2021 BBB Scam Tracker™ RISK REPORT

Highlights

TOP 5 RISKIEST SCAMS REPORTED BY CONSUMERS

1. **ONLINE PURCHASE**
   Scammers use technology to offer attractive deals, but once the payment is made, no product or service is delivered. In some cases, fraudsters send low-quality or counterfeit products.

2. **CRYPTOCURRENCY**
   Investors are scammed into paying money or trading their own digital assets, known as cryptocurrencies, even though the scammer has no intention of building a company. These scams also involve scenarios in which investors store cryptocurrencies with fraudulent exchanges.

3. **EMPLOYMENT**
   Job applicants are led to believe they are applying for or have just been hired for a promising new job when instead they have given personal information via a fake application 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.

4. **HOME IMPROVEMENT**
   Door-to-door solicitors offer quick, low-cost repairs and then either take payment without returning, do shoddy work, or “find” issues that dramatically raise the price. These types of schemes often occur after a major storm or natural disaster.

5. **INVESTMENT**
   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.

More than one third (37.4%) of all scams reported in 2021 were online purchase scams.

59.8% reported shopping online more this year as the pandemic continued.

46.4% reported spending more time browsing online and/or social media.

Almost 3 out of every 4 (74.9%) of those targeted by online purchase scams reported losing money.

Online scams were more likely to result in a reported monetary loss than those perpetrated in person or via phone.

BBBMarketplaceTrust.org/RiskReport
10 General Tips for AVOIDING A SCAM

1. Never send money to someone you have never met face-to-face.

2. Don’t click on links or open attachments in unsolicited email or text messages.

3. Don’t believe everything you see or read. Scammers are great at mimicking official seals, fonts, and other details. Just because a website or email looks official does not mean it is. Even Caller ID can be faked.

4. Take precautions when making online purchases.
   - Don’t shop on price alone. Scammers offer hard-to-find products at great prices.
   - Don’t buy online unless the transaction is secure. Make sure the website has “https” in the URL (the extra s is for “secure”) and a small lock icon on the address bar. Even then, the site could be shady. Research the company first at BBB.org.
   - Avoid making quick purchases while browsing social media. Scammers advertise websites that offer great deals, but either don’t deliver the product at all or deliver counterfeit products.
   - Do more research on those products you found via online search.

5. Be extremely cautious when dealing with anyone you’ve met online.

6. Never share personally identifiable information with someone who has contacted you unsolicited.

7. Don’t be pressured to act immediately.

8. Use secure, traceable transactions when making payments for goods, services, taxes, and debts.

9. Whenever possible, work with businesses that have proper identification, licensing, and insurance.

10. Be cautious about what you share on social media.

Learn more at BBB.org/AvoidScams