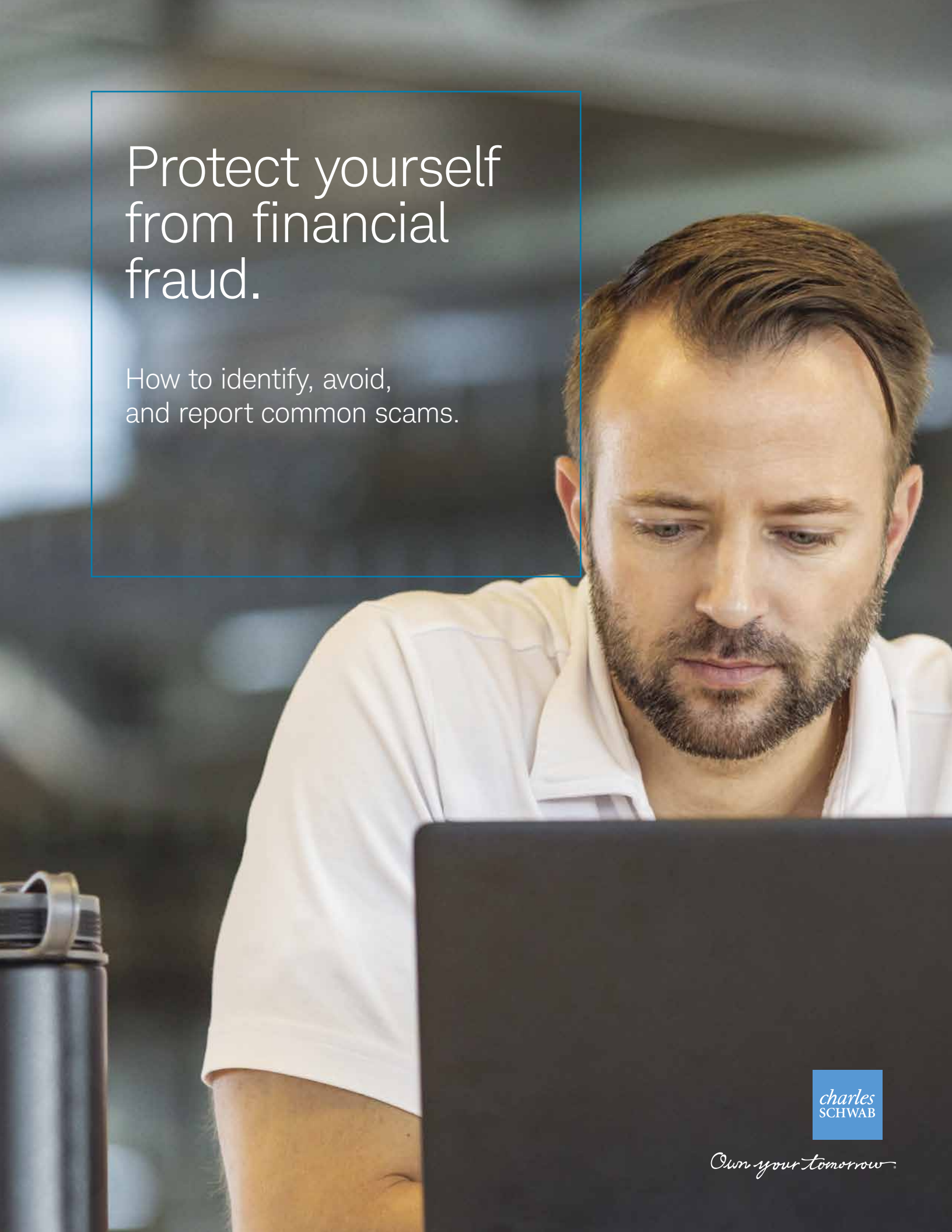

Protect yourself from financial fraud.

How to identify, avoid, and report common scams.

charles SCHWAB

Own your tomorrow®

What are scams?

