Tips to Protect Yourself

- Do not share sensitive information via phone, email, text, or social media.
- Do not transfer or send money to unknown locations.
- Consider designating a "safe word" for your family that is only shared with family members and close contacts.
- Do not provide any personal or sensitive information to an online chatbot.
- Report potential scams to the authorities and the companies involved.

For More Information on How to Protect Yourself and Others:

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

The Consumer Financial Protection Bureau (CFPB):
https://www.consumerfinance.gov/consumer-tools/fraud/

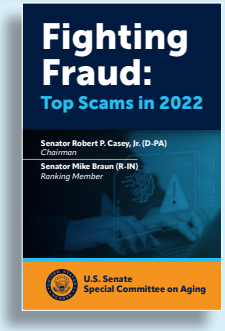
U.S. Senate
Special Committee on Aging

Fraud Hotline

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

1-855-303-9470

Monday – Friday • 9 AM to 5 PM ET

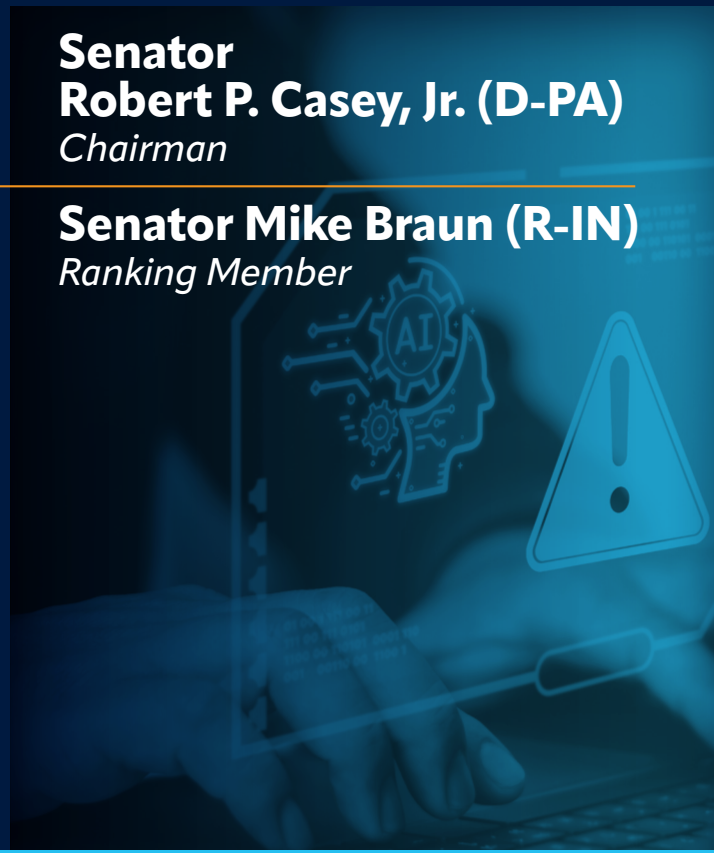


The Committee's annual Fraud Book educates consumers on common scams, red flags to watch for, and tips to protect against bad actors. Find it here:
www.aging.senate.gov.

Emerging Threat: Artificial Intelligence

Senator
Robert P. Casey, Jr. (D-PA)
Chairman

Senator Mike Braun (R-IN)
Ranking Member



U.S. Senate
Special Committee on Aging

U.S. Senate
Special Committee on Aging

U.S. Senate
Special Committee on Aging

What is AI?

Artificial Intelligence (AI) is a technology that enables machines to mimic certain human-like behavior, such as speech or writing. AI, while a useful tool in some circumstances, can be exploited by bad actors to make scams more convincing.

Three Terms to Know

1. 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.

2. Voice Cloning Technology:

Voice cloning uses AI to mimic the voice of someone you may know.

3. 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 conversation to build trust, with the goal of tricking the target into sending them money.

Examples of AI in Frauds and Scams

It may be difficult to know if someone is using AI-technology in a scam. One thing is certain: AI makes traditional frauds and scams easier to deploy on a large scale and are all the more convincing.

Fake Family Emergency Scam

Fake Text Message

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