family matters:
how scammers are targeting families, children, and older adults

With new scams targeting every age group, today's schemes are more personal, more convincing, and more costly.

Allstate®
IDENTITY PROTECTION

May 2025

Prologue

In the world of crime, scammers and fraudsters are among the most cunning and creative criminals. They're constantly inventing new ways to steal personal information and trick unsuspecting people out of their money. And with the rise of communication platforms like social media and the metaverse, and more ways to steal and access data through breaches and data brokers, scammers and identity thieves now have more opportunities than ever.

From children to older adults, no one is off-limits. Since 2020, money lost by victims 20 and younger has increased significantly. In 2023, victims under 20 lost a total of $312 million,[1] a steep rise compared to previous years. However, seniors are the most victimized group, losing over $4.8 billion in 2024.[2]

In this white paper, we'll examine how scammers are targeting families through schemes that are more personal, more convincing, and ultimately more costly. In 2024 alone, identity theft and scam losses surged to $47 billion, up $4 billion from the prior year, affecting 40 million victims—one million more than in 2023.[3]

With this increased targeting of families and children it's more important than ever to be aware of the latest scams—and how to combat them. Drawing from industry research and internal insights, this white paper outlines these scams and fraud schemes, including how parents and caregivers can recognize these scams, the steps they can take to prevent them, and how an identity protection solution can prevent and protect from these scams.

Losses for victims under 20, 2022-2024

$544.5M

Losses for victims 60+, 2022-2024

$11.7B

1: Social Catfish, State of Internet Scams, July 2024
2: Federal Bureau of Investigation, Internet Crime Report, 2021-2024
3: Javelin 2025 Identity Fraud Study: Breaking Barriers to Innovation, March 2025

Table of contents

Big losses for younger victims

Scams targeting families are particularly insidious because they exploit the loving bond that family members share. This can cause victims to act without fully considering their actions—which is exactly what scammers want. In these heightened emotional moments, people may share sensitive information or send payments they would never consider under normal circumstances.

When a cry for help isn't what it seems

In an emergency scam, otherwise known as a "grandparent scheme", someone contacts a family member (like a parent or grandparent) pretending to be a close family member, such as a son, daughter, or even a close friend. **The scammer, pretending to be a loved one, will claim that they're in some sort of trouble. They might claim they're under arrest, stranded somewhere, experiencing car trouble, or in another dire situation.**

Then, they'll request money to help them get out of the situation. Scammers typically reach out via text, phone call, email, or even hijacked social media accounts. And to make it even more convincing, they might use number spoofing to make it seem like the message is coming from a trusted number.

Scammers often do their homework before launching this kind of scheme—stalking social media for personal details like where someone goes to school, the kind of car they drive, or recent travel plans. When they combine that information with number spoofing, the result can feel incredibly real. Emergency or "grandparent" scams have been particularly effective for scammers as they use a perfect blend of personal information and emotional manipulation. In fact, the United States Attorney's Office recently indicted 25 Canadian nationals and 9 other individuals from other countries that defrauded elderly individuals from more than 40 states using this scam, resulting in losses of over $21 million.[5]

How number spoofing makes the scam feel real

Number spoofing is when scammers fake the caller ID to make a call or text look like it's coming from someone you know. It's surprisingly easy to do with online tools or apps that let scammers pick any number they want to display. That means a scammer calling from across the country can make it look like they're calling from your neighborhood or from someone in your contacts list.

5: U.S. District Court for the District of Vermont, 25 Canadian Nationals Charged in Vermont in Connection with Nationwide Multimillion-Dollar "Grandparent Scam", March 2025

Make a plan before the call comes

To avoid becoming a victim of an emergency scam, follow a series of established best practices, including:

- **If parents get a message from an unfamiliar number, email, or social media account, they should immediately be cautious.** Paying close attention to how the person communicates is key—if their loved one is using unfamiliar words, phrases, or mannerisms, it could be a sign that someone's impersonating them. Scammers count on targets to act without thinking. If someone suddenly asks for money to cover bail, a car accident, or being stranded, especially with little to no detail, that's also a red flag.

- **Take a breath, stay calm, and think before acting.** Parents shouldn't respond to suspicious messages. Instead, they should call their loved one using a number they know and trust. Parents can also reach out to other family members as they can help confirm whether there's an actual emergency.

