“Scam Awareness Guide”

Lumoset Foundation, Inc.

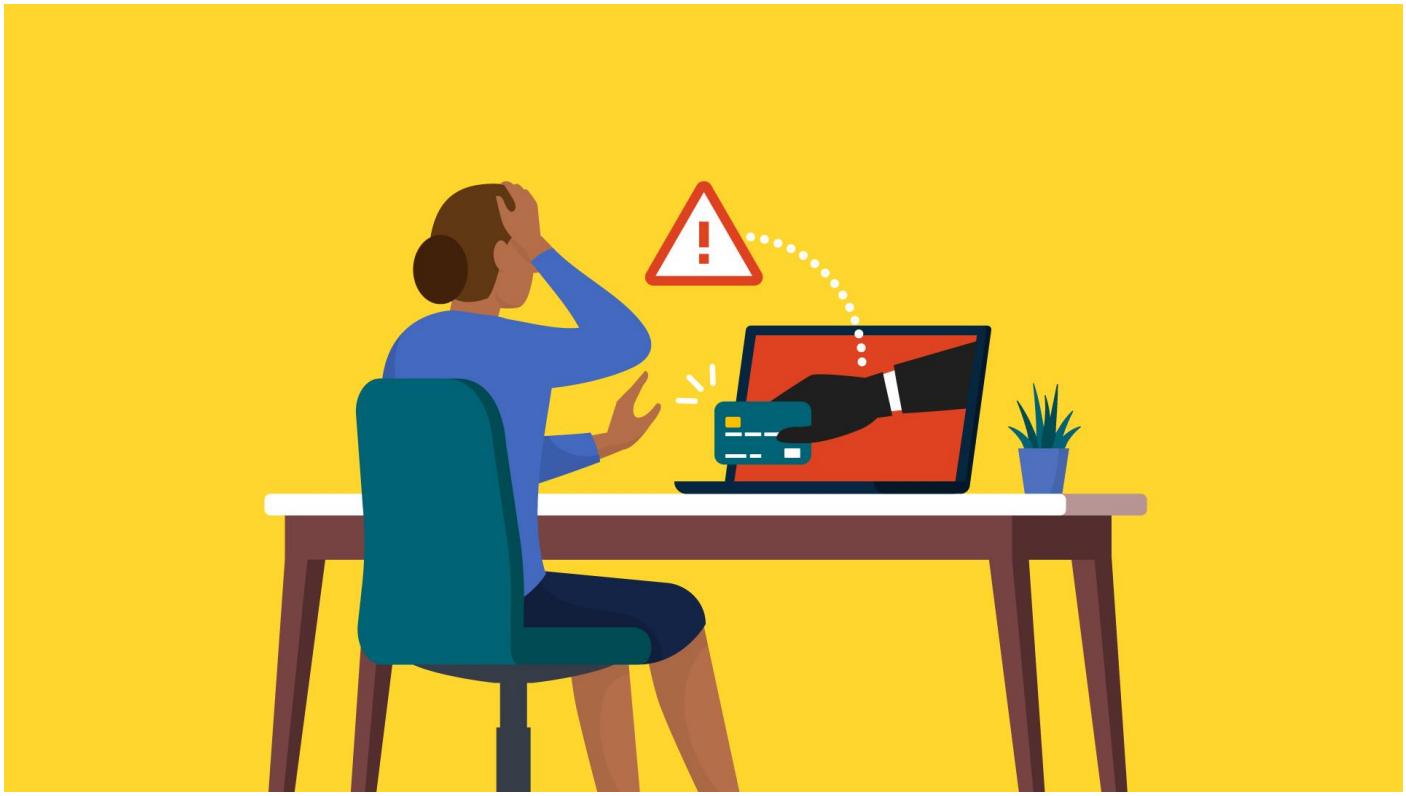
How to Protect Yourself from Online Scams

A Free Resource by Lumoset

- Version 1.0 | Published: 05, 2025.
- Author: Lumoset Digital Safety Team W
- Website: https://lumoset.org/

Table of Contents

1. Introduction: Why Scam Awareness Matters



Online scams are more common than ever in 2025, costing individuals and businesses billions of dollars every year. Scammers use psychological tricks to pressure victims into giving away money or personal information.
This guide will help you:

- Identify common scam tactics used online and over the phone.
- Learn practical steps to avoid scams.
- Know what to do if you or a loved one is targeted.

This isn't just about protecting yourself—it's about protecting your friends, family, and community from becoming victims.

