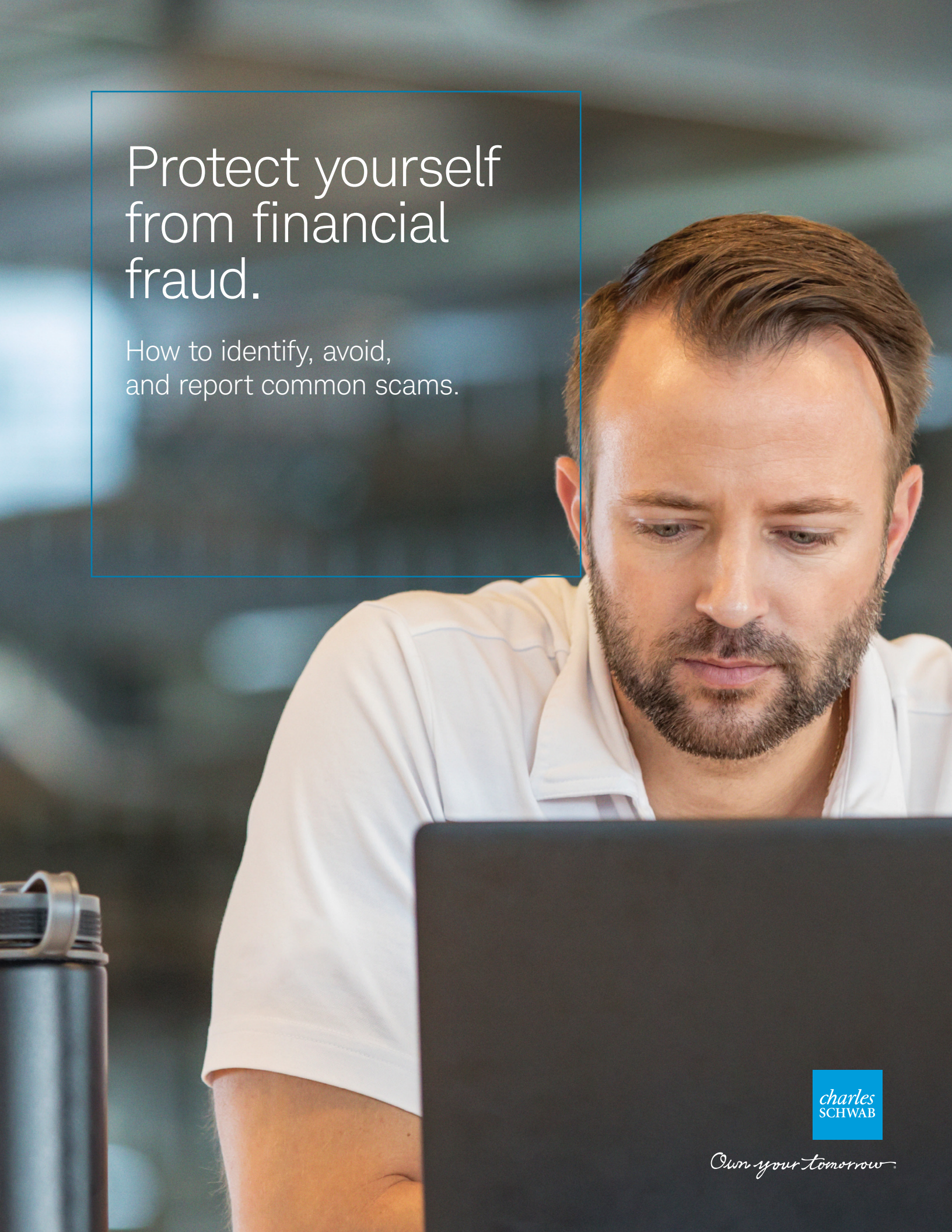
Protect yourself from financial fraud.
How to identify, avoid, and report common scams.
charles SCHWAB
Own your tomorrow®

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
- Text
- Mail
- Phone
- Social media
- Messaging apps

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.

- 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 that 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 who 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. Research the recipient, product, or company to validate the legitimacy of the request and search for scams or complaints associated with the other party.
- Use appropriate disbursement channels and methods to make payments. Avoid prepaid debit cards, gift cards, and digital currency.
- When possible, 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:

- **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 that they have accessed the target's accounts, emails, or webcam using malware and now possess personal files or videos that could be damaging if made public. A payoff is demanded, usually by a quick and difficult-to-trace payment method, with an urgent deadline. In some cases, the extortionist will provide information that makes the claim seem legitimate, such as sharing a password that actually was harvested through an unrelated data breach and sold on the dark web.

