Scam definitions and prevention client guide

As you know, protecting your assets and data is priority number one for our firm. But it's also important that you know about threats you may encounter in other interactions online—from your personal email account to social media and dating apps. In each of these channels, you may run into scams specifically designed to steal your information or assets. To help you recognize and avoid such situations, we're providing this guide, which explains what scams are and some telltale signs to help you recognize a number of prevalent ones. We also outline steps that you can take if you ever fall victim to a scam. By reviewing this information, maintaining best practices, and exercising caution in your online activities, we can work together to keep you safe.

What is a scam?

A *scam* is a dishonest or fraudulent scheme. In a typical scam, victims are convinced to send money or provide personal information, believing it's for a legitimate purpose or going to a trusted recipient. A scammer might also attempt to involve an individual as an intermediary, using them to launder funds stolen from another individual, business, or government agency.

Communications from scammers can originate from almost any source—including mail, email, social media, telephone, and text message—and are often made to appear as though they are from trustworthy parties.

Scams are on the rise, and no one is immune. People of all ages and levels of financial experience have been and continue to be affected. The first step in protecting yourself from falling victim is to be aware of the types of scams and the telltale signs that one may have targeted you.

Types of scams

GALECKI FINANCIAL MANAGEMENT

1. Romance/marriage/sweetheart

Seeking romance online can have a major downside: the internet is rife with scammers ready and willing to take advantage of people looking for love. According to a recent study, as many as 10% of online dating profiles are fraudulent.[1]

In addition to using online dating profiles, scammers have been known to initiate contact through more general platforms that have messaging or chat features, including social media and gaming sites. As a rule, these schemes avoid in-person interactions, preferring instead to focus exclusively on messaging apps and other online channels.

The scam works something like this: Your romantic interest may claim to live in another part of the country or to be abroad for business or military deployment. They seem to be really interested and eager to get to know you. They work to cultivate an emotional attachment by:

- Asking a lot of personal questions to help prepare responses that appeal to you; for example, “Are you interested in a lifetime relationship?”
- Quickly urging you to communicate through personal email or text rather than a monitored channel like messaging through a dating app
- Lavishing you with attention and often professing love very early in the relationship
- Claiming to have no immediate family, sometimes mentioning the loss of a loved one

Once an emotional attachment is established, the scammer is eager to meet you in person. When the opportunity arrives, however, something invariably comes up—an accident, a health crisis, or other such unexpected occurrence; that is usually followed by an urgent request for financial assistance. For example, the scammer may claim to be stranded or detained, needing to pay a medical bill, or unable to meet an expense related to a quick business payout. If you can help out, they will pay you back as soon as they’re out of the current circumstances.

The scammer then instructs you to send money, promising a quick payback. But there is no return of funds, and, in some instances, they ask for yet more money.

How to protect yourself

- Be wary of profiles set up very recently.
- Right-click and use your browser’s search feature to see if the person’s profile picture was copied from somewhere else on the internet, if the person is known by more than one name, or if the photo has been associated with other fraud or scam claims.
- Take things slowly, asking plenty of questions and noting any inconsistencies or red flags. Unwillingness to meet in person or speak on the phone can be cause for concern.
- Use caution when sharing personal information with someone you know only online.
- Consult a friend, family member, someone at our firm, or another trusted individual if red flags arise. Be willing to listen if they express concern.
- Do not send money to or accept money on behalf of an individual you’ve never met in person.

Questions to ask yourself

- Do I know the recipient of the funds and have I met them in person?
  - In many romance scams, the victim has never met the scammer face-to-face.
- Did the recipient initiate contact?
- Have they requested funds in the past?
- Was I told that there was an “emergency” situation that caused financial need?
  - A scammer may send a video or picture of an accident or other event to lend credibility.
  - If you answered yes to any of these questions, cease communication with the individual and discuss the request with your advisor.

1. https://besedo.com/blog/welcome-to-the-age-of-fake-dating-profiles/

2. Sweepstakes/lottery

Who wouldn't love winning a million dollars, a fancy new car, or the chance to take a dream vacation? In this type of fraud, scammers take advantage of such desires, imitating the many legitimate sweepstakes and contests.

Scammers may contact you through mail, email, social media, a text message, or even a phone call, congratulating you on "winning." All that's required to collect your prize is a small fee to cover taxes, shipping, customs charges, or some other expense.

They may also claim that they need personal information to prove your identity or that they need bank account details to deposit your "winnings." This is the information they subsequently use to drain your account.