- **The best defense is preparation.** Setting up a family safety word ahead of time can help parents confirm they are speaking with a loved one. It should be something unique that only their family knows. If parents ever receive a suspicious call or message, they should ask for the safety word or pose a question only the real person could answer, like a shared memory or inside joke.

- **For businesses focused on supporting the wellbeing of their employees, a proactive approach to employee education and awareness is crucial.** This could involve regular training sessions on common scam tactics and promoting resources that empower employees to identify and avoid potential threats.

Emergency scams in action: kidnapping scams

Kidnapping scams are an extreme version of an emergency scam. In this scheme, a scammer calls a parent and claiming that they have kidnapped their child. To make the threat feel more real, the scammer may also contact the child first, warning them that their parents are in danger unless they follow instructions. The child is then pressured to isolate themselves and take staged photos, which are sent to the parents as "proof" of the fake kidnapping.

Scammers often use stolen personal information—like phone numbers, addresses, or family details—gathered from the dark web or social media to make the scenario feel real. The goal is to create panic and urgency, so both the child and parent act out of fear.

Unfortunately, this scam can be incredibly convincing. In 2024, a Chinese exchange student fell victim to this scam when scammers convinced him that they would hurt his parents if he didn't comply. Once the scammers had isolated the student in the Utah wilderness and gotten pictures of him, they sent those pictures to his parents and convinced them he was in danger. The parents eventually paid over $80,000 to the scammers[6], only for them to discover it was a scam.

6: BBC, Kai Zhuang: Chinese teen found alive in US after 'cyber kidnapping', January 2024.

Identity theft isn't just a problem for adults

Although identity theft has traditionally been a threat to adults, it's quickly becoming one of the most prevalent risks facing children. This type of fraud is especially harmful because it often goes undetected for years. **By the time the fraud is discovered, often when the child applies for a student loan or job, the damage can be extensive.**

Fraudsters usually gain access to children's personal information through data breaches at schools, hospitals, or other institutions that store sensitive data. These breaches are alarmingly common. In fact, in 2024 alone, 1 in 43 U.S. children had their personal identifying information (PII) exposed in a hack or online compromise.[7] Once exposed, this data is often sold on the dark web.

But data breaches aren't the only risk. Scammers also target kids directly through phishing attacks—posing as friends on social media, sending malicious links, or even disguising scams as fun "quizzes" that trick children into giving up personal details. Once the information is in hand, it can be used to build synthetic identities and commit long-term fraud.

"In 2024 alone, **1 in 43 U.S. children** had their personal identifying information (PII) exposed in a hack or online compromise."

7: Javelin 2024 Child & Family Cybersecurity Study, Social Media and Children: A Dangerous Game of Trust and Deceit, 2024

According to recent data from the Federal Trade Commission, identity theft involving minors has surged by 40 percent over the past three years,[8] with an estimated 1.1 million children impacted by identity fraud, or about 1 in 50.

The red flags of child identity theft

Recognizing the signs that a child's identity has been compromised is the first and most critical step in preventing further damage.

- One of the first signs of child identity theft is a credit report existing at all. Since children typically don't use credit, this alone is a red flag.
- Parents might start receiving preapproved credit cards or loan offers addressed to their child. In more serious cases, families may be contacted by collection agencies or lenders about unpaid bills tied to the child's name.
- The IRS might even send tax notices for income a child has never earned. If someone receives a tax notice for one of their children, that child's identity has almost certainly been stolen.

Pro tip from Allstate Identity Protection's customer care team

"To protect children from identity theft, parents can take proactive measures such as placing a credit freeze with the three credit bureaus, who will create a credit file and freeze it if a credit file does not already exist. They can also check to see if their children have a credit report and ensure that no information is present. Additionally, parents can take the opportunity to educate their children about the risks associated with sharing personal information online and the importance of being cautious when interacting with others on the internet to mitigate the risk of identity theft."

8: Javelin 2024 Child & Family Cybersecurity Study, Social Media and Children: A Dangerous Game of Trust and Deceit, 2024

Where kids connect and play, scammers lurk

Whether they're uploading a TikTok video, taking pictures using Snapchat, sending reels to their friends on Instagram, or playing games on their phone, social media and mobile apps play a pivotal role in the lives of children. And while social media apps and games provide a range of opportunities for children to connect with their friends and influencers, they can also serve as fertile ground for scams.