Protect yourself.

- Use unique passwords for all accounts.
- Use two-step authentication, when available, for extra protection.
- Install anti-malware and antivirus software, and make sure you install updates and patches as they become available.
- 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 to the target 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 using a known phone number 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. 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 using a known number.
- 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. Criminals have also been known to initiate contact through other apps that have chat features, like gaming apps. 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.

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 a financial crisis in an attempt to get the victim to either send money or deposit a check into the victim's account or another party's account that the scammer ultimately controls. For instance, the scammer may claim to be injured, in the hospital, stranded, or detained. Reasons for funds may be for travel or medical expenses or fees, or even an investment deal where they claim they will receive a large and quick payout.

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 as to why they are unable to.
- 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 an online 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.
- 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. It is not uncommon for the fraudster to research social media ahead of time to gather information about the person they are impersonating so they are more convincing when reaching out to the target. 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 who could verify the claims.

How does it work?

These criminals commonly impersonate a grandchild who has supposedly been arrested, been in an accident, or is 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 a known phone number 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 upfront 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, leaving the victim on the hook.

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 or customer support

What is it?

Victims are contacted by what appears to be a technical or customer support team member from a trusted and known company, like an online retailer or financial institution, to fix a fabricated technical issue, to secure an account, or to discuss a suspicious transaction.

How does it work?

Typically deployed by phone calls, phishing emails, or web pop-ups, these scams usually warn of a non-existent issue. The scammer will create a scenario that creates a sense of urgency 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.
- Provide online credentials to accounts.

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 emails or pop-ups. Instead, contact the company directly by navigating to their official website to find contact information.
- If you receive an unsolicited and unexpected phone call from an alleged technical or customer support representative, proceed with caution. 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?

Impostors 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.

While most crowdfunding efforts are legitimate, fraudsters are using these known and official crowdfunding 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. Investment scams exploit individuals' desires for financial gain by weaving elaborate tales of lucrative opportunities.

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 some scams, the fraudster uses social engineering and technology. The scam often begins when the fraudster makes contact through social media, a dating site, or a chat app. After establishing a friendship or bond, the fraudster will introduce an investment opportunity. It is not uncommon for the fraudster to direct the target to a fake investment site, where it appears as if there are high returns being made. When the victim attempts to withdraw their funds after investing, they will be told taxes or fees need to be paid first. Eventually, the fraudster will cease all communication.

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 upfront 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 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 victim 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, a trusted contact, or an attorney if you have any indication the inheritance is not legitimate.

IRS/tax

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, and may also imitate government websites or contact potential victims via official-looking email. These techniques are known as "spoofing." 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 cards, gift cards, or cryptocurrency.

Timeshare resale

What is it?

Timeshare owners are targeted by scammers with promises that they have a buyer or can easily sell the timeshare but need funds up front to close the deal.

How does it work?

Scammers pose as timeshare resale agents or brokers through unsolicited emails or phone calls claiming they can sell the owner's timeshare. They allege that the deal will be fast or even that the buyer is willing to pay a higher value than the property is worth. Scammers attempt to further legitimize their claims with fraudulent purchase agreements or details about the potential buyer. To obtain their assistance, the owner needs to pay money up front for fees, taxes, or other services. Once the funds are sent, the scammer disappears.

There are also specific schemes within this type of scam targeting owners of timeshares in Mexico or scammers acting as intermediaries for a buyer in Mexico or elsewhere. Scammers may exploit the victim's lack of understanding of real estate and timeshare laws and regulations to convince them that there are additional costs to close on the deal. It doesn't stop there. Often with these scams, the fraudsters will later try to scam the victim again by posing as representatives of companies that can help the victim recover timeshare scam losses.

Protect yourself.

- Be wary of unsolicited outreach from individuals or companies claiming to be able to assist with a timeshare, especially if upfront fees are demanded or they make promises of a quick transfer of ownership.
- Don't wire money, pay in cash or cryptocurrency, or send a money order or a certified bank or cashier's check. Money sent by these methods is very difficult for law enforcement officials to recover. It's as good as lost.
- Look up the company online to see how long it's been operating and if its official site has contact information.
- Consider hiring an attorney to review the documents before taking any action.

