GLOSSARY OF SCAM TYPE DEFINITIONS

Scams reported to BBB Scam Tracker are classified into 30 scam types. These classifications represent common scams seen by BBB over time and are also informed by classifications used by the Federal Trade Commission and the Internet Crime Complaint Center of the FBI. While scams vary widely, nearly 95% of all scams reported to BBB Scam Tracker can be classified into one of these general types.

Scam Types	Definitions
Advance Fee Loan Scams	In this scam, a loan is guaranteed but, once the victim pays upfront charges such as taxes or a "processing fee," the loan never materializes.
Business E-mail Compromise	This financial fraud targets businesses engaged in international commerce. Scammers gain access to company e-mail and trick employees into sending money to a "supplier" or "business partner" overseas.
Charity Scams	Charity scams use deception to get money from individuals who believe they are making donations to legitimate charities. This is particularly common in the wake of a natural disaster or other tragedy.
Counterfeit Products	Counterfeit goods mimic original merchandise, right down to the trademarked logo, but are typically of inferior quality. This can be a life-threatening health or safety hazard when the counterfeit item is medication or an auto part.
Credit Card Scams	This con typically involves impersonation of a bank or other credit card issuer. By verifying account information, con artists try to fool their targets into sharing credit card or banking information.
Credit Repair/ Debt Relief Scams	Scammers posing as legitimate services collect payment in advance with promises of debt relief and repaired credit but provide little or nothing in return.
Debt Collection Scams	In this con, phony debt collectors harass their targets, trying to get them to pay debts they don't owe.
Employment Scams	Victims of employment scams are led to believe they are applying or have just been hired for a promising new career while they have, in fact, given personal information or money to scammers for "training" or "equipment." In another variation, the victim may be "overpaid" with a fake check and asked to wire back the difference.
Fake Checks and Money Orders	In this con, the victim deposits a phony check and then returns a portion by wire transfer to the scammer. The stories vary, but the victim is often told they are refunding an "accidental" overpayment. Scammers count on the fact that banks make funds available within days of a deposit, but can take weeks to detect a fake check.
Fake Invoice Scams	This scam targets businesses. Scammers attempt to fool employees into paying for products that the business did not order and that may not even exist. Fake invoices are often for office supplies, website or domain hosting services and directory listings.
Family/Friend Emergency Scams	This scheme involves the impersonation of a friend or family member in a fabricated urgent or dire situation. The "loved one" invariably pleads for money to be sent immediately. Aided by personal details provided on social media, imposters can offer very plausible stories to convince their targets.
Government Grant Scams	In this con, individuals are enticed by promises of free, guaranteed government grants. The only catch is a "processing fee." Other fees follow, but the promised grant never materializes.
Health Care, Medicaid and Medicare Scams	These schemes run the gamut, with many attempting to defraud private or government health care programs. The con artist is often after the insured's health insurance, Medicaid or Medicare information to submit fraudulent medical charges or for purposes of identity theft.
Home Improvement Scams	In this con, door-to-door solicitors offer quick, low-cost repairs and then either take payments without returning, do shoddy work or "find" issues that dramatically raise the price.
Identity Theft	Identity thieves use personal information (e.g., Social Security numbers, bank account information and credit card numbers) to pose as another individual. This may include opening a credit account, draining an existing account, filing tax returns or obtaining medical coverage.
Investment Scams	These scams take many forms, but all prey on the desire to make money without much risk or initial funding. "Investors" are lured with false information and promises of large returns with little or no risk.
Moving Scams	These schemes involve rogue moving services offering discounted pricing to move household items. They may steal the items or hold them hostage, demanding additional funds to deliver them to the new location.
Foreign Money Exchange Scams	In this scam, the target receives an e-mail from a government official, member of royalty, or a business owner offering a huge sum for help getting money out of their country. The victim fronts costs for the transfer believing that they will be repaid.

Scam Types	Definitions
Online Purchase Scams	These cons involve purchases and sales, often on eBay, Craigslist, Kijiji or other direct seller-to-buyer sites. Scammers may pretend to purchase an item only to send a bogus check and ask for a refund of the "accidental" overpayment. In other cases, the scammer will simply never deliver the goods.
Phishing	Communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information or passwords.
Rental Scams	Phony ads for rental properties ask for advanced payments. Victims later discover the property doesn't exist or is owned by someone else.
Romance Scams	An individual believing they are in a romantic relationship is tricked into sending money, personal and financial information or items of value to the perpetrator.
Scholarship Scams	This con hooks victims, often students struggling with tuition costs, with the promise of government scholarship money, but upfront "fees" never actually materialize into those much needed funds. Sometimes a fake check does arrive, and the student is asked to wire back a portion for taxes or other charges.
Malware	Any kind of computer bug with malicious intent. One type of malware, called "spyware," is designed to steal personal information. "Adware" displays unwanted ads. "Ransomware" can hold data on a device hostage until the scammer is paid to unlock it.
Sweepstakes, Lottery and Prize Scams	This con fools victims into thinking they have won a prize or lottery jackpot, but need to pay upfront fees to receive the winnings, which never materialize. Sometimes this con involves a fake check and a request to return a portion of the funds to cover fees.
Tax Collection Scams	In this con, imposters posing as an Internal Revenue Service representative in the United States or as the Canada Revenue Agency in Canada attempt to coerce the target into either paying up or sharing personal information. Threats of immediate arrest and other scare tactics are common.
Tech Support Scams	Tech support scams start with a call or pop-up warning alerting the target to a computer bug or other problem. Scammers pose as tech support employees of well-known computer companies and hassle victims into paying for "support." If the victim allows remote access, malware may be installed.
Travel and Vacation Scams	Con artists post listings for properties that either are not for rent, do not exist, or are significantly different than pictured. In another variation, scammers claim to specialize in timeshare resales and promise they have buyers ready to purchase.
Utility Scams	In this con, scammers impersonate water, electric and gas company representatives to take money or personal information. They frequently threaten residents and business owners with deactivation of service unless they pay immediately. In another form, a "representative" may come to the door to perform "repairs" or an "energy audit" with the intent of stealing valuables.
Yellow Pages/Directory Scams	This con targets businesses, attempting to fool them into paying for a listing or ad space in a non-existent directory or "Yellow Pages." In some cases, the directory will technically exist, but will not be widely distributed and a listing will be of little or no value—these directories are essentially props in the scammer's ploy.