Children and teens on social media are often pressured or convinced by scammers to provide personal or financial information that can be used to blackmail them for direct payments, facilitate other scams, or compromise their identity. **One of the most popular schemes involves scammers posing as legitimate pages or influencers and offering giveaways, raffles, or the opportunity to purchase items at an incredible discount.** Unable to tell that this is an imposter account, children then click on the link, which then prompts them to enter sensitive information like their email and password, social media credentials, or credit card information.

These malicious links can also download malware onto their device, which will then steal personal information stored on that device. This scam can also be executed on platforms like Twitch and Kik, where scammers will pose as famous streamers and post links or QR codes that promise free video game skins or the chance to enter in a giveaway.

Scammers might also pose as peers of similar age. They then begin a friendship with the targeted child or teen, eventually convincing them to expose personal information or even directly send them payments.

$2.7B — total reported consumer loss from social media scams from 2021-2023[9]

Pro tip from Allstate Identity Protection's customer care team

"Scammers are creating fake social media profiles to trick people into sharing personal details or money. If someone you don't know reaches out, always be cautious."

9: Federal Trade Commission, Social media: A golden goose for scammers, October 2023

Sextortion scams: an escalating threat

The most nefarious, and often dangerous, scam is known as "sextortion". In this scam, the fraudster will pose as a love interest and begin an online relationship with the targeted child. They will then send explicit photos of the person they are pretending to be and will request explicit photos in return. Once the targeted child has sent those photos, the scammer will then reveal the scam and threaten to send the explicit photos to the child's friends and family unless they send payments or more explicit material.

Unfortunately, this scam is very common—in 2023, the National Center for Missing and Exploited Children received 26,718 reports of financial sextortion, or an average of 812 reports per week.[10] This scam can be particularly dangerous to children's mental health as they often suffer from unbearable shame and anxiety, which can result in suicide attempts and self-harm.

Mobile apps and scams: a gateway to fraud

And as social media has grown in popularity among children, so has the use of mobile devices, and by extension, mobile apps and games. 51 percent of children 8 and younger now have their own mobile device[11], and these young children are inevitably accessing mobile apps and games while using these devices.

By creating intriguing thumbnails or apps that mimic the appearance of popular apps, scammers can trick children into downloading a malicious app or game. Once the app or game is downloaded, the app will ask users for sensitive information like login credentials or payment information. These apps can also contain malware, which can steal information, damage systems, or take control of devices.

Because it can be difficult to host these apps or games on commercial stores, scammers often host them on third-party app stores that have less strict or no safeguards. Links to these third-party stores are often distributed through social media, ads, email, or other communication methods.

"26,718 reports of financial sextortion, or an average of 812 reports per week."

Pro tip from Allstate Identity Protection's customer care team

"A frequent mobile game scam involves the promotion of 'free' online casino games where you can 'win' a lot of money without making any purchases. It's a typical bait, hook, and catch scam used in phishing attacks. The ultimate objective of the fraudster is to get a child's email address and then ultimately their financial information.

The "bait" is an actor screaming with excitement when they just 'won' money on the game app. The "hook" is a child downloading the app and adding their personal information to use the app. The "catch" is when the child uses the app for the first time and they 'win' $5-10. The game requests that the child add their bank account, PayPal, or Venmo accounts for them to deposit the winnings into. The best advice: Buyer beware! There is no such thing as free money.

10: Thorn, National Center for Missing & Exploited Children, Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline Data, June 2024
11: Common sense, The Common Sense Census: Media Use by Kids Zero to Eight, February 2025

Protecting kids starts with a conversation

All children will have some degree of secrecy about their social media use, but extreme secrecy can be a red flag. Similarly, while behavioral changes are a normal part of growing up, a sudden shift, like increased anger or signs of depression, may indicate that a child has been targeted by a scam. If a child suddenly deactivates or deletes their social media accounts, it could also be a sign that something has gone wrong.

- **Make sure they understand to never share personal details like login credentials or financial information, never send money under any circumstances, and never share explicit images with anyone.** Because it's difficult to monitor every interaction children have online, it can be challenging to protect them from social media scams. That's why it's essential to make sure children understand these concepts.