2. Common Online Scams and How They Work

Scammers use different strategies to trick people. Here are some of the most widespread scams in 2025:

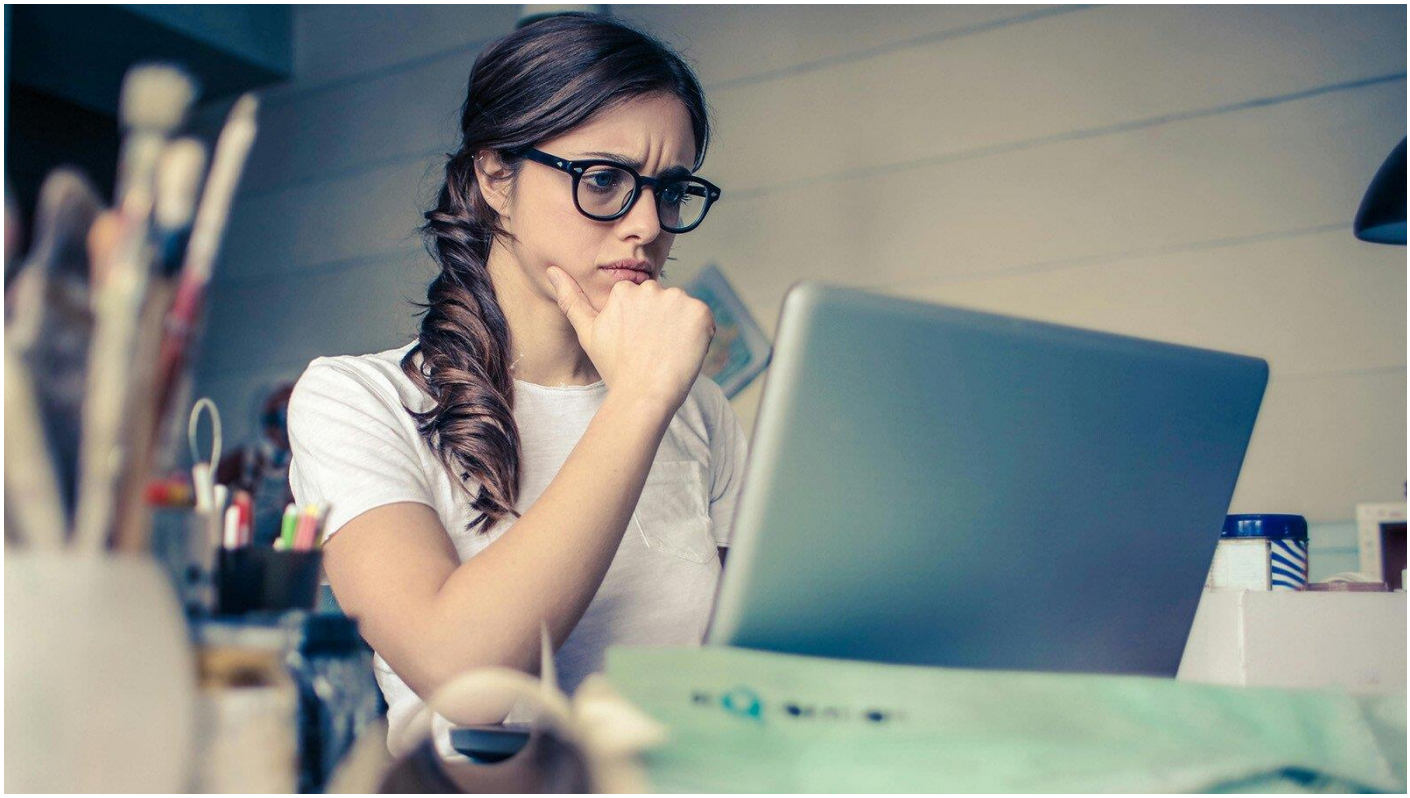
- **Phishing Scams:** Fake emails or texts pretending to be from legitimate organizations like Amazon, PayPal, your bank, or even government agencies, asking you to click a link and "verify" your account or update your information.

These links often lead to fake websites designed to steal your login credentials or personal data.

- **Job Offer Scams:** Scammers post fake job listings on job boards or social media, or contact people directly with “work-from-home” offers that seem too good to be true. These scams often require an upfront payment for training materials or equipment, or may ask for personal information that can be used for identity theft.
- **Tech Support Scams:** These scams typically involve a caller or a pop-up message claiming that your computer has a virus or a critical error. They use scare tactics to pressure you into paying for fake tech support services, often gaining remote access to your computer to install malware or steal your data.
- **Investment & Crypto Scams:** These scams lure victims with promises of high returns and low risks, often using fake testimonials and high-pressure sales tactics. They may involve Ponzi schemes, pump-and-dump schemes, or fake cryptocurrency offerings. Victims are often persuaded to invest large sums of money, which the scammers then disappear with.
- **Romance Scams:** Scammers create fake profiles on dating sites or social media to build online relationships with their victims. They often use emotional manipulation and fabricated stories to gain trust, then ask for money for emergencies, travel expenses, or other false pretenses.
- **Lottery/Sweepstakes Scams:** Victims receive fake notifications claiming they have won a lottery or sweepstakes. To claim their prize, they are asked to pay fees, taxes, or processing charges. The scammers then disappear with the money, and the victim never receives the promised prize.
- **Charity Scams:** Scammers exploit people's generosity by setting up fake charities, often after natural disasters or emergencies. They solicit donations using emotional appeals and fabricated stories, but the money never reaches the intended recipients.

Understanding these scams is the first step to protecting yourself.