Law enforcement or government agencies

What is it?

Scammers claim to be law enforcement agents or representatives from government agencies, either foreign or domestic, and tell the victim they are under investigation or will be arrested for a crime or other violation.

How does it work?

There are variations of the scheme, but typically the fraudster calls a target and claims to be a law enforcement officer or government agent. They commonly allege that there are unpaid fines or an open investigation, or they may claim that the target's money needs to be transferred due to a compromise. In some cases, victims have been given wire instructions under the guise that they need to move their money to a "secure" account.

In more elaborate variations, scammers pose as representatives of a foreign government, like an official from the Chinese consulate, and claim that the victim, who may be an immigrant, will be deported from the U.S. if they do not cooperate by sending money as part of an ongoing investigation. Some victims have reported receiving images of government identification or documents that are purportedly related to the investigation. Like many scams, the victim is told to keep the matter a secret and that if they share details about it with anyone, there could be additional charges.

Protect yourself.

- Advance warnings of arrests are not given, nor would law enforcement call for unpaid fees.
- Government bodies will not call and ask you for money to open or continue an investigation or to resolve a potential arrest or deportation.
- Pause and take time to confirm that the government agent or law enforcement official and the investigation are both legitimate by verifying the claim through official channels.

Crypto

What is it?

Cryptocurrency scams are fraudulent schemes that exploit the digital nature of cryptocurrencies to deceive individuals into handing over their assets or money. Scammers often impersonate legitimate businesses, create fake investment opportunities, or promise unrealistic returns to trick victims. Their goal is typically to steal cryptocurrency or manipulate victims into making payments under false pretenses. Unlike traditional scams, cryptocurrency scams can be harder to trace due to the anonymity and decentralization of blockchain technology, making them particularly dangerous.

How does it work?

Scammers exploit the growing interest in cryptocurrency through various deceptive tactics designed to trick people into handing over their money or digital assets. Here are some common types of cryptocurrency scams:

- **Romance Crypto Scams:** Scammers create fake profiles on dating apps or social media, posing as potential romantic partners. After building trust, they introduce the idea of investing in cryptocurrency, often promising quick and significant returns. If someone you meet online pushes you to invest in crypto, share your wallet details, or send them cryptocurrency, it's almost certainly a scam.
- **Impersonation Scams:** Scammers may pose as legitimate entities like financial institutions, government agencies, or utility companies. They often claim that you owe money for overdue taxes, fines, or other legal obligations, demanding payment in cryptocurrency. In some cases, they may say your bank account is compromised and instruct you to transfer your funds to a crypto account for "safekeeping." Legitimate organizations will never ask for payment or transfers in cryptocurrency.
- **Fake Posts, Ads, and Celebrity Endorsements:** Scammers often use fake social media posts, ads, and endorsements from celebrities to lure victims into cryptocurrency scams. These schemes typically promise free cryptocurrency giveaways or exclusive investment opportunities. The scam might direct you to a website where you are asked to verify your account by making a small payment in cryptocurrency, or it might claim that a celebrity is giving away crypto to their followers. In reality, these are fraudulent schemes designed to steal your money or personal information. Always be skeptical of offers that seem too good to be true, especially when they involve cryptocurrency.
- **Blackmail Scams:** Criminals may claim they have compromising photos, videos, or personal information about you. They threaten to release this information unless you pay them in cryptocurrency. These threats are usually empty, and paying only encourages further extortion.

Crypto

Protect yourself.

Cryptocurrency scams are becoming more sophisticated, but there are ways to avoid becoming a victim and steps you should take if you are victimized:

- **Be Skeptical of Unsolicited Contacts:** Whether it's a message from a "new friend" or an urgent email from a company or government agency, be wary of anyone asking you to pay with cryptocurrency. Never click on links or send money without verifying the authenticity of the request.
- **Research Before Investing:** Before you invest in any cryptocurrency or engage with a new crypto service, thoroughly research the platform and its reputation. Avoid investments that sound too good to be true, as they often are.
- **Secure Your Wallet Information:** Never share your cryptocurrency wallet details with anyone, especially online. Use secure and reputable wallets, and enable two-factor authentication to add an extra layer of security.
- **You can report crypto scams** to the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), or the FBI's Internet Crime Complaint Center (IC3).