- **Keep an eye on how children use their devices, and make sure they ask before downloading any apps.** It's important to set up devices so apps can't be downloaded without the proper credentials. Protecting children against game and mobile app scams is equal parts education and supervision. Parents should also teach children how to spot fake apps by encouraging them to read user reviews, checking the number of downloads, and avoiding apps hosted on third-party sites.

- **Teach children to be cautious about accepting friend or follow requests from people they don't know.** They should also be wary of accounts or influencers offering giveaways, cheap products, or raffles, and never respond to Direct Messages (DMs) from people they don't know on apps like Instagram and Facebook.

- **Organizations can help families avoid social media and mobile app scams by providing education around communicating effectively with children about the dangers of social media and apps and how to monitor and manage their children's mobile device use.** This includes providing training and resources regarding safe social media and app use and how to recognize the signs that children have become a victim of a scam.

Older adults remain prime targets

Older adults are consistently among the most targeted groups for scams. It's important to recognize that digital literacy varies widely within this population; many older adults are highly proficient with technology. However, scammers often exploit segments of this demographic who might be less familiar with emerging online threats or who manage significant personal finances, viewing these individuals as low-risk, high-reward targets.

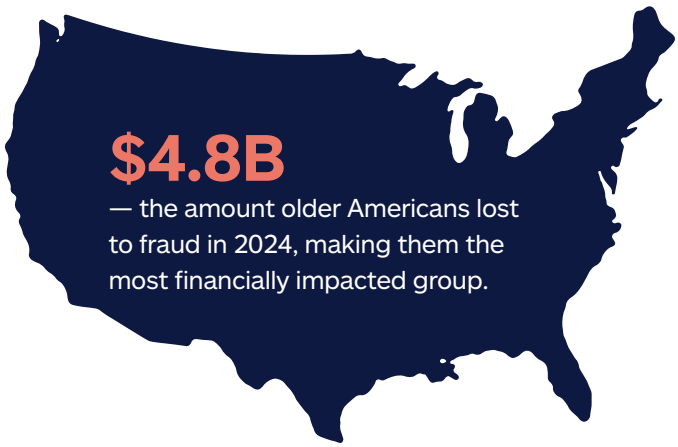
These scams are often emotionally manipulative and designed to create a sense of fear, confusion, or urgency that pushes victims into making fast decisions without seeking outside advice. Common scams targeting older adults exploit their trust, generosity, and sometimes a lack of digital literacy. They often involve impersonation, tech support fraud, or schemes designed to tug at their heartstrings.

A wolf in sheep's clothing

For the older generation, and even digital natives, technology can be intimidating with its many features, settings, and cyber threats. And this lack of knowledge about technology and how it works provides a unique opportunity for scammers, especially when it comes to older adults.

In a tech support scam, scammers will reach out to a target, often an older individual, and offer their "services" in helping them address an issue. This contact may come in the form of a phone call, text, or email from a "trusted source".

Scammers may also initiate contact by sending a pop-up notification to a target's device that urges them to contact them by phone or by clicking a link. These pop-up windows will often look like an error message from the operating system or an anti-virus solution. Fraudsters may even take advantage of those looking for tech support by running online ads or hosting fraudulent webpages promising to help them that appear when a target searches for help on a search engine.



12: Federal Bureau of Investigation, Internet Crime Report 2024, 2024

The fraudsters will often claim that a device or computer is infected with a virus, is out of warranty, is missing critical software, and more. They may also claim that a target's account or profile is experiencing an issue, such as suspicious activity, and will offer to help them fix it.

Once the scammers have a target on phone, they have several methods to steal funds or personal information.

- **Scammers will often request remote access to a device.** This grants them access to all the information stored on that device, including payment information, credentials, and more.
- **Fraudsters may direct targets to a website that asks for personal information or may infect their device with malware.** This allows them to collect personal information that can be used to compromise their target's identity, such as social security numbers or credentials like usernames and passwords.
- **Selling fraudulent device maintenance, warranty programs, phony software or repair services is a common tactic to collect payment.** Scammers will claim the service or product is essential to the health or operation of a device.

