






Top Ten Scams of 2022

Below, you'll find descriptions of some of 2022's most reported scams and ways to keep you, your information, and your loved ones safe.

- 1. "Amazon" Impersonators** | [Scammers](#) call about suspicious activity or unauthorized purchases on your Amazon account. They will ask you to give them access to your computer or phone, so they can browse through your personal information and pretend to "fix" the problem. Per Amazon, while some departments at Amazon will make outbound calls to customers, **Amazon will never ask you to disclose or verify sensitive personal information, or offer you a refund you don't expect.**¹
- 2. Cryptocurrency Payment Scams** | Scammers will [pretend](#) to be a representative from a government agency or law enforcement, or prize promoters. They trap the public via call, text, email, or social media messages, scaring you into "protecting" your money by taking out cash and feeding it into a cryptocurrency ATM. **Only scammers will demand payment in cryptocurrency or guarantee profits.** 
- 3. Government Scams** | Scammers call and [pose](#) as the Internal Revenue Service (IRS), the Social Security Administration (SSA), or Medicare. They say you owe money and need to pay by sending a wire transfer or purchasing pre-paid gift cards. Per guidance issued by the Massachusetts Attorney General's Office, **the U.S. government will not request payments from you over the phone or in the form of a wire transfer, gift card payment, cryptocurrency, payment, cash, or pre-paid cards.**²
- 4. Gift or Donation Scams** | Scammers pose as [a friend](#), [boss](#), or [charity](#) asking for a favor. They ask for irreversible payments, particularly through gift cards or money transfer requests using Venmo, Zelle, and/or CashApp. **Do not send payments until you know if the request is legitimate.** 
- 5. Emergency Fund Scams** | Similarly, scammers will pose as a [distressed](#) friend or family member in need of money. They claim they lost their wallet, were arrested, were in a car accident, or are in the hospital. **Remain calm and hang up the phone.** Call that person or anyone connected to them to identify if the person is safe. Never wire funds, send cash, or purchase prepaid cards until you know if the call is real. 

1. Source: <https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B>

2. Source: <https://www.mass.gov/doc/savvy-senior-booklet-april-2019/download>



Top Ten Scams of 2022

Below, you'll find descriptions of some of 2022's most reported scams and ways to keep you, your information, and your loved ones safe.

6. **Computer Tech Support Scams** | A live person will call and pose as [IT support](#), or you will see a pop-up ad on your computer telling you your device has been infected with a virus. The person or message will convince you to give them control of your computer and/or demand payment at the end of the call. **Never allow anyone who calls you unsolicited remote access to your computer.**



7. **QR Code scams** | [Fake](#) Quick Response (QR) Codes are found on parking meters or contactless payment methods; they are sent in the mail attached to surveys, sweepstakes, or in email, or social media. **Avoid scanning them, especially in emails and paper mail. If the QR Code looks suspicious, don't click on it.**



8. **Lottery and Sweepstakes Scams** | A scammer will call and congratulate you on winning a [lottery](#), sweepstakes, or grand prize. They will then request that you pay taxes or fees on your winnings. **Do not send cash, checks, or wire money to pay taxes or fees to collect a prize or sweepstakes.**

9. **Robocalls for Voice Recordings** | An [automated](#) voice will call and ask, "Can you hear me?" When the recipient says "[Yes](#)," the machine records their voice and hangs up. **Avoid responding when prompted by an unknown robocaller.**

10. **SIM Swapping** | Scammers collect your data through social media, phishing, or other attacks. They then call your phone [provider](#) and impersonate you, tricking your carrier into switching your number to the attacker's SIM card. If you get locked out of your account, lose cell service, or receive account notifications for activity that isn't yours, **contact your cell phone provider immediately.**



This publication contains general information and predictions only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

ABOUT DELOITTE

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms



For questions and additional resources, please contact safecircle@deloitte.com.

Copyright ©2022 Deloitte Development LLC. All rights reserved.