



DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

Elder Fraud Awareness: The 2022 Elder Fraud Report

The Internet Crime Complaint Center’s (IC3) 2022 Elder Fraud Report showed a 300% increase in reported crimes committed against people over the age of 60. Victims over 60, in fact, suffered greater losses than any other age group.

The IC3 is spearheaded by the FBI and serves as an intake point for victims to report fraud. The complaints the IC3 receives are shared with FBI field offices and other agencies for further investigation.

Along with other partners, including the Department of Justice’s Elder Fraud Initiative, the FBI is continually identifying and bringing perpetrators of these schemes to justice.

Victims by the numbers:

- 88,262 victims over 60^[1]
- \$3.1 billion in losses^[1]
- 84% increase in reported crimes compared to 2021^[1]
- Average loss per victim: \$35,101^[1]
- 5,456 victims lost over \$100,000^[1]

2022 CRIME TYPES

VICTIMS OVER 60 COUNTS			
Crime Type	Victims	Crime Type	Victims
Tech Support	17,810	Lottery/Sweepstakes/Inheritance	2,388
Non-payment/Non-Delivery	7,985	Other	2,016
Personal Data Breach	7,849	Real Estate	1,862
Confidence/Romance	7,166	Employment	1,286
Credit Card/Check Fraud	4,956	Overpayment	1,183
Identity Theft	4,825	Harassment/Stalking	754
Investment	4,661	Data Breach	333
Extortion	4,285	SIM Swap	301
Spoofing	4,201	IPR/Copyright and Counterfeit	235
Phishing	4,168	Ransomware	215
BEC*	3,938	Threats of Violence	166
<i>(Reporting a potential business victimization)</i>	2,552	Malware	125
<i>(Reporting a personal victimization)</i>	1,386	Crimes Against Children	84
Government Impersonation	3,425	Botnet	33
Advanced Fee	3,153		
VICTIM OVER 60 LOSSES			
Crime Type	Loss	Crime Type	Loss
Investment	\$990,235,119	Spoofing	\$22,261,276
Tech Support	\$587,831,698	SIM Swap	\$19,515,629
BEC*	\$477,342,728	Data Breach	\$17,681,749
<i>(Reporting a potential business loss)</i>	\$369,773,371	Extortion	\$15,555,047
<i>(Reporting a personal loss)</i>	\$107,569,357	Phishing	\$14,453,929
Confidence/Romance	\$419,768,142	Overpayment	\$10,977,231
Government Impersonation	\$136,500,338	Employment	\$6,403,021
Real Estate	\$135,239,020	Malware	\$1,851,421
Personal Data Breach	\$127,736,607	Threats of Violence	\$376,458
Lottery/Sweepstakes/Inheritance	\$69,845,106	Harassment/Stalking	\$254,659
Credit Card/Check Fraud	\$61,649,198	Ransomware**	\$210,052
Non-payment/Non-Delivery	\$51,531,615	IPR/Copyright and Counterfeit	\$203,140
Advanced Fee	\$49,322,099	Botnet	\$120,621
Identity Theft	\$42,653,578	Crimes Against Children	\$48,373
Other	\$31,410,237		

Common frauds affecting victims over 60

Call center fraud

Illegal call centers overwhelmingly target the elderly, with devastating effects.

Tech support scams are an industry-wide issue where scammers use scare tactics to trick victims into getting unnecessary technical support services that supposedly fix software and device problems that don't exist.

How the scam works

Scammers take over links on legitimate websites and online ads to direct victims to a fake tech support page.

Using scare tactics and urgency, the scammers attempt to get victims to contact them or click certain links. On these websites, there's often a popup message that warns the victim their computer is infected, and that they should contact the scammers right away.