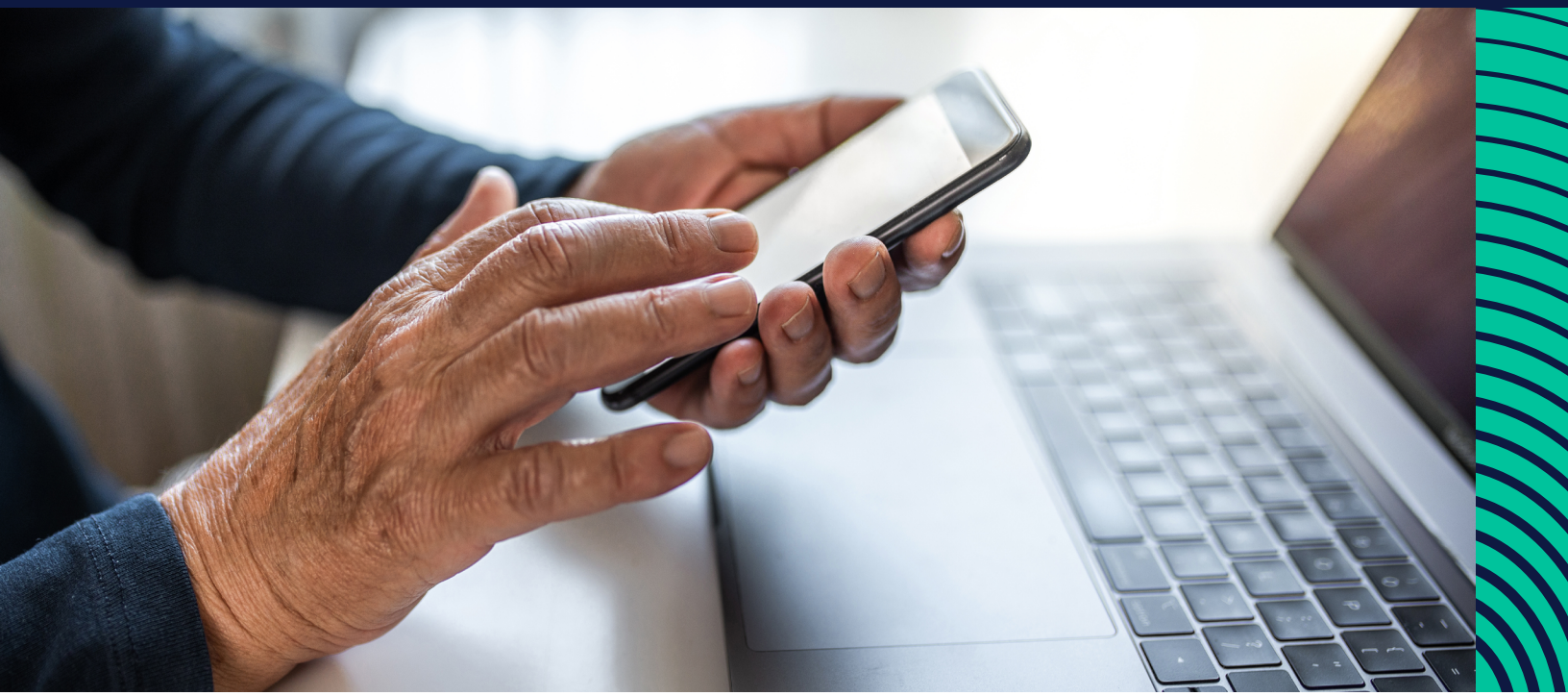
In 2024, victims 60 and older reported losing **$982 million** to tech support scams.[12]

Stopping tech support scams in their tracks

With the prevalence of tech support scams targeting older adults educating older adults on how to avoid becoming a victim of these scams is critical. Here are some important tips that older technology users should be equipped with:

- **Anyone, regardless of age, receiving a tech support phone call regarding their device or account should immediately be suspicious.** Technology companies will never contact customers by phone to report an issue.
- **Carefully analyze any pop-up windows or notifications**. Legitimate pop-up windows or notifications will always appear within an application and will never appear while using an internet browser. Pop-ups from real tech companies will also never ask customers to call a number or click a link.
- **Tech support will never ask for payment.** Legitimate tech support teams will never ask for payment for their services and will never try to sell a piece of software, warranty, or maintenance program.
- **Organizations can also join the fight against tech support scams by offering specific resources and training on how to spot and avoid tech support scams.** They can also help by offering public-facing resources on their site outlining their tech support policies and details about how customers can get the help they need with their technology questions.

