FLORIDA CONSUMER
NEWSLETTER
February 2024
A publication of the Florida Department of Agriculture and Consumer Services

5 SIGNS OF ROMANCE SCAMS

As online dating continues to rise in popularity, unfortunately, so do romance scams. The Federal Trade Commission reported last year that losses from romance scams hit a staggering $1.3 billion in 2022, the most recent year for which complete data is available.

The Federal Bureau of Investigations says a romance scam occurs 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.

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, but that will never happen. Eventually, they will ask for something of value. That ask may include one of the following: money for a medical emergency, unexpected legal fee, or travel expenses to visit the victim; Personally Identifying Information (PII) that can be used to drain existing bank accounts or set up fake accounts in the victim's name; or sensitive or personal photos or information that can be used to extort money from the victim.

So, how do you protect yourself from romance scams? By keeping your eyes open – and your arms wrapped around your money and your PII. Here are five romance scam red flags to look for:

1. Your new love interest quickly asks to move your communication off the dating service or social media platform where you met. They will want to contact you privately through your personal email or phone.
2. They will share their photo with you but won't join a live call or chat where you can actually see them.
3. They profess love right away, after messaging for only a short period of time and before you have met in person.
4. They don't use your name, but rather use terms of endearment such as sweetheart and honey. This is usually because they are juggling many different victims and it's easier to use a term of endearment as opposed to running the risk of using the incorrect name.
5. They claim to have an urgent need to get money – for instance, they have a family or medical emergency and are unable to get to their funds.

When it comes to romance scams, fraudsters don't discriminate on age or income. Anyone who meets people online is a potential victim. To safeguard yourself, never give out your account information or wire money to someone you've only met online.

If you have been a victim of a romance scam, there are several steps you should take:

- Call your bank or credit card company and let them know if you have given out your account number or other information.
- File a complaint with the FBI's Internet Crime Complaint Center at IC3.gov.
- Report it to the FTC at ReportFraud.ftc.gov.
- Report it to the online service through which first contact was made, e.g., dating website, social media service, etc.

Visit FloridaConsumerHelp.com and click on **Scams and Fraud** to learn more about romance scams and what to do you if you think you or a loved one may be entangled in one.

SCAMMERS USE PROMISE OF TAX REFUNDS TO STEAL ID

By Larissa Bungo, Senior Attorney, Federal Trade Commission

Got an email or text message about a tax refund? It's a scam.

IRS impersonators are at it again. This time, the scammers are sending messages about your "tax refund" or "tax refund e-statement." It might look legit, but it's an email or text fake, trying to trick you into clicking on links so they can steal from you. How? They tell you to click a link — supposedly to check on your "tax refund e-statement" or "fill out a form to get your refund." But it's a scam and if you click that link, the scammer might steal your identity or put malware on your phone or computer.

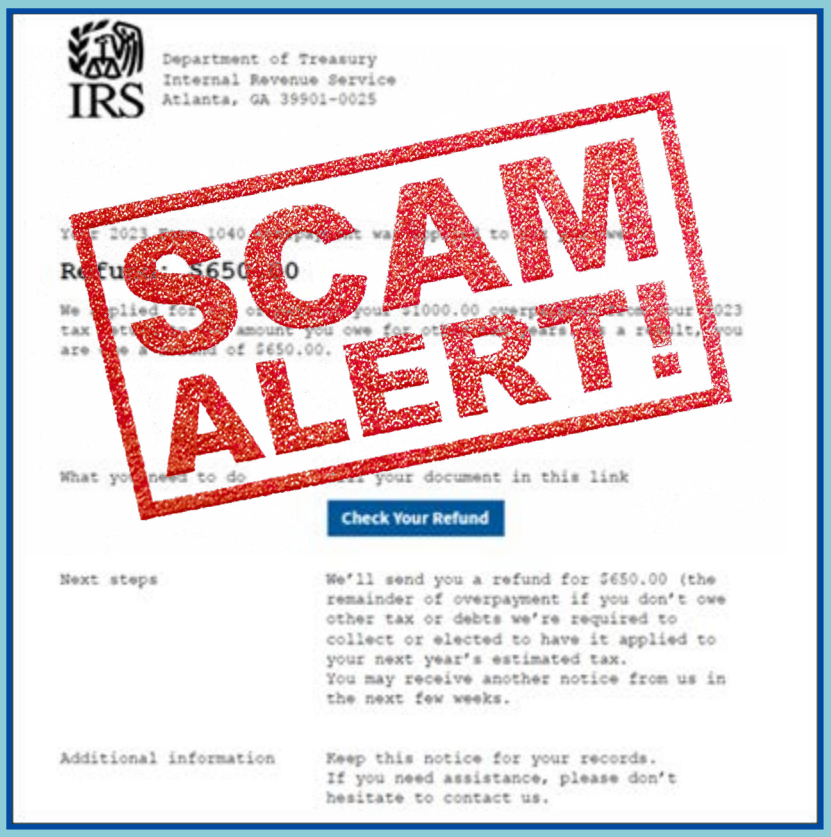
If someone contacts you unexpectedly about a tax refund, the most important thing to know is that the **real IRS won't contact you by email, text message, or social media** to get your personal or financial information. Only scammers will.