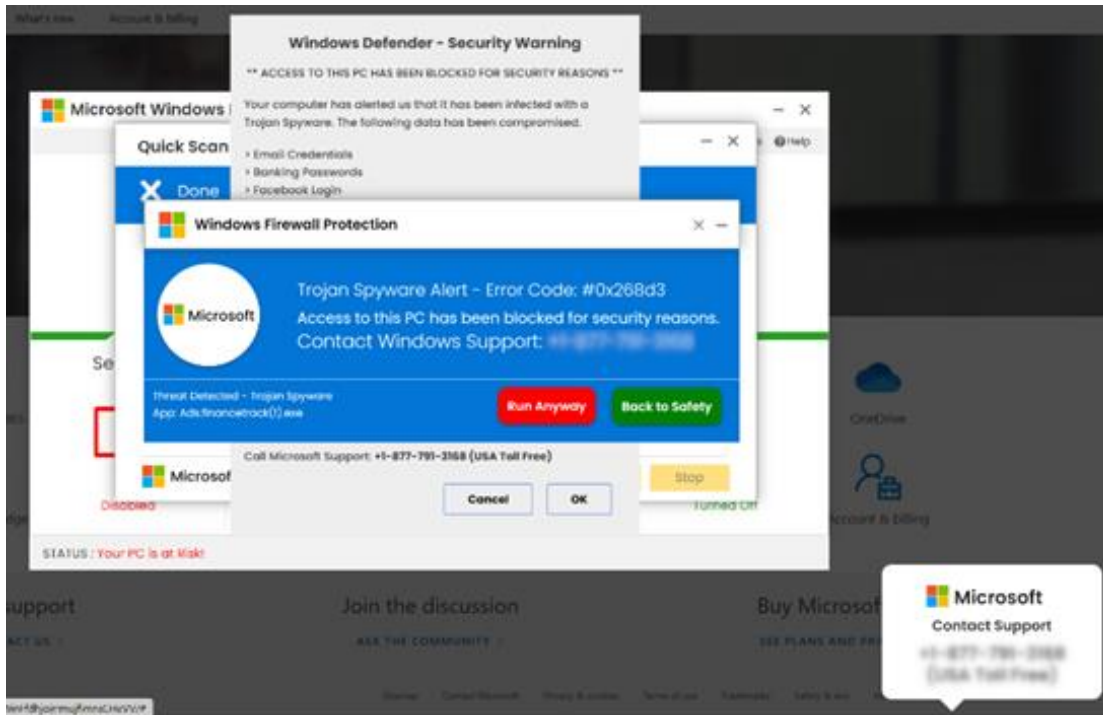
No matter the avenue, the scammers will try to compromise the victim's computer and steal their personal information.

What can you do?

If you get one of these messages, delete the message or close your internet browser altogether. Restart your browser afterwards.

If you want to verify the message, contact support directly using your Microsoft account or software support contact of any other application that may be involved. Never trust the contact information that the warning provides.

Additionally, you can ask someone you trust that knows computers to check the warning.



An example of fake warning screens.

Investment fraud

Investment fraud involves complex financial crimes often characterized as low-risk investments with guaranteed returns.

How the scam works

These scams often target their victims online, and most commonly involve cryptocurrency. Scammers try to gain the victim's trust and offer an opportunity to invest in a low-risk, unusually high-yield scam.

Victims over 60 can be pressured into accessing their retirement accounts, the equity of their home, and are even sometimes convinced to go into debt to invest as much money as possible into the fraudulent scheme.

This is devastating to elderly victims. Their income is typically limited, and many victims of this scam lose their entire life savings.

What can you do?

If you receive an investment opportunity, investigate it thoroughly.^[2] Never rush into investing. If it seems too good to be true, it is.^[3]

The SEC offers a service that allows you to check your investment professional [here](#).

Confidence and romance scams

This category encompasses scams designed to pull on a victim's heartstrings.

Romance scams are when a criminal adopts a fake online identity to gain a victim's affection and confidence. The scammer uses the illusion of a romantic or close relationship to manipulate and steal from their victims.^[4]

The criminals who carry out romance scams are experts at what they do and will seem genuine, caring, and believable.

Most common internet dating scams

Fake dating sites

Scam dating sites that claim to be legitimate but are instead filled with scammers. These websites are designed to mine information from their victims.

Photo scams

Scammers convince their victims to send personal information in exchange for intimate photos.

Military romance scams

A scammer poses as a member of the military, usually deployed. They build trust by using military titles and jargon, then ask for money to cover military-related expenses such as flights home.

Intimate activity scams

A scammer connects with their target on multiple social media websites. Once the scammer is close to the victim, the scammer convinces them to undress and then threatens them with the recordings.

Code verification scams

Scammers send a fake verification code through email or text, posing to be a dating app or website. Once the message is clicked on, the link victims are taken to asks for personal information such as credit card numbers and the victim's Social Security number.

Inheritance scams

Scammers make their target believe they need to get married to get an inheritance. In this case, the scammer asks the victim to help pay for something like airfare.

What can you do?

Protect yourself and elders by raising awareness

Although this can be an uncomfortable topic, make sure you, your family, and your friends are familiar with romance scams. The more you know about these scams, the better equipped you are against them.

Check in on elders

Scammers target people who are more vulnerable: those living alone or those who are grieving the loss of a spouse.

Limit what you share online

Scammers use details shared on social media and dating sites to better understand and target their victims.

Do your research

Research the individual's photo and profile using online reverse searches to see if the image, name, or other details have been used elsewhere.

Go slowly and ask questions

Don't let the individual rush you into leaving a dating service or social media site to communicate directly.

Listen to your gut

If the individual seems too good to be true, talk to someone you trust.