12: Federal Bureau of Investigation, Internet Crime Report 2024, 2024



Government imposters target older adults

Receiving a call from the government, especially when it's a call about owing money, can be a nerve-wracking experience. The idea of owing money to an entity as imposing as the government, and facing legal or financial penalties as a result, is frightening. In an IRS imposter scam, fraudsters leverage this fear by masquerading as the IRS and convincing their target that they owe money to the agency.

Older adults are often targets of these scams because they may be more trusting and are typically more trusting and polite. Older adults also often have financial assets like retirement savings, which make them an attractive target for scammers looking for a big score.

Scammers will usually initiate contact by phone but may also send texts or emails. These communications will often threaten arrest or severe financial penalties if the target doesn't pay what they supposedly owe. To make the scam more convincing, criminals will often use fake names and provide falsified IRS badge numbers.

On the flip side, the scammers may also claim that the target is due a tax refund. They will then claim that to send the payment, they need confidential information such as social security numbers, credit card numbers, or bank account numbers.

In an IRS imposter scam, fraudsters leverage this fear by **masquerading as the IRS and convincing their target that they owe money to the agency.**

Don’t be intimidated by imposters

In an IRS imposter scam, the fraudsters will do everything they can to get their target to act quickly and supply confidential information or payment. But by taking their time and looking for the signs of an IRS imposter scam, targeted individuals can spot the scheme and avoid becoming a victim.

- **The IRS will only contact taxpayers by phone, text, or email if they have received permission to do so.** If the IRS wants to get in touch with someone, they will contact them by mail. If someone receives an unsolicited email or text from the IRS, they should avoid opening the message or clicking on any link contained in that message, as it may lead to a site that will steal their information or download malware on their device.

- **IRS agents will also never ask for financial information.** If the IRS needs to collect funds from a taxpayer, they will provide legitimate methods of paying. The same goes for issuing refunds—tax refunds will arrive via check, and the IRS will not ask for financial information to deliver them. Also, if someone claiming to be an IRS agent is asking for payment via an unusual method like a gift card or wire transfer, it’s certainly a scammer.

- **The IRS will never threaten to call law enforcement or immigration officials.** Legitimate IRS personnel will also never threaten to take someone’s citizenship status, driver’s license, or business license.

- **Apart from offering employees training on how to recognize an IRS scam, they can also offer resources that show employees how to discuss these scams with the elder members of their family.** These resources can also include methods to teach older adults how to avoid these scams, as well as tools they can access if they suspect they are being targeted by scammers.