Scams are on the rise, making it more important than ever to stay vigilant and take extra steps to protect your accounts. Awareness is one of the most valuable tools that may help prevent you from becoming a victim.

A scam is a fraudulent scheme intended to trick an individual out of money or possessions. Victims are convinced to willingly send money or provide information to a scammer under the belief it's for a legitimate purpose or going to a trusted recipient.

Scammers contact potential victims in various ways:

- Email
- Phone
- Text
- Social media
- Mail

Scammers also frequently attempt to use an unwitting individual as an intermediary for fraudulent schemes. After acquiring money illegally, a scammer may trick a target into transferring the funds in person, through a courier service, or electronically to people working with the scammer. For example, in a romance scam scenario, a victim may accept funds at the request of their "sweetheart" and agree to resend the funds to another recipient account, which is controlled by the scammer.

What are the impacts?

Scams are often regarded as more harmful than other identity theft and cybercrime schemes.

- The FTC reports that in 2018, victims of imposters scams lost $488 million. While this figure is staggering, it's likely the actual impact is even larger, since it's estimated that only 15% of scam victims in their seventies report these crimes to law enforcement.
- A person may not immediately know they've been victimized. For example, days or weeks may pass before they discover an intended recipient did not receive funds that were sent or an item they purchased never materialized. This delay gives fraudsters added time to remove the funds from the receiving account and can lower chances that the funds will be recovered.
- The intent of a scam is to trick you into sending information or funds to a recipient that is not who you believe they are. Typically, the information will be of a nature that allows them to access your bank or credit card accounts. The money you send or that they steal will be gone quickly and may not be available for recall.
- Scams often have an emotional component. Whether or not there has been a financial loss, when the victim realizes they've been deceived, they may feel hurt, violated, or foolish.

Protect yourself from scams

Tips to protect yourself against scams.

- Verbally verify money movement instructions with the recipient and ask for supporting documentation.
- Perform your own due diligence. Google the recipient/product/person to validate the legitimacy of the request or search for scams/complaints associated with the other party.
- Use appropriate disbursement channels/methods to make payments. Avoid prepaid debit cards, gift cards, and digital currency.
- When you can, view goods in person, pay after services are completed, and send money only to people you've met in person.
- Use services that have purchase protection and/or an escrow service, especially for high-dollar transactions.
- Phone numbers can be spoofed. Do not rely on your caller ID to verify who is calling you.

What to do if you suspect a scam.

If you're suspicious about activity that you believe might be a scam, call us at 1-800-435-4000.

You can learn more about scams from these external resources:

- https://www.fbi.gov/scams-and-safety
- Consumer.ftc.gov/features/scam-alerts

Types of scams

Extortion

What is it?

Extortionists falsely assert they have information about the victim and that they will make it public unless they are paid.

How does it work?

An extortionist may claim to have used malware to access the target's online credentials or webcam and to now possess personal files or video that could be damaging if made public. A payoff is demanded, usually in Bitcoin, with an urgent deadline. In some cases, the perpetrator will provide information that makes the claim seem legitimate, such as a password that was harvested through an unrelated data breach and sold on the dark web.

Protect yourself.

- Use unique passwords for each site you access.
- Use two-step authentication, when available, for extra protection.
- Install anti-malware/antivirus software to regularly scan your computer.
- Report suspected scams at the FBI's internet crime complaint center: www.ic3.gov.

Real Estate

What is it?

A real estate scam can come in many forms related to property purchases, renovations, and rentals.

How does it work?

