# Tips to Protect Yourself

Do not share sensitive information by phone, email, text, or social media.

Do not transfer or send money to people or accounts you don't know.

Consider establishing a 'safe word' that you only share with family members and close contacts.

Do not share any personal or sensitive information with an online chatbot.

Report potential scams to the authorities and the companies involved.

## For More Information on Protecting Yourself and Others:

The Federal Trade Commission (FTC):
www.consumer.ftc.gov/scams

*U.S. Senate Special Committee on Aging*

## Fraud Hotline

The Aging Committee operates a toll-free Fraud Hotline that serves as a resource for older Americans and their family members to report suspicious activities and provides information on reporting fraud and scams to the proper officials, including law enforcement.

**1-855-303-9470**

Monday – Friday • 9 AM to 5 PM ET

The Committee's annual Fraud Book helps consumers recognize common scams, spot red flags, and protect themselves from bad actors.

Find it here:
**www.aging.senate.gov/scam**

# Emerging Threat: Artificial Intelligence




**Senator**
**Rick Scott (R-FL)**

*Chairman*

**Senator**
**Kirsten Gillibrand (D-NY)**

*Ranking Member*



UNITED STATES SENATE
SPECIAL COMMITTEE on AGING
CHAIRMAN RICK SCOTT

# What is AI?

Artificial Intelligence (AI) enables machines to mimic certain human-like behavior, such as speaking or writing.

While AI can be a useful tool in some circumstances, bad actors can exploit it to make scams more convincing.

## Three Terms to Know

### Chatbots:

A chatbot is a computer program that may use AI to simulate human conversation and could be used maliciously to obtain, store, or manipulate your personal data.

### Voice Cloning Technology:

Voice cloning uses AI to mimic a person's voice, including that of someone you know.

### Deepfakes:

A deepfake is an authentic-looking AI-generated video or image.

## AI-Powered Scams to Watch Out For

### Phishing Attacks

Using AI, scammers can quickly personalize phishing emails, imitate dialogue, and bypass spam filters, making it harder for individuals to distinguish between genuine and fraudulent communications.

### Family Emergency Scams

Scammers can utilize voice cloning and deepfakes to impersonate a loved one who claims they are in danger and need money.

### Romance Scams

Fraudsters can use AI technology to operate fake profiles on dating websites and social media platforms. AI-powered chatbots then simulate realistic conversations to build trust, with the goal of tricking the target into sending them money.

## Examples of AI in Fraud and Scams

It can be hard to tell whether someone is using AI in a scam, especially as AI has made traditional fraud and scams easier to deploy at scale and even more convincing.




**Fake Family Emergency Scam**

***Transaction Update: Your account is being debited for an iPhone 13: USD $599.97. Not you? Call Amazon at (888)*** ******

**Fake Text Message**