Scammers pulling at heart strings

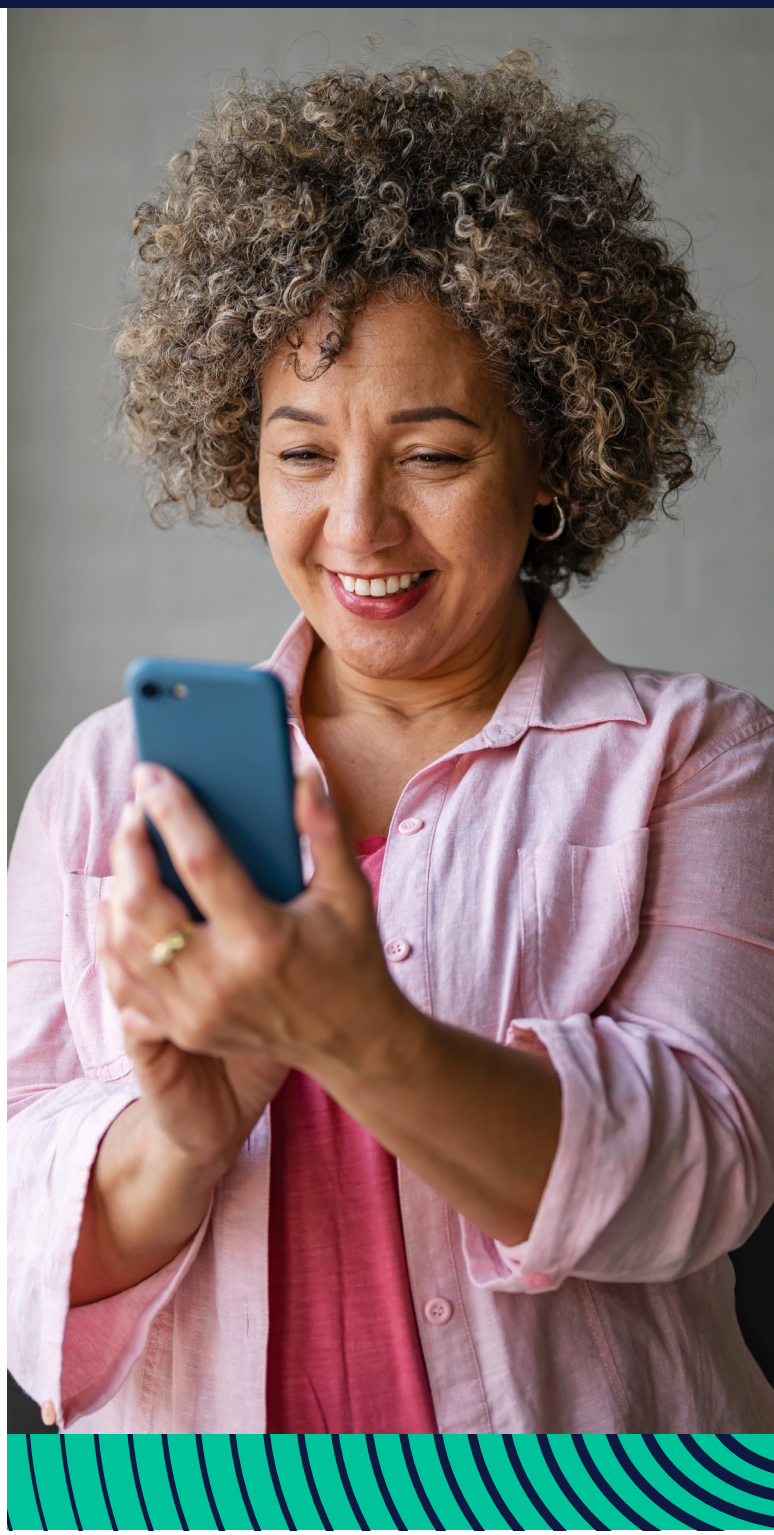
As humans, we crave connection—and scammers have recognized that they can leverage our desire for romantic relationships for nefarious purposes. **In a romance scam, a fraudster will contact a target on a dating app or social media using a fake profile and pretend to be romantically interested in them.**

They will then develop a relationship with the target over time, eventually convincing the targeted individual to share personal information or send them payments. Older adults are a perfect target for this kind of scam as they can have few friends or opportunities to develop romantic relationships, and often have savings that scammers want to get their hands on. And while older adults are often targeted by this kind of scam, with victims 60 and older losing over $389 million in 2024 alone[12], romance scams are a threat to people of all ages.[13]

To execute their scam, scammers will often create a fabricated story alongside their fake profile. These fabricated stories often involve experiencing financial problems or health issues and are intended to play on the target's sympathies.

The fraudsters will then start "love bombing" the victim, which involves overwhelming them with attention and affection. They will often quickly declare their love for the target, seeking to gain their trust as quickly as possible.

Once they've managed to gain their target's affections and trust, scammers will begin asking for money. They will usually fabricate an emergency like legal trouble, health emergencies, or damage to their home. Scammers may also ask for money to help with their living expenses, investments, travel costs, or for gifts.



"Elderly are increasingly being targeted by this kind of scam, with victims **60 and older losing over $389 million in 2024 alone.**"

12: Federal Bureau of Investigation, Internet Crime Report 2024, 2024
13: BioCatch, Romance Scams: Which Generation is Most at Risk?, 2024

Don’t be fooled by romance scams

Romance scams can happen across dating apps, text, email, or even phone, making them very difficult to avoid—especially with the ability to create AI-generated video and voices. However, older adults can prevent heartache and financial losses by recognizing some of the red flags associated with romance scams and following best practices.

