Scam Definitions and Prevention

Protecting your assets and data is a priority 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 to 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 document, which explains what scams are and some telltale signs that will help you recognize a number of popular scams. We also provide steps 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 and your assets 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 becoming a victim is to be aware of the types of scams and the telltale signs that one may have targeted you.

Types of scams

1. Romance/Marriage/Sweetheart
2. Sweepstakes/Lottery
3. Government Impersonators
4. Investment
5. Tech or Fraud Support
6. Business Email Compromise

1. Romance/Marriage/Sweetheart

Seeking romance online can have a major downside: the internet is full of scammers ready and willing to take advantage of people looking for love. According to the Better Business Bureau, out of 3.5 million dating profiles online, 500,000 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 the victim with attention and often professing love very early in the relationship
- Claiming they have no immediate family, sometimes mentioning the loss of a loved one

Once an emotional attachment is established, the scammer is eager to meet in person. When the opportunity arrives, though, something will come 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 will 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 a 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.

1. https://www.timesrecordnews.com/story/news/local/2020/02/13/study-online-dating-site-fraud-attacks-up-sharply/4736697002/

2. Sweepstakes/Lottery

Who wouldn't love winning millions of 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 or email, social media, a text message, or even a phone call, congratulating you on "winning." The only thing required to collect your prize is a small fee to cover taxes, 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 sweepstakes or lottery would not ask you to pay to collect your prize.
- Don't deposit a check from a sweepstakes or lottery without doing due diligence, like researching the sender's name on a site like the Better Business Bureau 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.

3. Government Impersonators

In these scams, the criminal pretends to be from a government agency like the Social Security Administration (SSA), the Internal Revenue Service (IRS), or law enforcement. 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 or Medicare impersonators

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 impersonator 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

The 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 demands immediate payment for these fictional infractions, or 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.

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 contacts you claiming to be with a government agency. If you suspect a scam, hang up the phone and 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 known agencies.
- Don't click on links in unexpected emails or text messages. Scammers send emails and text 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.

4. Investment

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.

Some scammers may first make an emotional connection, aka romance scam, and try to convince you that they have an opportunity for you.

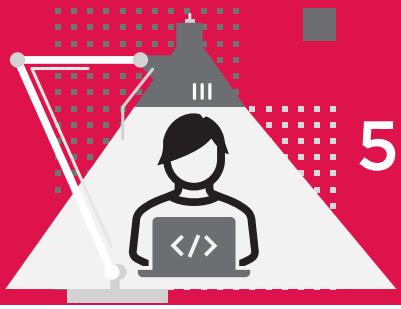
They offer a "once-in-a-lifetime opportunity" that will double or even triple your money in a short time followed by promises of high returns with little risk. They may use such phrases as "incredible gains," "breakout stock," or "huge upside." Recommendations of foreign or "offshore" investments may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

The scammers then encourage 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 scammers want 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.

How to protect yourself

- 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
- Always check the investment professional's credentials with your state securities regulator or the Financial Industry Regulatory Authority.
- Get all the details of an investment in writing but still do your own research.
- Ask questions about costs, timing, risks, and other issues.
- Don't invest just because the person offering the investment seems nice or trustworthy or has professional titles.
- 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.



5. 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, such as 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.

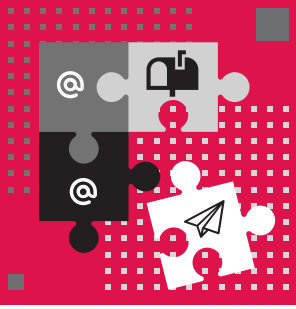
In another variation, the scam involves a claim that you are due a refund for a canceled subscription service, one you likely do not recall signing up for. The scammer will request (and steal) your credit card number, then use remote access to install actual malware that will continue stealing your information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

Fraud support

This "refund scam" typically starts with an unsolicited call or email claiming that a charge was made in 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 through 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 if 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 on a number you know to be correct.
- Don't call a number in a pop-up virus alert. Real 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 if 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.



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 the "manager," asking the assistant to purchase dozens of gift cards to send out as employee rewards. The "manager" asks for the serial numbers so the assistant 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** vs. **john.kelley@examplecompany.com**) fool you into thinking 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 time requests or send messages so that accountants or financial officers don't question payment requests. 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 in 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 a 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 pressing you to act quickly.