If someone does reach out, here's what to do:

- **Never click on any links**, which can put malware on your computer or phone, letting scammers steal from you.
- **Check the status of any pending refund on the IRS official website**. Visit Where's My Refund to see if you're really getting a refund.
- **Share what you know**. By telling your friends and family members about the scam, you can help protect your community.

If you clicked on a link in one of these messages, or you shared personal or financial information, report it at IdentityTheft.gov to get a free, customized recovery plan.

If you see this or any other a scam, even if you didn't lose money, report it to the FTC at ReportFraud@ftc.gov.



ARTIFICIAL INTELLIGENCE IN MODERN SCAMS

Artificial intelligence has experienced a massive resurgence in the past 10 years to become more widespread, powerful, and easier to use than ever before. A few of the recent developments in AI have led to its use in detecting cancer, predicting equipment failure for manufacturing, and detecting fraud in banking. Consumer demand for AI enhanced products and services has led to a nearly $98 billion annual investment in AI research and development worldwide.

While there are many positive benefits to AI, scammers are notorious for bending positive applications to work their nefarious schemes. Deepfakes, AI-developed images that look nearly identical to a real-life person, and voice clones, which can mimic the voice of a loved one, can easily deceive victims into giving away valuable personal information or money. In these cases, AI amplifies the impact of scams, enhancing their believability and emotional appeal through personalization. Any person, of any age, can fall victim to these highly convincing scams.

Some of the most common scams utilizing these deepfake and cloning techniques are impostor scams, generally known as emergency scams or grandparent scams. These scams usually begin with a call or a text that appear to be coming either from a loved one, most often a child or grandchild, or someone that might speak with authority, like law enforcement or an attorney's office. The AI-generated voice on the other end of the line can quickly convince the intended victim that their loved one needs immediate assistance, usually in the form of some monetary payment made through a method that is quick and irreversible.

Scammers may be using new technologies to make their scams more effective, but they continue to deploy many of the same tactics used in more traditional scams. Avoiding scams requires vigilance, awareness, and careful consideration of the information and requests you receive. Here are some steps you can take to protect yourself from falling victim to AI-enhanced scams:

- **Stay Informed**: Knowledge is your first line of defense. Educate yourself about common types of scams and how they operate, including the latest advancements in AI and how it may be used in scams. This awareness can help you spot suspicious activities.
- **Verify Requests**: Verify the identity of individuals or organizations before sharing any sensitive information or making financial transactions. Use official contact information from reliable sources, not information provided in unsolicited messages or calls.
- **Be Cautious of Unsolicited Messages**: Be skeptical of unexpected emails, messages, or calls, especially if they request sensitive information, ask for money, or promise unrealistic returns.
- **Check URLs and Links**: Hover over links in emails to see the actual URL destination before clicking. Be cautious of shortened URLs and unfamiliar domains.
- **Use Strong Authentication**: Whenever possible, use strong and unique passwords, enable multi-factor authentication (MFA), and consider using password managers to keep your accounts and devices secure.
- **Guard Personal Information**: Be cautious about sharing personal information online or on social media platforms. Scammers might use this information to personalize their scams. It only takes about 30 seconds worth of a person's voice for AI voice generating software to create a voice clone.
- **Beware of Urgent or Threatening Language**: A scammer's goal is to get you to send payment before you get a chance to think about it or discuss it with a trusted family member or friend. If you receive a call with a family member's voice, reach out directly to that family member or call their work number of other family members to verify the story.
- **Trust Your Instincts**: If something feels off or too good to be true, it probably is. Exercise caution and always check with a trusted source or individual.
- **Report Suspicious Activity**: Report suspected scams to relevant authorities, your bank, or any platform you're using. Reporting helps prevent others from falling victim.
- **Be Aware that Deepfakes are Possible**: Be cautious of video or voice calls that seem unusual or unexpected, even if they appear to be from someone you know. Verify the caller's identity through other means if possible. Be skeptical of anyone who pushes back on questions or requests for time to verify identity or circumstances.

