# Common Scams to Know

Adapted from lemmy.one/post/244313

**Package Delivery:** These scams start with a text or email. They often say that the package cannot be delivered to you due to incomplete address information, and a link for you to follow. These messages are almost always scams. If you are expecting a package and get a message like this, log into the mail carrier's website or use tracking information to check the status instead.

**Wrong number/Mandy**: An intentional wrong number text is the entry point to multiple types of scams. Because these are so prevalent, it is recommended that you do not reply to them, even out of courtesy. If you receive a wrong number inquiry that assumes a connection with you and there are no pictures included, then you may be at the beginning of a cryptocurrency scam. If you receive a random text from a woman that is trying to play up a relationship/hook-up angle and includes an alluring photo, you have encountered what is often called the Mandy scam.

**Tech Support:** Tech support scams can start with the scammer contacting you through a random phone call, pop-up on a website, notification, or email. You can also run into tech support scams by Googling a support phone number and seeing an advertisement placed by a scammer meant to look like a legitimate support page. If you're talking to support and they mention anything about gift cards, hang up.

**Refund**: Refund scams usually start with a spam message about a fake transaction. The message will provide you with a phone number to call if you want to cancel the transaction, and if you call the scammers will try to get you to provide credit card or banking information in order to receive your refund. Scammers have been taking advantage of Paypal's invoice system to send out realistic scam emails through Paypal.

**Rental**: Rental scammers usually list apartments at lower than market rate, and will ask for some money up front, or will offer you the keys for money up front. Seeing the apartment in person is a good way to find out if you are being scammed or not.

**Job**: Fake job scams come in many varieties. The scammers usually conduct interviews over Google Hangouts or a similar online service. They will offer high wages for the work being done, and they will "hire" you by telling you that you are hired, rather than going through the normal process. If they mention anything about a check or about receiving and sending out transactions, it is a fake check scam. If they mention anything about receiving, processing, or inspecting packages, it is a parcel mule scam. If they ask you to purchase items up-front, ask you to pay a fee in order to be hired, or ask you to purchase gift cards, it is an advance-fee

scam. If the job involves posting advertisements on Craigslist or eBay, they are using you and your account to scam people. If the job involves Bitcoin ATMs, it's a scam.

**Romance**: Romance scammers pretend to be in love with their victims in order to ask them for money. They sometimes spend months grooming their victims. They tend to be extremely good at taking money from their victims again and again. Romance scam victims are emotionally invested in their relationship with the scammer, and will often ignore evidence they are being scammed.

**Advance-fee**: Whether presented as investment opportunities, money transfers, job offers, or online purchases, the bottom line is always the same: you will pay money up front and receive nothing in return. Sometimes the scammers will simply take your first payment and disappear, but sometimes they will take your initial payment and then make excuses that lead to you making additional payments. Common examples include purchasing fake concert tickets, work from home job offers that require you to buy equipment, or various career opportunities that ask you to put down a deposit for an initial consultation.

**Blackmail**: These claim to have placed software/malware on an adult video site and have a video of you using the site. They threaten to release the video, and they demand that you pay them in order for them to delete the video. This is a very common campaign and there is no truth behind the email or the threats.

**Courier**: Courier fraud usually starts with a phone call from a scammer who may know lots of information about you. Scammers will impersonate bank employees, police, or other government officials. They will say that your account has been linked to fraud or another crime, and will request your assistance. You'll be asked to either withdraw money, or purchase gift cards or expensive items, and you'll be directed to give the money to the scammers in some way, often in a local meetup.

**Crypto**: Victims are told to buy cryptocurrency and then send it to a wallet address where it will be invested. All the money actually goes directly to the scammer.

**Fake check**: You receive a check (online or in real life), deposit it and see the money in your account, and then give money to the scammer (usually through gift cards, Western Union, or cash). Sometimes the scammers will ask you to order things. The bank will eventually take the initial deposit back, and any money you sent will come out of your own personal funds.

**Pin/verification**: You will receive a legitimate authentication text from a company like Google, Craigslist, or Microsoft, and you will also have someone else asking you for the pin. Sometimes the scam starts on Craigslist, and the scammer will ask you to verify that you are a real person. Sometimes you will receive a random authentication text, and the scammer will text you without any previous contact. The goal of the scammer is to access your accounts.