How to protect yourself

- Ask yourself if you entered a particular contest. If you didn't, the prize notice is likely a fake.
- Don't wire money; mail cash, checks, or money orders; or share gift card numbers with someone claiming to represent a sweepstakes or lottery. A legitimate contest would not ask you to pay to collect your prize.
- Don't deposit a check from a sweepstakes or lottery without doing due diligence, such as researching the sender's name on the Better Business Bureau website to validate the source of the request. Also note that many scams will ask you to send part of the payment back. Legitimate sweepstakes send only certified checks to prizewinners.
- Don't provide personal or financial information to anyone who contacts you about a lottery prize.

Questions to ask yourself

- Is there a sense of urgency or a strict deadline to redeem the prize?
- Did I enter a sweepstakes or lottery?
- Was I told that I must pay (a small fee) in advance to get the prize?
- Did I receive any advance payment in paper form, such as a check or money order?

3. Government impersonator

In this type of scam, the criminal pretends to be from a government agency like the Social Security Administration (SSA), the Internal Revenue Service (IRS), or law enforcement.[1] They attempt to intimidate you into paying a fine or penalty that you supposedly owe to the government.

They may contact you initially through an email, a text message, or social media, but usually these scams start with a phone call. The scammer advises you that unless you act immediately, you will suffer the loss of a benefit or even face a large fine or criminal charges. The scammer can be aggressive and may threaten to confiscate property, freeze bank accounts, or send authorities to arrest you.

SSA and Medicare impersonators

In this type of fraud, the scammer claims that unless you pay immediately, your Social Security or Medicare benefits will end or your Social Security number will be suspended. They often request personal information, such as your Social Security or Medicare number, to steal your identity while they're scamming you out of money.

To be clear: The SSA and Medicare will not threaten to end your benefits, nor will they suspend your personal ID number.

IRS impersonators

The fraudster claims that you owe taxes and uses threats of arrest or deportation if you do not pay immediately. They may also claim that your driver's or professional license will be revoked if you fail to cooperate. To appear more authentic, they may pretend to have information about you, including your Social Security number or taxpayer ID number.

The IRS communicates primarily through the mail, including in cases involving delinquent taxes. The IRS never demands immediate payment, nor does it make threats of arrest or to call the local police.

Law enforcement impersonators

This type of impersonator claims to be with the local court, sheriff's office, or police department and asserts that you missed a court date, failed to appear for jury duty, or have delinquent taxes or unpaid citations. The scammer threatens that unless immediate payment for these fictional infractions is made, a warrant will be issued for your arrest.

Law enforcement agencies do not call individuals and demand money, nor do they accept gift cards as payment.

There have also been instances of scammers impersonating foreign governments or law enforcement agencies.

1. https://www.consumer.ftc.gov/articles/how-avoid-scam

How to protect yourself

- Don't wire money, mail cash, or use gift cards or cryptocurrency to pay someone who claims to be from the government. Scammers may request that you use these methods because they are hard to track and it's almost impossible to get your money back.
- Don't give financial or other personal information to anyone who calls you claiming to be with a government agency. If you suspect a scam, hang up, then call the government agency directly at a number you know to be correct.
- Don't trust your caller ID. It is common for impersonators to spoof the names and numbers of government agencies.
- Don't click on links in unexpected emails or text messages. Scammers send messages that look like they're from a government agency but are designed to steal your money and your personal information. Report the message as phishing to the real government agency, then delete the message.

Questions to ask yourself

- Did I call the person back at the number they provided? Can I find that same phone number on the IRS or other government agency website?
- Was there a sense of urgency regarding the payment?
- Were there any threats made if payment wasn't received?
- Was I asked for any personal information and did I provide it?
- How did the "representative' contact me?
- Did I click any hyperlinks in an email or text message?

GALECKI FINANCIAL MANAGEMENT

4. Tech or fraud support

Scammers often exploit your fear of computer viruses and hackers to try to steal your money or identity.

Some pretend to be connected with well-known companies, like Apple, Microsoft, or Amazon. Others claim to be employees of a familiar security software company such as Norton or McAfee. The storylines vary based on the company they're pretending to be with, but the tactics are always similar.

Tech support

This scam typically starts when you respond to an unsolicited phone call or pop-up warning on your device. The scammer will ask for remote access to your computer to run a phony test, which pretends to detect malware or viruses. After using this to scare you, they pressure you to pay for "repairs," new software, and other products and services you don't need.

In a variation, the scam involves a claim that you are due a refund for a canceled subscription service, one you likely do not recall signing up for. The scammer will request (and steal) your credit card number, then use remote access to install actual malware that will continue stealing your information and funds long afterward.