2. 5 Ways to Spot an Online Scam



If something feels off, trust your instincts. Here are five major red flags to look for:

1. **Unusual Payment Requests**

Scammers often ask for payment using unconventional methods like gift cards, wire transfers, or cryptocurrency, as these transactions are difficult to trace or reverse.

- **Example:** A scammer posing as the IRS might claim you owe back taxes and demand immediate payment in Bitcoin.
- **What to Do:** Legitimate businesses and government agencies rarely ask for payment in gift cards or cryptocurrency. If you're unsure, contact the organization directly using their official website or phone number to verify the payment request.

2. **Too-Good-To-Be-True Offers**

If an offer seems too good to be true, it probably is. Scammers often lure victims with promises of easy money, high returns, or incredible deals.

- **Example:** "Congratulations! You've won $100,000! Just send us a $500 processing fee to claim your prize."
- **What to Do:** Be wary of any offer that seems unrealistic or promises something for nothing. Do your research and verify the legitimacy of the offer before committing to anything.

3. Fake Urgency & Fear Tactics

Scammers often create a sense of urgency or fear to pressure you into acting quickly without thinking. They may threaten negative consequences if you don't comply with their demands.

- **Example:** "Your account will be shut down in 24 hours unless you click this link and verify your information now!"
- **What to Do:** Don't panic. Legitimate organizations will give you reasonable time to respond and verify requests. If you're feeling pressured, take a step back and assess the situation before taking any action.

4. Unverified Links & Attachments

Phishing scams often rely on fake links or attachments to steal your personal information or install malware on your device.

- **Example:** A fake email from "Amazon" might ask you to update your payment information by clicking on a link that leads to a fake website designed to capture your data.
- **What to Do:** Never click on links or open attachments from unknown or unverified senders. Hover your mouse over links to see the actual destination URL before clicking. If you're unsure, contact the organization directly to verify the legitimacy of the email.

5. Poor Grammar & Unprofessional Emails

Many scam emails and messages contain awkward grammar, typos, and generic greetings, indicating that they may not be from a legitimate source.

- **Example:** "Dear customer, you is win gift card. Click link fast!"
- **What to Do:** Be wary of emails that are poorly written or unprofessional. Legitimate companies typically use proper grammar and branding in their communications.

6. What to Do If You Think You're Being Scammed

If you're suspicious about an email, call, or message, follow these steps:

- Do not click links or open attachments.
- Verify with the company directly—look up their official website and contact info.
- Ignore high-pressure tactics—scammers want you to act fast so you don't think.

- Check for online scam reports—search the scam description to see if others have reported it.

If you feel uncertain, assume it's a scam until proven otherwise.

7. What to Do If You've Already Been Scammed

If you sent money or gave personal information to a scammer, take these steps immediately:

- Contact your bank or credit card company – Ask if they can reverse the transaction.
- Change your passwords – If you clicked a suspicious link, reset your passwords immediately.
- Report the scam – Many governments and organizations track scam activity to help others avoid falling victim. (See Section 6 for reporting links.)

Taking action quickly can reduce the damage and prevent further harm.

8. Official Reporting & Trusted Resources

- Report Scams to Authorities:
  - USA: FTC Report a Scam
  - Global: Scamwatch

- Verify Before Acting:
  - Check if a Website is Legit
  - Online Job Scam Check

- Stay Updated on Scams:
  - Sign up for scam alerts from consumer protection agencies.

9. Bonus: Scam Spotting Checklist

☑ **Use this quick checklist to determine if something might be a scam:**

- ✓ Are they demanding gift cards, wire transfers, or cryptocurrency?
- ✓ Is the offer too good to be true?
- ✓ Are they using pressure or scare tactics to rush you?
- ✓ Are there grammar mistakes or generic greetings in the message?
- ✓ Does the link or sender's email look suspicious?

If you check “yes” to any of these, don’t engage—report and delete the message!

10. Real-Life Scam Stories

These stories are based on real cases, but names and identifying details have been changed to protect the victims' privacy.

Story 1: The Fake Lottery Win

An elderly woman received a phone call congratulating her on winning a large lottery prize. The caller, claiming to be from the lottery commission, informed her that she needed to pay a processing fee and taxes upfront to claim her winnings. Excited about the unexpected windfall, the woman followed the instructions and wired the money. However, she never received the promised prize, and her calls to the supposed lottery

commission went unanswered. She lost thousands of dollars and was left feeling devastated and betrayed.

Story 2: The Romance Scam

A recently widowed man connected with a woman on a dating website. They exchanged messages and phone calls for several weeks, and the woman expressed strong feelings for him. She claimed to be living overseas and facing a financial emergency. The man, feeling sympathetic and wanting to help, sent her several thousand dollars. However, after sending the money, the woman disappeared, and he realized he had been scammed. He was left heartbroken and financially drained.

Download & Share This Guide

- **Found this helpful? Send it to someone who needs to see it! Copy this link & share with your family, friends, or coworkers: [Insert Website URL Here]**
- **Want more tips? Visit our website for updated scam alerts & digital safety resources.**
- **Stay safe and stay informed!**