



BBB 2025 Scam Categories Explained

Online Purchase

These cons involve purchases conducted via e-commerce websites. Consumers may click on a social media ad or find an appealing website which offers a variety of merchandise. Victims report being charged immediately after the purchase, but in many cases the ordered items are never delivered, or occasionally, what arrives is of inferior quality or damaged, with little chance of a refund.

Employment

Victims of employment scams are led to believe they are applying or have just been hired for a promising new remote-based career while they have, in fact, given personal information, including bank account or credit card information, to scammers for “training” or “equipment.”

Phishing

This scam involves communication impersonating a trustworthy entity, such as a bank, insurance or mortgage company, intended to mislead the recipient into providing personal information or passwords.

Sweepstakes/Lottery/Prizes

This type of scam begins with contact with a consumer informing them that they are a prize or contest winner. The catch is that in order to collect the “prize”, the consumer must pay a fee. Occasionally these scammers will send a fake check to the consumer for “taxes” but then ask the consumer to send a portion of the check money back to them using a gift card or money transfer. These scams can often impersonate well-known legitimate companies who offer prizes.

Government Agency Imposter

This type of scam involves the impersonation a government agency (such as the U.S. Postal Service, U.S. Customs & Border Protection, or Social Security Administration). The scammer may attempt to trick the consumer into giving away personally-identifiable information, purchase counterfeit products or pay bogus fees.

Advance Fee Loan

This scam involves the solicitation of a consumer seeking a loan, either via email, text or a slick-looking website. The lender promises a speedy application process and immediate funding, but before the money is released, the scammer requests an upfront fee, sometimes portrayed as “collateral” or “insurance” payments. Some consumers who have paid these advance fees report that the scammer then demands another round of payments before the loan can be processed, but in these cases, no loan money is ever delivered.

Travel/Vacation/Timeshare

Many of these schemes involve phony online travel agency websites and spoofing or posing as an airline reservation representative who charges high fees to change or cancel an existing travel reservation. Others can include solicitations for sale of timeshare properties from non-existent buyers, which come with a steep host of “fees” and “taxes” levied to the seller.

Investment

This scam frequently originates from social media - sometimes via a hacked account. The approach to invest by an “advisor” can also arrive via unsolicited messages using mobile software such as WhatsApp. The investment platforms will vary; it could be stock trading, Forex (foreign exchange), or cryptocurrency. The consumer often believes the investments have increased in value and may add more money to the platform. Eventually, when the consumer attempts to withdraw the capital, the platform and/or advisor disappears or blocks them, or they are caught in a never-ending loop of fees, commissions, and taxes in which they never see their money again.

Debt Collections

In these kinds of schemes, phony debt collectors contact their targets to try to get them to pay debts they don’t owe or have already discharged. In some cases, the scammers can use harassing or intimidating tactics, such as threats of legal action, in an attempt to persuade the consumers to make payments.