Fraud support

This refund scam typically starts with an unsolicited call or email claiming that a charge was made to your account. Once you deny knowledge of the charge, the scammer claims that they can help you get a refund. They request access to your computer and have you sign into your bank account to "deposit" the refund. Once you do, they may steal your money or convince you that they deposited too much money and that now you must pay them back—usually via wire, gift card, or cryptocurrency.

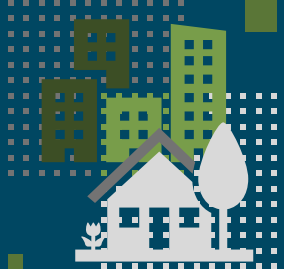
How to protect yourself

- Don't give remote access to your computer or payment information to someone who calls you unsolicited.
- Don't rely on caller ID to determine whether a caller is legitimate. Scammers use "spoofing" techniques to make it look like they're calling from a legitimate number or company. Hang up and call the company at a number you know to be correct.
- Don't call a number in a pop-up virus alert. Legitimate warnings from your operating system or antivirus program do not ask you to call anyone for support.
- Don't click links in a pop-up, even to close the window. This could redirect you to a scam site or launch a "dialogue loop," continually serving pop-up messages.
- Don't buy security software from a company you don't know. If the name is unfamiliar, do an internet search to see whether it has been linked to adware or scams.
- When you restart your browser after getting a scam pop-up, don't open previously closed sites if prompted to do so.
- Don't give financial information to someone who calls a few days, weeks, or months after you've made a purchase and asks if you are satisfied. If they ask for your financial information, it's probably a refund scam.

Questions to ask yourself

- Did I click any links or navigate to any websites per their instruction?
- Did the caller mention any consequences if the problem was not resolved?
- Did I provide my login ID or password or allow anyone to see me enter it?
- Did they say that money was erroneously deposited into my account?
- Did they show me a screenshot of my account on my device's screen?

GALECKI FINANCIAL MANAGEMENT



5 . Real estate scam

According to the Consumer Financial Protection Bureau, during the closing process scammers send spoofed emails to homebuyers, posing as the real estate agent, settlement agent, legal representative, or another trusted individual with false instructions for wiring closing funds.

How bad actors carry out real estate scam

Scammers engaging in closing transaction scams may employ the following strategies:

- Compromise the email address of the title/escrow company that sends the wire instructions
- Provide phony contact information on correspondence
- Fraudulently establish accounts in the name of a title/escrow agent or law firm
- Use phishing to install malware onto a victim's device
- Intercept email correspondence from the actual title/escrow company

Caution

Email, phone applications, and SIM cards can be compromised by scammers. Always verify wire instructions verbally when they are received by electronic means.

Scammers use phony contact information on fraudulent emails containing the phony wire instructions.

How to protect yourself

- Verify the closing instructions in person, if possible, or by calling the title/escrow company at a number known to you.
- Verbally verify payment instructions and any change to an account number with the person making the request.

Questions to ask yourself

- Have I wired to this specific account before? Did the title/escrow company acknowledge receipt of the wire?
- How did I receive the wire instructions (text, email, verbally, or in person)?
- Did I use a phone number from the title/escrow company's website?
- Did I see the property in person with a registered real estate agent/broker?

GALECKI FINANCIAL MANAGEMENT

6. Business email compromise

Business email compromise (BEC)—also known as email account compromise—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business, both personal and professional.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, as in these examples:

- A vendor your company regularly deals with sends an invoice with an "updated" mailing address.
- An assistant gets a request from her "manager," asking her to purchase dozens of gift cards to send out as employee rewards. The "manager" asks for the serial numbers so that she can email them out right away.
- The client is in the process of purchasing a home and receives a message from the "title company" with instructions on how to wire the down payment.
- A "payroll representative" sends an email asking for direct deposit information.

How bad actors carry out BEC scams

- **Spoof an email account or website.** Slight variations of legitimate addresses (*john.kelly@examplecompany.com* versus *john.kelley@examplecompany.com*) fool you into thinking that fake accounts are authentic.
- **Send spear-phishing emails.** These messages appear to be from a trusted sender to trick you into revealing confidential information, enabling criminals to access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information can then be used to send messages or time payment requests so that accountants or financial officers don't question their legitimacy. Malware also lets criminals gain undetected access to your data, including passwords and financial account information.

How to protect yourself

- Verify payment and purchase requests in person, if possible, or by calling the person at a number known to you.
- Verbally verify any change to an account number or payment instructions with the person making the request.
- Be careful what you share on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your passwords or answer your security questions.
- Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one the potential scammer is providing) and call the company to verify that the request is legitimate.
- Scrutinize email addresses, URLs, and spelling used in any correspondence. Scammers make subtle changes to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- Set up two-factor (or multifactor) authentication on any account that allows it—and never disable it.
- Be especially wary if the requestor is pressuring you to act quickly.

