University of Kentucky
College of Agriculture, Food and Environment
Cooperative Extension Service

A BAD DEAL IN DISGUISE:
TYPES OF SCAMS

A Bad Deal in Disguise: Types of Scams

By Kelly May
Family Finance and Resource Management

We all know to beware of things that sound "too good to be true." The trouble is, sometimes it is difficult to tell what is false from what is true. Especially since many times scammers appear in disguise or use other tricks to convince us to take part.

The Federal Trade Commission received 2.9 million fraud reports in 2021. Of those reports, about a quarter of them resulted in a loss, equaling a total of $6.1 billion. The best way to avoid becoming one of these statistics is to learn more about different types of scams so you can avoid falling victim.

IMPOSTER SCAMS

Many scams start with a scammer in disguise. One in five people lost money to **imposter scams**, at a $1,000 median loss, according to 2021 data from the Federal Trade Commission. In an imposter scam, the scammer pretends to be someone else – a trusted source or a business you probably already have dealings with – to trick you into sharing information or money.

Sometimes scammers will play on your trust, pretending to be someone you know, such as in a phishing attempt, grandparent scam, or romance scam. Sometimes they try to scare you into paying something they falsely claim you owe, such as in IRS, deputy sheriff, or tech support scams. If they ask for money, they typically want you to use a wire transfer or pay by gift card – which can't be tracked or reversed. Let us explore a few of these scenarios in greater detail.

In **phishing scams**, the scammer pretends to be someone else to trick you into sending money or to get your information, such as a password, account number, or Social Security number. Most people know your bank will never ask for your account number – they already have that information on file. However, when you get an email or text message that looks like it is from your bank and requests information, it is tempting to reply. The scammer is counting on this reaction.

Phishing attempts come in many forms. Someone may claim to be a long-lost relative or a prince from a far-away land with an inheritance to share. It may look like a well-known shipping service with a link to track "your order" that you don't recall placing. It may appear that a service you subscribe to, like a television streaming service or utility, has "declined" your payment, with a request to update your credit card information. Sometimes the scammer claims to be a well-known company or store and says they need to access your account to "investigate fraudulent charges."

Always beware of clicking on links in emails and on websites. These could lead to false websites with malware, malicious software that could damage your computer, phone, or tablet or make your information vulnerable. Check links and email addresses by hovering your mouse over them and waiting for the box to pop up to show where the link really goes.

A **"grandparent" scam** often targets seniors. A caller on the phone claims to be the senior's grandchild (or other relative) in trouble. In this scenario, the false relative has been arrested or stranded and needs money immediately. Often, they will ask for suspicious forms of payment, such as a wire transfer, pre-paid credit cards, or gift cards. The caller stresses urgency and secrecy, not wanting to upset "mom and dad." If you get a call like this from a "grandchild" or someone supposedly representing a relative, hang up. If you want to verify, you can contact the relative or relative's family directly to make sure they are safe.

Romance scams are another type of imposter scam that often begins through online contact. Typically romance scams will use social media,

dating platforms, or messaging apps. A scammer may research you and pretend to have common interests or use a profile you might find attractive. If your new romantic interest is reluctant to meet in person that could be a red flag. Another red flag is if the relationship moves along very quickly – although some scammers are quite patient. After some time and trust has built, your new love interest needs money. The premise might be that they are in trouble, or they need money to settle accounts or pay for travel to visit or move closer. Watch out if payment methods are those that can't be tracked or reversed.

Imposter scams may prey on your urge to help others in need, or they may pretend to offer you help. For example, people are often generous in times of tragedy or natural disaster. Scammers know this and may pretend to represent a charity. **Charity scams** may take the form of false charities asking for money transfers. On the other hand, in **tech support scams**, the imposter pretends to "assist" you with computer issues you may not have known about – because they don't exist. This may happen through phishing, phone calls, pop-up ads, or via a locked screen providing a number to call and "fix" it.

Finally, sometimes imposters use a disguise to threaten or scare you into paying money or revealing information. Reported disguises have included the **Internal Revenue Service (IRS) scam**, sheriff or

deputy sheriff scam, the **Social Security scam**, or the **Medicare scam**. Threats can sound scary, like your Social Security number being linked to "criminal activity" or a warrant for your arrest. Sometimes they may claim that your benefits will be suspended or that your identification will be revoked. They ask that you wire money or use gift cards to pay fees or settle accounts. If you have real concerns about any of these issues, contact local officials directly in a separate call using a verified office phone number.