Visit FloridaConsumerHelp.com and click on Scams and Fraud to find more information about Artificial Intelligence and Scams.

FCC TAKES ACTION AGAINST ROBOTEXTS

The Federal Communications Commission recently adopted new rules to further protect consumers from scam communications by directly addressing some of the biggest vulnerabilities in America's robotext defenses and closing the "lead generator" robocall/robotexts loophole. The new rules allow blocking of "red flagged" robotexting numbers, codifies do-not-call rules for texting, and encourages an opt-in approach for delivering email-to-text messages.

Combating Robotext Sources

The new rules allow the FCC to "red flag" certain numbers, requiring mobile carriers to block texts from those numbers. The rules also codify that Do-Not-Call list protections apply to text messaging, making it illegal for marketing texts to be sent to numbers on the registry. And the order encourages providers to make email-to-text messages an opt-in service, which would limit the effectiveness of a major source of unwanted and illegal text messages.

Closing the Lead Generator Loophole

The new rules close a loophole through which unscrupulous robocallers and robotexters inundate consumers with unwanted and illegal robocalls and robotexts. The new rules make it unequivocally clear that comparison shopping websites and lead generators must obtain consumer consent to receive robocalls and robotexts one seller at a time – rather than have a single consent apply to multiple telemarketers at once.

Groundwork for Future Steps

In addition to the rules, the Commission also proposed and will take public comment on additional steps it might take against robotexts. This notice proposes additional blocking requirements when the FCC notifies a provider of a likely scam text-generating number. The Commission will also seek further comment on text message authentication – modeled on the successful implementation of STIR/SHAKEN protocols for phone calls – including on the status of any industry standards in development. The notice also proposes requiring, rather than simply encouraging, providers to make email-to-text services opt-in.

Visit FloridaConsumerHelp.com to file a complaint or to find more information on Scams and Fraud and Florida's Do Not Call List.

GET READY FOR THE BIG GAME

If you are planning on having friends and family over to watch the big game, take timeout to serve food safely. Watch our Food Safety for the Big Game short video to learn several food safety practices for your upcoming gathering. Tips include:

- Use a food thermometer to ensure your foods are properly cooked. Make sure chicken wings are cooked to an internal temperature of 165˚F.
- Be sure to separate ready-to-eat foods from raw food like raw meat, poultry, seafood, and eggs to help prevent cross-contamination and foodborne illness.
- Refrigerate leftovers within 2 hours to decrease the risk of foodborne illness.

Visit the Division of Food Safety's Consumer Resources and Outreach website to find helpful videos, flyers, and more listed by category and season!

ABOUT THE FDACS DIVISION OF CONSUMER SERVICES

FDACS is Florida's state consumer protection agency responsible for regulating charities and handling consumer complaints. FDACS handles more than 400,000 consumer complaints and inquiries, oversees more than 500,000 regulated devices, entities, and products like gas pumps and grocery scales, performs over 61,000 lab analyses on products like gasoline and brake fluid, performs nearly 9,000 fair ride inspections, and returned over $2.8 million to consumers through mediations with businesses.

The Division of Food Safety monitors food from the point of manufacturing and distribution through wholesale and retail sales to ensure the public of safe, wholesome and properly represented food products.

CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.

The Consumer Product Safety Commission provides consumer product recall information as part of the agency's mission to protect consumers and families from hazardous products.

CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.

The Florida Department of Agriculture and Consumer Services is the state's clearinghouse for consumer complaints, protection and information. Consumers who would like information about filing a complaint against a business or who believe fraud has taken place can visit us online at FloridaConsumerHelp.com or contact the department's consumer protection and information hotline by calling 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) for Spanish speakers.