- **Romance scammers will try to develop the relationship quickly.** The faster they gain the affection and trust of a target, the sooner they can ask for money. Any online acquaintance that quickly expresses their feelings shouldn’t be trusted.
- **Refusing to meet in person is a strong indication of a romance scam.** If someone constantly refuses to meet in person or consistently cancels plans to meet, it could be a sign of a scam. These excuses could include an inability to meet because of health issues or residence in a different state or country.
- **Asking for money for any reason is a major red flag.** Although their story might be convincing or heartbreaking, anyone online asking for any sort of payment should immediately be treated with caution. No matter how tempting it is to help a person in need, nobody should ever send payment to someone they haven’t met in person.
- **By providing access to effective resources, training, and tools, organizations and their employees can significantly reduce the number of older victims of romance scams.** However, romance scams take place over personal communication methods, it can be difficult for organizations and employees to protect older adults.

Protection that meets the moment

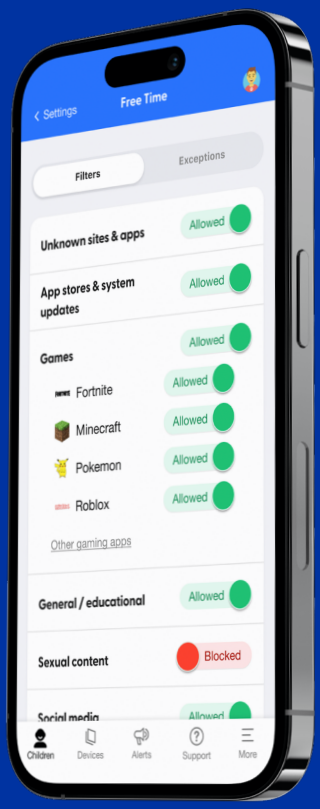
When it comes to protecting the family, and especially children and seniors, education is the first step. By knowing what scams are out there, the key signs of those scams, and how to avoid them, families are better equipped to avoid them entirely.

But knowledge alone isn't always enough. With the complexity of modern scams and the constantly evolving tactics of scammers, having an identity protection solution that provides automated scam protection and reimbursement in case a scam succeeds is also critical.

For employers, offering this kind of protection to employees isn't just a perk—it's a powerful statement. It shows your commitment to employee wellbeing and a proactive approach to modern threats. It also sets you apart in the talent market, where candidates are increasingly looking for benefits that extend to their loved ones and protect what matters most: their family and finances.

Beyond peace of mind, it can also protect your bottom line. Falling victim to a scam can consume an employee's time, energy, and emotional bandwidth. A strong identity protection solution helps prevent lost hours and reduced productivity caused by dealing with financial recovery and emotional stress.

Of course, not all solutions are created equal. To truly protect your workforce and their families, it's important to choose a provider with the right features. Here's what to look for in a comprehensive identity protection solution:



Child safety content monitoring and alerting
With content monitoring and alerting across texts, photos, emails, social media apps, and more, families can detect suspicious or harmful activity that can lead to scams on their devices

Malware, phishing, and virus protection
Best-in-class protection from malware, phishing, and other viruses can prevent sensitive information from being stolen and prevent users from clicking on fraudulent links

Automated scam detection
Automated detection can block a scam call, text, or email, stopping a scam before it can even start

Location services
By being able to see where children and minors are, parents and others can avoid falling victim to emergency and kidnapping scams

Child credit check
With the ability to easily check a child's credit and receive help in addressing identity theft, employees can avoid or prevent further damage from child identity theft

Account takeover monitoring
By monitoring employee's social media accounts for signs of an account takeover, they can prevent scams that target family members, friends, coworkers, and others

Exceptional customer support
With an experienced customer care team on call, families can get expert advice on what to do if they are targeted by a scam or need to confirm whether something is a scam or not

Customer education & 1-1 coaching
Frequent updates on the latest scams and schemes can keep employees informed and prevent successful scam attempts, while personalized coaching can help employees get the most out of their plans, avoid scams, and equip them with critical knowledge

Dark web monitoring
By automatically monitoring the dark web for employees' personal information, they can proactively prevent identity theft and protect their accounts

Automated data removal
With a feature that automatically monitors data brokers for employee's information and removes it, there is a lower chance of an employee's information being exposed in a data breach

Broad family protection
Identity and scam protection that extends to children and older family members is essential for protecting an employee's peace of mind, health, and finances

To learn more about how an identity and scam protection solution can help protect employees and position your company as a leader in benefits offerings, contact our sales team at sales@aip.com.

Allstate®
IDENTITY PROTECTION