Questions to ask yourself

- Do I personally know the sender?
- Did I check for minor spelling errors in the email?
- Is the information requested something they should already know?
- Was there a change in the original instructions?
- Did I call the sender to confirm the request or information after receiving the email?
- Did I click the link or go directly to the official website?
- Was I expecting an attachment?

7. Investment scam

Investment scams often begin with an offer of a “once-in-a-lifetime opportunity” that will double or even triple your money in a short time, followed by promises of high returns with little risk. They may use such phrases as “incredible gains,” “breakout stock,” or “huge upside.” Recommendations of foreign or “offshore” investments may also be shared.

Financial manipulation schemes, also known as “pig-butchering” scams, is a type of investment fraud that lures individuals into investing their money in seemingly legitimate and profitable ventures. Scammers gain trust, manipulate emotions, and exploit financial vulnerabilities to steal money.

How bad actors carry out investment scams

- Scammers make contact through a call, a text, an email, or a social media message. They may send you a friend request or claim to know you through a “mutual” party.
- Scammers spend weeks or months building a relationship with you, often feigning romantic interest. They engage in frequent, friendly communication, showing interest in your life and sharing personal stories to create a false sense of intimacy. They do not initially bring up anything about money or investments. They may use “mirroring” techniques to match your language, interests, and beliefs to create a sense of connection and familiarity. Scammers may sometimes even send small gifts or tokens of affection to gain your trust and emotional investment.
- The scammer then encourages you to pay through wire transfer or cryptocurrency. They may use websites that make it appear that your money has actually been invested and is earning the promised returns.
- For claims of an offshore investment, the scammer wants you to transfer the funds overseas, knowing that once the money is out of the country it is more difficult for U.S. law enforcement to assist you in getting it back.
- Pig-butchering scammers often use fake images and impressive yet fraudulent investment portfolios to convince you of the legitimacy of their schemes. Once you are hooked and have invested a significant amount of money, the scammer suddenly disappears, leaving you no way to contact them to recover your funds.

How to protect yourself

- Be cautious of unsolicited messages and group chats.
- Don’t give in to pressure to invest immediately, and don’t be influenced by promises that seem too good to be true.
- Always discuss any investment opportunities with someone at our firm—after all, why we're here!
- Verify the legitimacy of brokers and always check the investment professional’s credentials with your state securities regulator or the Financial Industry Regulatory Authority—or ask someone at our firm to do so for you.
- Get all the details of an investment in writing—and still do your research. Ask questions about costs, timing, risks, and other issues.
- Be skeptical of investments with promises of high returns and low risks. Don’t invest just because the person offering the investment seems nice or trustworthy or has professional titles.
- Be wary of "affinity" fraud. Don’t invest based on claims that other people “just like you” have invested.
- Don’t feel obligated to invest, even if the professional gave you a gift, bought you lunch, or reduced their fee.
- Report suspicious activity. If you encounter a potential pig-butchering scam, report it to law enforcement and our firm.

Questions to ask yourself

- Do I know the person who contacted me? Did I recognize the phone number?
- What research have I performed on the broker and/or firm that contacted me?
- Was I promised a certain return or high profits? Was it mentioned that this offer is available only for a limited time? Was there an aspect of “everyone is doing it”?
- Did the seller give me something for free?
  - Salespeople count on those freebies to guilt you into buying what they are selling.
- Was I given investment details, such as a prospectus and performance history, in writing?
- Were there any misspellings or unusual things about any documents or correspondence?
- Did I ask if the investment was registered?

GALECKI FINANCIAL MANAGEMENT

Remember: If you are ever suspicious of any situation like the ones discussed here, please call us. We are eager to help you, especially when it comes to your security.

Do you suspect a scam or that you may be the victim of a scam?

Immediately contact our firm or call Schwab Alliance at **800-515-2157**

Learn more about scams from these trusted external resources:

- SchwabSafe/Protect yourself from financial fraud
- www.fbi.gov/scams-and-safety
- consumer.ftc.gov/features/scam-alerts

According to the Federal Trade Commission (FTC), the **email is the most common contact method** for scammers.[1]

FTC data shows that **consumers reported losing more than $10 billion** to fraud in 2023.[2]

Nearly **1 in 3 Americans report being a victim** of online financial fraud or cybercrime.[3]

1. https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business
2. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
3. https://www.ipsos.com/en-us/nearly-1-3-americans-report-being-victim-online-financial-fraud-or-cybercrime#:~:text=Nearly%201%20in%203%20Americans%20(31%25)%20report%20being%20a,18%2D34%20(22%25)

GALECKI FINANCIAL MANAGEMENT