Utility

What is it?

Utility customers are frequent targets of fraud as scammers use emails, phone calls, or text messages that threaten to cut off service unless money is sent immediately. Scammers typically demand money using online payment platforms such as Zelle®, or prepaid debit cards and wire transfers, which are difficult to trace. It's almost impossible to recover the money once it is sent.

How does it work?

- Impersonators will often make contact regarding supposedly delinquent bills, threatening to terminate service. They'll typically time attacks during peak utilities seasons to create urgency and pressure the victim.
- Utility impostors send out phishing emails or "smishing" text messages aimed at convincing you to make a payment or to supply personal or financial data to resolve a service issue.
- Scam callers might also say you've overpaid, and ask for bank account or credit card information to make a "refund." Or they may say they'll sign you up for a government program that reduces energy bills.
- Identity thieves also use stolen personal information to open utility accounts and run up charges in the victim's name.

Protect yourself.

- Utility companies will not request personal information over the phone, and they do not cut off service without advance warning. If a caller claims to be from a utility company and pressures you for immediate payment or personal information, hang up and call the customer service number on your utility bill. Scammers will sometimes "spoof" the real number for a utility company, so even if your caller ID shows the company's official number, it is best to hang up and call back if the call seems suspicious.
- Beware of unusual payment methods. If the caller demands you send payment via a prepaid debit card or wire transfer, that is generally a red flag that the call is part of a scam.
- Don't click on links in a utility-related email or text message unless you're certain it's from the real company.
- If you receive a utility shut-off scam call, you should report it to your utility company and your local police department or sheriff's office. You can also report utility shut-off scams online to the Federal Trade Commission ("FTC").

Online marketplace

What is it?

Online shopping or marketplace scams typically involve fraudsters pretending to be legitimate online sellers, either with a fake website or a fake ad on a genuine retailer site. These types of scams are increasing with the prevalence of mobile apps and social media such as Facebook Marketplace. Scammers may also seed phony sites, apps, or links in pop-up ads and email coupons with malware that infects your device and harvests personal information for use in identity theft. Not surprisingly, these frauds flourish during the holiday season and other major shopping events.

How does it work?

- Many fake online stores mimic trusted retailers, with familiar logos and slogans and a URL that's easily mistaken for the real thing. They offer popular items at a fraction of the usual cost and promise perks like free shipping and overnight delivery, exploiting the premium that online shoppers put on price and speed.
- A buyer, sometimes using a stolen credit card, will pay the seller more than the requested amount for an item, then claim to have made a mistake and request a partial refund. The victim will return the overage amount, but the original payment is declined and never ends up in the seller's account, so the victim is stuck paying the bill while the criminal pockets the money.
- Scammers may ask to communicate outside the online marketplace, including through text messages or WhatsApp, and lure victims into sharing personal information, like a phone number, an email address, or a photo ID, to confirm their identity. Once they have this information, they can commit other acts of fraud using the victim's identity.

Online marketplace

Protect yourself.

General red flags when using an online marketplace include not being able to meet in person, shoddy website design/misspellings, being redirected to conduct transactions on a different website, prices that are too good to be true, and paying in advance through untraceable means, including gift cards, wire transfers, or P2P payment apps. Additional things to consider and steps to take if you become a victim are detailed below:

- Use trusted sites rather than shopping with a search engine. Scammers can manipulate search results to lead you astray.
- Research unfamiliar products or brands with search terms like “scam” or “complaint,” and look for reviews.
- Read delivery, exchange, and refund policies. If they are vague or nonexistent, take your business elsewhere.
- Look for misplaced or transposed letters in URLs or website names.
- Don’t provide more information than a retailer needs. That should be only your billing information and the shipping address.
- Don’t use sites that require you to download software or enter personal information to access coupons or discount codes.
- If you’ve been victimized by an online marketplace scam, file a report with the FTC and the FBI’s Internet Crime Complaint Center. The FTC website also has advice on safe online shopping.
- Report suspicious online marketplace operations to the BBB Scam Tracker, which also lets you search for scams in your region, and file a complaint with your state’s consumer protection agency.

©2024 Charles Schwab & Co., Inc. All rights reserved. Member SIPC.
CC11537344 (1024-WHJY) MKT104427SCAM-03 (10/24)