ADVANCE FEE SCAMS

Other scams revolve around trying to get you to pay money up front in the hopes that you will receive a larger "reward" later. The Federal Trade Commission's top 10 fraud categories included **advance fee scams** such as online shopping, sweepstakes and lotteries, and fake check scams, among others.

Online purchase scams are on the rise according to the Better Business Bureau (BBB), making up more than 38% of scams reported to the BBB in 2020. More than a third of those reports were about pets and pet supplies, such as specific breeds of dogs. Most often, victims of this scam paid for a product or service and never received it. Others received a fake or lower-quality item or something else entirely. This could happen on an unfamiliar website, or when using seller platforms like Facebook Marketplace or Craigslist.

Government grant scams and **fake loan scams** work in a similar way. These claim to be loans or government grants for college, home repairs, home business costs, or other expenses. You may be asked for an advance payment for fees or taxes before you can receive the money. Alternatively, they may ask for your checking account information so they can "deposit the money" or "withdraw a one-time processing fee." Everyone has access to a free list of available federal grants at grants.gov; you should never have to pay for this list.

The **prize, lottery, or sweepstakes scam** continues to circulate, possibly because the idea of winning

sounds so tempting. Real prizes are free, and you have to enter to win. Scammers might surprise you with a "win" you weren't expecting. If you need to pay a fee, such as for taxes, processing, or shipping, then it is probably a scam. You also cannot increase your odds of winning by paying – that is another version of the scam.

Another type of advance fee scam is the **home improvement scam**, which preys on victims of natural disasters. When a weather event leaves destruction behind, there may be door-to-door construction workers who claim to have "leftover" materials they want to use, and they offer a "discount" for their work. Often, they take the deposit but never complete the project.

Fake check scams, conversely, are like an advance fee scam in reverse. Someone sends you a check or money order that is "accidentally" more than the purchase price. The sender says to deposit the check and wire transfer the extra money back to them. However, that check could be counterfeit or may bounce.

Similarly, **employment scams** may involve an "employer" who sends "the employee" a check and asks for money to be sent back in return. Or the

employer promises to reimburse your costs and fees for doing a service, but never pays. In another version, the company may require up-front money for license, registration, or insurance. The false employer may even provide forms or contracts that are very convincing.

TIPS TO AVOID SCAMMERS

No matter who you're dealing with, it pays to **do some research**. Verify online businesses through a trusted outside source before paying. When shopping online, **use sites that are encrypted**. Look for the "s" in https in the website address and/or for the lock symbol. Finally, don't trust people who contact you unsolicited. They probably don't have your best interests at heart.

Don't pay with a gift card, wire transfer, or cryptocurrency. The Kentucky Attorney General's Office reports that in 2021, victims most often paid with a gift card or other reloadable card. Scammers will ask for these forms of payment because they cannot be tracked or reversed. In short, **never send money to get money**. Also, don't deposit a check into your account and then pay it back to someone else. You could lose your money if the check doesn't clear.

We can all help prevent scams **by reporting fraud attempts** to the authorities. Unreported scams will continue to thrive and cost us all. Report suspected scams to the following authorities:

- Kentucky Attorney General at ag.ky.gov/scams or 888-432-9257
- Federal Trade Commission at reportfraud.ftc.gov or 877-FTC-HELP
- Better Business Bureau at bbb.org/scamtracker
- Cybercrime such as online phishing – Internet Crime Complaint Center (IC3) at www.ic3.gov
- Identity Theft – IdentityTheft.gov

Learning to check it out when something sounds "too good to be true" can be a real money saver. Reporting scam suspicions to the authorities could prevent future fraud attempts. These are some of the best ways to keep yourself safe from scams.

Sources and References

- Better Business Bureau. 2021 *BBB Online Purchase Scams Report*. (Retrieved March 15, 2022.) https://bbbfoundation.images.worldnow.com/library/d94746d3-524e-4d00-9ae1-8e6e6d542025.pdf
- Federal Trade Commission's Consumer Sentinel Network. *Data Book 2021 Snapshot*. Data as of Dec. 31, 2021. (Retrieved March 15, 2022, from data published Feb. 22, 2022.) https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic
- Federal Trade Commission's Consumer Sentinel Network. *Top 10 Fraud Categories*. Data as of Dec. 31, 2021. (Retrieved March 15, 2022, from data published Feb. 22, 2022.) https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports
- Kentucky Office of the Attorney General. (2020) *Consumer Alerts*. Retrieved March 2, 2022, from https://ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Comsumer%20Alerts.aspx.