- Closing transactions: Scammers often target people who are buying a home. Automated Clearing House (ACH) or wire transfer instructions are sent via an email that appears to be from the title company or real estate agents. These fraudulent transactions, often for high dollar amounts, aren't caught until the title company confirms the funds were not received. Home buyers should call their title company to verbally verify all details of a transfer before any money leaves their account.
- Fictitious properties: Properties which don't actually exist may be listed for rent or sale. There have been reports of scams involving vacation rentals on sites such as Airbnb, VRBO, and Craigslist. Scammers insist on receiving either a down payment or full purchase price for the property, yet deny a physical viewing of it, show a different property, or fail to produce any type of valid documentation.
- Fake buyers/renters: Property owners are often targeted by scammers posing as potential renters or buyers. They may provide, by "accident," a down payment for an amount greater than the deposit and ask the owner for repayment. The deposit fails to clear, and the scammer walks away with the overage amount.

Protect yourself.

- Verbally verify payment instructions received by email, directly with the escrow/title company.
- Do not send payment for properties you have not seen or to landlords/owners you have not met in person.
- Beware of deals that appear too good to be true or vendors who request money early in the transaction.
- Obtain a full contract before sending money.
- Do an internet search to seek out complaints or fraud claims against the recipient.

Romance/ marriage/ sweetheart

What is it?

Most often, a romance scam is perpetrated by highly organized criminals through an online dating site. In fact, Consumer Reports estimates that 12% of online dating profiles are fake. Fraudsters post false bios, photos, and personas to trick victims into falling in love, then they ask the target to send money or accept money as an unwitting accomplice. The Better Business Bureau reports that in the last 3 years, over 1 million Americans have been victims of romance scams.

How does it work?

In many cases, all correspondence is solely via online channels. Once an emotional attachment is established, the scammer claims to be in the middle of an elaborate financial crisis in an attempt to get the victim to either send money or accept a check on their behalf. For instance, the scammer may claim to be injured, in the hospital, stranded, or detained. The scammer instructs the victim to deposit the money into an account the scammer controls.

Scammers cultivate false romantic feelings by:

- Asking a lot of personal questions to help the scammer prepare responses that appeal to the victim.
- Quickly pushing to communicate through personal email or text, rather than a dating site.
- Professing love for the victim very early in the relationship.
- Insisting they want to meet, but consistently coming up with excuses why they cannot.
- Claiming they have no immediate family to turn to for assistance.

Protect yourself.

- Do not send money to or accept money on behalf of an individual you've never met in person.
- Consult with a family member or trusted individual before sending money or if you have any concerns there may be fraud.
- Perform a Google image search with the person's profile picture to see if results yield any fraud or scam claims or if other names are associated with the person.
- Be wary of profiles set up within the past few days.
- Use caution when sharing personal information with someone you only know online.
- Be on the lookout for spelling and grammar errors, inconsistent details in their stories, or avoidance of video or phone interactions.

Emergency or person in need

What is it?

A fraudster claims to be a family member or friend who is in distress and is in dire need of funds. Adopting an air of urgency, the perpetrator will trick the individual into acting quickly and sending funds before having the opportunity to thoroughly assess the situation or consult with individuals that could verify the claims.

How does it work?

These criminals commonly impersonate a grandchild who has supposedly been arrested, in an accident, or in another emergency situation. A request for money may be made via email, text, or phone call. They will often plead to "not tell the parents" in an effort to keep the situation secret.

In other cases, scammers may impersonate a friend or family member who is supposedly overseas and needs money for bail, medical expenses, or another emergency. Or they may claim to be an attorney, police officer, or doctor calling on behalf of the loved one.

Protect yourself.

- Take time to think through the situation and verify that the person and situation are legitimate.
- Ask the individual questions that only the actual person would know.
- Call the individual on the phone to validate the issue, or speak to another family member or trusted contact.
- Requests for payment using prepaid debit cards, money orders, gift cards, or other anonymous forms of payment are red flags.

Employment/ job opportunity

What is it?

This scam operates under the guise of an employment opportunity that requires up-front payment for services, equipment, or other job prerequisites that come with a cost.

How does it work?

Fake job opportunities or job placement services are posted via the internet, flyers, newspapers, or other channels and require the prospect to provide payment before the job is offered. This may include fees for certification, employment, background checks, equipment, or materials.

