# Identity theft protection: How to spot a scam.



When identity thieves scam you, the outcome can be more than frustrating. It can lead to situations that are both financially and emotionally tolling. The Security Awareness Company shares, “While many cyberattacks are financially motivated, data theft is also a common goal. Confidential information such as full names, addresses, national ID numbers, and other personal details carry a lot of value.”

Because identity thieves adapt their methods almost daily, consumers must stay especially alert and take measures to protect themselves and their information immediately. Be aware of possible scams if:

1. **You’re contacted out of the blue.** Many identity theft scams start with unexpected contact, whether it’s by mail, phone, email, text, or social media. If you receive unexpected contact from an organization or person you don’t know, always assume the possibility of a scam. A sneaky tactic scammers use is catching people when they are busy or tired, making them more likely to arrive at quick decisions without much thought. If a call seems unexpected, unwarranted, or comes at an odd hour, keep your guard up high.

2. **You’re asked to provide personal or financial information.** Banks, companies, and government agencies rarely ask customers to provide a list of personal information over the phone. If the individual who contacted you starts asking for information like your passwords, bank information, Social Security number, etc., end the conversation immediately. If your curiosity is piqued, use your web browser to look up the organization’s contact information on its website. Just be sure you don’t click on any suspicious links. Then, directly contact the organization to review

what happened and tell them the information you were asked to give to confirm the legitimacy of the call.

3. **Threats or fear tactics are used.** Identity thieves and scammers may use fear or threats like losing your job, losing your house, or going to jail to scare people into handing over so-called required payments or personal information. Don't fall for this fear-based approach before doing more research.

4. **You notice spelling or grammar mistakes.** Multiple spelling or grammatical errors in an offer, document, or mail piece should put you on guard for a scam. Similarly, a company with minimal branding, no address listed, or a random email address may not be a legitimate company at all. Check all facets of the communication and don't respond if any pieces appear suspicious.

5. **You're encouraged to act quickly.** Psychology is often used to bait individuals into scams. Phrases like, "Only the first 100 people will qualify," or "This offer won't be available once you hang up," coerce people into acting in haste and jumping into otherwise questionable situations. The Security Awareness Company shares, "Any scenario that triggers emotions should also trigger your suspicions. Scammers leverage emotions by using threatening language, pushing a sense of urgency, and offering unrealistic promises."

6. **You've been asked for money in an unusual way.** Were you asked to purchase gift cards or send money through transfer apps or wire services? These are all red flags and should make you pause and investigate before proceeding.

7. **Something sounds too good to be true.** If an offer sounds too good to be true, it likely is. Trust your gut and follow your instincts. When in doubt, ask for a callback number. That way, you can hang up and tell someone else about the conversation to get a second opinion.

8. **It's a scam you've heard of or seen before.** Taking a proactive approach can save you from falling for a scam. How can you do that? By following safety sites, doing your own research, and listening. Local and national sites such as the Federal Trade Commission offer email lists and resources to keep you in the loop about common scams. Because scams can have trends, too, being alert to the current tactics can keep you from falling for them. The more you know about scams and how they operate, the safer you are.

Now that you know how to better spot a scam, you can reduce your risk of fraud. For even more peace of mind, talk to a local, independent agent about supplemental identity theft protection services offered by insurance companies.