Resist the pressure to act quickly. Criminals create a sense of urgency to instill fear and the need for immediate action.

Be cautious of unsolicited phone calls, mailings, and door-to-door service offers.

Never provide any personally identifiable information.

Never wire money to persons or businesses you have solely met online. Verify any email requests for money.

Ensure all computer anti-virus and security software are up to date. If you receive a suspicious pop-up or locked screen on your device, immediately disconnect from the internet and turn off the device.

Do not open any emails or click on attachments or links you do not recognize or were not expecting.

Research online and social media advertisements before purchase to determine if a product or company is legitimate.

Stop communication with the perpetrator, but expect the criminal will continue to attempt contact.
The Elder Abuse Prevention and Prosecution Act

This act was signed into law in October 2017 to prevent elder abuse and exploitation, and improve the justice system’s response to victims in elder abuse and exploitation cases. As a response to the increasing prevalence of crimes against the elderly, the U.S. Department of Justice (DOJ), along with other federal, state, local, and tribal partners, created the Elder Justice Initiative.

What is Elder Fraud?
The U.S. DOJ describes elder abuse as an intentional or negligent act by any person that causes harm or a serious risk of harm to an older adult, including financial exploitation and fraud.

The IC3 is the FBI office responsible for receiving Elder Fraud complaints.

IC3 Elder Fraud in 2022*
In 2022, over 82,000 victims over the age of 60 reported losses of almost $3.1 billion to the IC3. This represents an 84 percent increase in losses over losses reported in 2021. The average loss for over 60 victims exceeded $35,000. More than 5,400 elderly victims lost over $100,000.

*Age is not a required reporting field. These statistics reflect only those complaints in which the victim voluntarily provided their age range as “OVER 60.”

Common Elder Fraud Schemes

Romance scam: Criminals pose as interested romantic partners on social media or dating websites.

Tech support scam: Criminals pose as technology/customer support offering to help with non-existent issues, such as computer viruses or hacked accounts.

Grandparent scam: Criminals pose as a relative, usually a child or grandchild, claiming to be in immediate financial need.

Government impersonation scam: Criminals pose as government employees and threaten to arrest or prosecute victims unless they agree to pay.

Sweepstakes/lottery/inheritance scam: Criminals state the victim has won a lottery/sweepstakes, or is receiving an inheritance from a distant or unknown relative, but must pay fees and taxes to claim the money.

Investment scam: Criminals offer unsuitable investments, fraudulent offerings, and unrecognized products which can result in the theft or misappropriation of funds.

Charity scam: Criminals claim to work for a charitable organization to gain a victim’s trust and obtain donations.

Family/caregiver scam: Perpetrators are relatives or acquaintances of the elderly victims and take advantage of them or otherwise get their money.

Non-Delivery of Product: Victim does not receive an item purchased online, or the item is not as described. These items are often advertised on social media.