- Job placement services may be offered for a fee. The victim pays the fee, but job opportunities never materialize.
- The "employer" may convince their "new employee" to accept funds for deposit with a request to wire most of it to another recipient. In exchange, the victim is supposedly allowed to keep a portion of the funds. The initial deposit is often returned for insufficient funds.

Protect yourself.

- Request contracts or details in writing before making any commitments.
- Do online searches on the hiring company to determine if complaints of scams have been filed. You can also check with the Better Business Bureau.
- Look up the company online to see how long the company has been operating and whether their official site has contact information.
- Be discerning of jobs that offer higher-than-expected wages and seem too good to be true.
- Be skeptical of any job that requires payment for standard hiring expenses such as training or background checks.

Technical support

What is it?

Victims are contacted by what appears to be a technology support team to fix a fabricated technical issue or virus on their computer.

How does it work?

Typically deployed either by phone calls or web pop-ups, these scams usually warn computer owners of non-existent viruses on their computers. The scammer may pretend to be with a well-known company such as Microsoft or Apple to persuade the victim to:

- Pay a fee for services for unnecessary software to “repair” the machine.
- Give the scammer remote access to their computer.
- Perform actions that allow the scammer to deploy malware on the machine.

Protect yourself.

- Do not respond to pop-up notices or calls regarding computer technical issues. If you suspect you have malware, contact your security software vendor or call a reputable computer specialist.
- Do not provide anyone with your login ID and password, and use good judgment when remote access is requested.
- Avoid clicking links in pop-ups. Instead, contact the company directly by navigating to their official website to find contact information.
- If you receive a phone call from an alleged tech support vendor, hang up. Do not rely on Caller ID to verify the caller’s identity, since phone numbers can be made to appear to be from the company being impersonated.

Fake charities/ crowdfunding

What is it?

Scammers present themselves as a reputable charity asking for donations from unsuspecting philanthropists.

How does it work?

Imposters pose as representatives of a legitimate organization soliciting donations via email, phone, mail, or in person. Following a natural disaster, it's common to see a proliferation of scams that claim to be raising funds to assist those affected. Funds are either retained entirely by the fraudster or a disproportionate amount goes to the fundraising efforts rather than the charity itself.

Recently there have been several scams associated with crowdfunding platforms such as GoFundMe and Kickstarter that are heavily publicized on social media platforms. While most crowdfunding efforts are legitimate, fraudsters are using these sites more and more as a way to take advantage of people's desire to help.

Protect yourself.

- Ask the solicitor for their relationship to the charity and what percentage of funds will actually go to the charity itself. It's generally best to donate directly to any charity you want to support.
- Be skeptical of requests to donate in prepaid debit or gift cards.
- Perform online searches, using the name of the charity along with key words such as "complaint," "scam," or "fraud" to determine if issues have been reported.
- Research the charity to determine how donations are used. The FTC suggests these resources:
  - BBB Wise Giving Alliance
  - Charity Navigator
  - CharityWatch
  - GuideStar

Investments

What is it?

This type of scam offers investments that either don't exist or are misrepresented and often claim high returns and minimal risk.

How does it work?

An investment scam can come in many forms:

- Ponzi schemes are scams offering investments that are funded by early investors who are then cashed out with the contributions of later investors.
- Scammers offer the chance to invest in promissory notes, precious metals, loans, and other investment opportunities that either don't exist or are misrepresented when sold.
- In what's known as a pump-and-dump scheme, the market is manipulated using recommendations to buy a thinly traded stock in large quantities. The stock, already held by the scammer, is sold once its price goes up.

Protect yourself.

- Be skeptical of claims of instant returns or high yields with no risk.
- Ask questions. Performing due diligence with any investment is key to mitigating the risk of a scam.
- Get all investment details in writing.
- Being pressured to make a decision quickly is generally a red flag.
- Ask if the investment is registered. Most investments must comply with regulatory filing requirements that can be reviewed by the public.