Don't overshare personal information

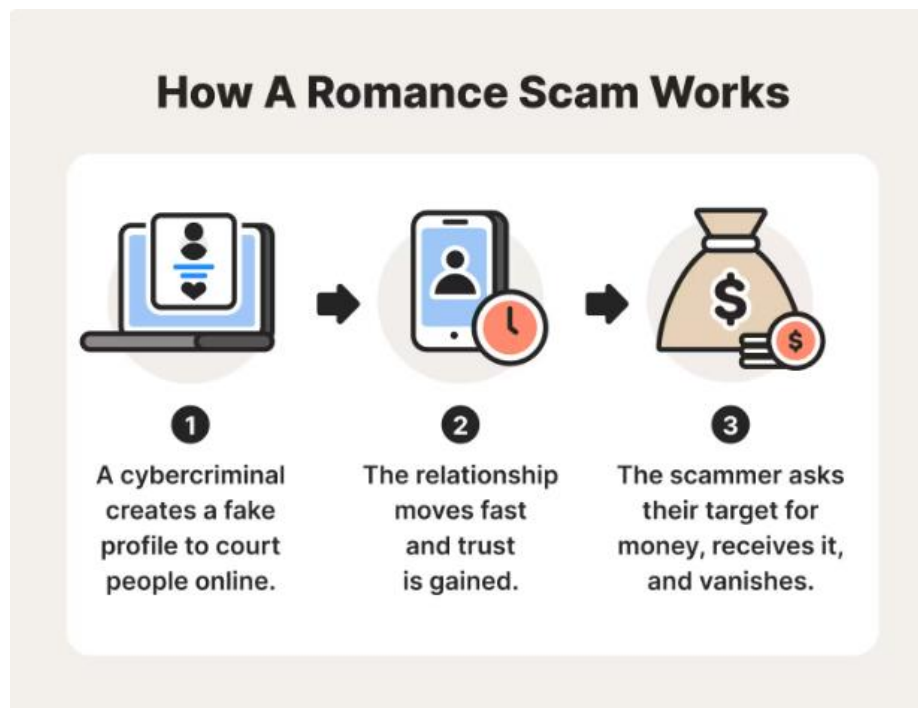
Requests for inappropriate photos or financial information could later be used to extort you.

Be suspicious if you haven't met in person

If the individual promises to meet in person, but consistently comes up with an excuse for cancelling, be suspicious.

Don't send money

Never send money to anyone you have only communicated with online or by phone.




How romance scams work.^[4]

Other common frauds

Extortion

Extortion is when a criminal demands something of value from their victim by threatening physical harm, financial harm, or the release of sensitive data.



Almost half of extortion victims over 60 reported to be victims of sextortion. Most believed they were in a relationship with the scammer and shared sensitive photos or information which were later used to sextort them.

Never share intimate information or pictures with someone you just met or cannot meet in-person. You can never be certain whether they're a real person or a scammer.

Non-payment and non-delivery



Elderly victims filed almost 8,000 non-payment/non-delivery complaints in 2022, totaling losses over \$51 million.^[1] Non-delivery was the second-most reported fraud against the elderly.

More elderly people are joining social media to connect with others. The combination of social media and online shopping creates an easy venue for scammers to post fake advertisements. Many victims report ordering items from links advertised on social media, and either receiving nothing at all or receiving something completely unlike what was advertised.

Purchase from legitimate mainstream vendors, such as the online presence of a department store or Amazon. With mainstream vendors, consumers have protection.

Grandparent scam




Grandparents often have a hard time saying “no” to their grandchildren. Scam artists know this all too well.

Scammers will mine social media accounts and purchase consumer data from cyber thieves to create storylines to prey on the fears of grandparents.^[5]

Scammers call the grandparents, impersonating their grandchild or another close relative, and set the stage for a crisis where they need immediate financial assistance.

The caller ID is also sometimes spoofed, making it appear as though the call is actually being made from a trusted source.

The crisis tends to involve an accident or an arrest.^[5] “Please don’t let mom and dad know” is often said by the scammer to keep the transaction secret, and the phone may be handed over to someone pretending to be a lawyer seeking immediate payment.



Grandparents who receive calls from grandchildren who are in trouble and need money should first contact the grandchildren's parents, or the grandchildren directly. Using known phone numbers, grandparents can verify the caller.

Wrapping Up



Crimes committed against the elderly are on the rise. Now, more than ever, it's important to equip yourself and your loved ones with the knowledge and awareness of the kinds of scams that are becoming more prolific and commonplace in the lives of the elderly.

With this knowledge comes power; the power to protect those around you from thieves and scammers.

References



1. [“Elder Fraud Report 2022”](#) Federal Bureau of Investigation. 17 April 2023
2. [“3 Of The Most Popular Investment Scams And H...”](#) Yahoo Finance. 11 April 2014
3. [“How to Spot an Investment Scam”](#) Charles Schwab. 14 October 2021
4. [“Romance scams in 2023: What you need to know + onlin...”](#) Norton. 10 July 2023
5. [“Grandparent’ Scams Ge...”](#) Federal Communications Commission. 9 March 2023

deer-brook.com



DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

