriminals and prevent others from becoming victims. Here are the key agencies to contact:

1. Federal Trade Commission (FTC): Report all fraud cases to the FTC to assist them in tracking the latest scams. You can also call their toll-free hotline at 1-877-382-4357.

2. Local Law Enforcement Agency: File a report with your local police department to initiate an investigation into the crime. Additionally, consider contacting your state's Attorney General and consumer protection office for further assistance.

3. FBI's Internet Crime Complaint Center (IC3): If you have fallen victim to a scam, you can report it to the FBI at IC3.gov


Connecting Generations
Cyber-Seniors™


be well
ILLINOIS


aetna®


BEYOND
FORCE


trail
TOTAL RETIREE ADVANTAGE ILLINOIS

Definitions

- ★ **Caller ID** is a telephone service that shows the caller's phone number on the receiver's phone. When the call is connected, it works with analog and digital systems, including voice-over IP.
- ★ **Cybercrime** is a criminal activity done using computers and the Internet.
- ★ **Dating apps** are online platforms that help people find romantic relationships or companionship. Users build profiles to share information about themselves and what they seek. They can browse other users' profiles and interact with them. These apps use algorithms to suggest matches based on compatibility, location, and other factors.
- ★ **Identity theft** occurs when someone obtains and uses another person's personal information without permission, such as their name, Social Security number, credit card information, or other identifying details.
- ★ **Online forums** are websites where people can post messages, ask questions, and share information on many topics. Each forum usually has specific sections, called "boards," for different subjects. This setup lets users have discussions, seek advice, and exchange ideas.
- ★ **Search engines** help you find information online, like a digital detective. When you type in a question, it looks through an extensive collection of web pages to show you the most relevant results. Popular search engines include Google, Bing, and Yahoo.

- ★ **Social engineering** uses psychological manipulation to deceive users into making security errors or revealing sensitive information.

- ★ **Social media privacy settings** allow you to control who can access your personal information, posts, and contact details. You have authority over the following:
  - Who can see your posts
  - Who can contact you
  - Who can view your personal information
  - Who can access your contact details

- ★ **Spoofed phone numbers** can mislead you about the identity of a caller by disguising the number that appears on your caller ID. Scammers often use this technique to conceal their true identity and make it seem like they are calling from a trusted source, such as a bank or government agency.

- ★ **Voice-over IP (VoIP)** is a technology that allows users to make phone calls over the Internet instead of traditional phone lines.