Goods/ services

What is it?

A person is tricked into purchasing goods or services that are never delivered or are falsely represented.

How does it work?

Items from magazines to cars are listed for sale on electronic channels such as Craigslist, eBay, or local classifieds. After payment is made, the purchased item fails to materialize.

In a related scam, if you are a seller, a purchaser may "accidentally" send an amount greater than the agreed-upon price and ask for a refund of the overage. Ultimately, the original payment is rejected by your bank due to insufficient funds.

Service scams follow a similar pattern. Services are offered, with an up-front deposit required, but the services are never performed.

Protect yourself.

- For transactions over a dollar amount you're not willing to lose:
  - Insist that you physically inspect the item you are purchasing before sending any funds.
  - Obtain formal documentation on the product or item in question, such as an independent appraisal performed by an expert you hire.
  - Require that the seller provide proof of their identity.
  - Some websites, such as eBay, offer guarantees that protect buyers and sellers. Before buying, find out what policies might be in place to protect you.
- Perform Internet searches on the person or service in question. Do not rely solely on positive reviews or recommendations, as they may be false or fabricated.

Prizes/ lotteries

What is it?

A scammer attempts to convince the target that they've won a nonexistent sweepstakes or prize that will be awarded upon payment of fees or taxes.

How does it work?

Attempts may be made by telephone, direct mail, online pop-up ads, or email to notify the target that they have won a sweepstakes or substantial prize that will be awarded following payment of taxes or a processing fee.

Alternatively, a target may receive a check said to be funds from a sweepstakes or other prize. The victim is directed to deposit the funds and immediately wire a portion of it back to cover the fees and taxes, only to find out later that the check was counterfeit.

Protect yourself.

- Use extreme caution before responding to any assertion that you have won a prize—particularly if you have not participated in any contests or if money is required in order to obtain the prize. It is most likely a scam.
- Do not provide any personal information, such as an account number, until the legitimacy of the prize is verified.

Inheritance

What is it?

Similar to the lottery/prize scams, an inheritance scam operates by tricking an individual into believing a person they knew has passed away and left them part of their estate. In order to receive the bequest, the person must provide money for taxes or fees up-front.

How does it work?

A fraudster poses as an estate locator, attorney, banker, or other party, informing the victim they are the beneficiary of an estate or that someone in their extended family has passed without a will. The target is told they are the sole heir and is often provided official-looking documentation to support the claim. The scammer then states that taxes or administrative fees must be paid in order to release the estate. If paid, additional fees will continue to be requested until the individual stops sending money.

Protect yourself.

- Use extreme caution if you're notified of an inheritance, as it is most likely a scam. Most legal and financial entities will not communicate these types of matters by email.
- Consult with your family if you have any indication the inheritance is not legitimate.

IRS/ government

What is it?

This scheme involves contacting individuals by phone or email and demanding immediate payment of taxes that are supposedly owed, by either wire transfer or prepaid debit card. Alternatively, individuals may be informed they are entitled to a large tax rebate and need to provide their banking information to receive the credit.

How does it work?

In many cases this fraud is conducted via phone. Criminals use various techniques to make calls appear to come from the IRS, such as imitating government websites and contacting potential victims via official-looking email. Scammers often use intimidation, threats of arrest, and fear of frozen assets to manipulate targets into making a payment. Payment may be requested via prepaid debit cards, gift cards, or money orders.

Scams such as these sometimes originate from overseas call centers whose sole function is to place calls to unsuspecting targets. Other domestic or foreign government agencies may also be impersonated in this type of scam.

Protect yourself.

Exercise caution and be familiar with IRS practices:

- The IRS never calls taxpayers. Communications are sent via physical mail.
- The IRS never requests credit card, debit card, or bank information over the phone.
- The IRS will never require payment via prepaid debit or gift cards.