IRS scam: Phony IRS agents reach you by phone, email or text message claiming you owe money. Threatening to take legal action, they urge you to send payment by money order, cashier's check or prepaid debit card immediately -- in some cases, insisting that you complete the transaction while you're still on the phone. How you know it's a scam: A legitimate IRS agent will always first contact you by mail, and the agency accepts checks and credit card payments. The IRS never insists on swift payment by debit card, cashier's check or wire transfer.

Tech support scams: The phone rings, and the caller claims to be a Microsoft or Apple tech support representative who has detected a problem with your computer. He or she urges you to visit a particular site, or type a series of keys into your computer, to give the fake support person the ability to control the machine and "fix" whatever is wrong.

Alternatively, a popup window appears on your screen, warning that your system isn't secure and you must download security software by clicking on a link in the popup immediately. In both cases, the scammer is aiming to download malicious software onto your machine to either steal your data or to hold your machine hostage until you pay some sort of ransom. How you know it's a scam: Real tech support departments don't call you out of the blue nor can they detect problems you haven't reported. And while you do need security software for your computer, you're not going to find it by clicking on a popup ad. Most computers come with security software. All that's necessary to keep yours up to date is to renew your annual subscription.

Grandkid scams: Con artists buy marketing lists, just like big retailers do, looking for vulnerable populations to exploit. The elderly are a particularly ripe target, with those over age 60 accounting for roughly 37 percent of fraud victims.

One common scam exploits grandparents by having a con artist pose as a young relative, who then maintains he's out of town and in trouble. Pleading with the grandparent not to tell anyone, the fake grandchild contends that the only way to get out of this bind is for the grandparent to send money via wire transfer. How you know it's a scam: A quick phone call or text message to your real relative is likely to find him/her at home. Not sure? Tell the caller that you'll have to call back. If the grandchild contends that's not possible, you know you're talking to a crook. These scammers use a sense of urgency to get you to send cash before you can check out the story. Rest assured, even Mexican jails have phones.

Online romance scams: Ever sign up for a dating site? Then you're a prime target for a romance scam, where a distant lover strikes up a conversation and quickly becomes besotted. Claiming that you're the man/woman of his/her dreams, this faux lover will say he/she would love to meet in person but is (a) out of town on business (b) stationed abroad in the military (c) living in another country or (d) hampered by a sick or dying relative. Once the faux beau is convinced that you're hooked, the requests for money start.

Typically, the con artist will contend that some emergency has left him/her desperately short of cash and in need of your help. Sometimes, the con artist pretends the only thing that keeps him/her from showing up on your doorstep is that he/she is short of the money to get there.

Of course, if the victim provides cash, another emergency will require more. The fake romance ends when the victim stops sending money.

How you know it’s a scam: If someone claims to be madly in love you with you, even though you’ve never met, it should raise a red flag. If the person has a litany of excuses of why you can’t meet in person, it’s almost assuredly a con. All you need for a final confirmation is to wait for the request for money.

Outside of romance scams, which are initiated and often pursued completely online, some 77 percent of impostors approach their victims via phone, federal officials say. One way to thwart these attempts is to let unknown callers go to your answering machine. Con artists rarely leave a message.

Additionally, the type of payment you’re asked to provide can also serve as a warning. Government officials said 58 percent of victims said they paid via wire transfer in 2016. Prepaid debit cards are also popular with scammers because these payments are untraceable and impossible to reverse. If you paid a crook by credit card, on the other hand, you can dispute the charge and likely get your money back.