

# Amazon Purchase Scam Prevention Checklist

## When You Receive a Suspicious Call

- ☐ Stay calm and don't provide any information immediately
- ☐ Ask for specific details they should already know (last 4 digits of card, account email)
- ☐ Tell them you'll call Amazon directly to verify the issue
- ☐ Hang up if they pressure you or refuse to wait for verification
- ☐ Check your actual Amazon account by logging in through the official website or app
- ☐ Look for any real notifications or unauthorized purchases in your account

## Red Flags That Indicate a Scam Call

- ☐ The call came out of the blue (Amazon doesn't typically call customers)
- ☐ They create artificial urgency ("act now or your account will be charged")
- ☐ They ask for personal information Amazon already has
- ☐ They request your password, PIN, or Social Security number
- ☐ They want remote access to your computer
- ☐ They pressure you to stay on the line

## When You Receive a Suspicious Email

- ☐ Check if the sender's email ends in @amazon.com (not variations like @gmail.com)
- ☐ Verify the email addresses you by name, not "Dear Customer"
- ☐ Look for poor grammar, spelling errors, or awkward phrasing
- ☐ Don't click any links in the suspicious email
- ☐ Go directly to Amazon.com to check your account instead
- ☐ Forward suspicious emails to [stop-spoofing@amazon.com](mailto:stop-spoofing@amazon.com)

## When You Receive a Suspicious Text Message

- ☐ Check if the message comes from an official Amazon number
- ☐ Look for generic greetings instead of your actual name
- ☐ Don't click any links in the text message
- ☐ Go directly to your Amazon account to verify any claims
- ☐ Delete the suspicious text after reporting it

Visit [www.CyberSmartSeniors.com](http://www.CyberSmartSeniors.com) to access premium guides, personalized checklists, and expert podcasts for less than the cost of a cup of coffee each month!

## Information You Should NEVER Share

- ☐ Account passwords or PINs
- ☐ Credit card numbers or banking information
- ☐ Social Security number
- ☐ Driver's license number
- ☐ Mother's maiden name or security question answers
- ☐ Remote access to your computer or devices

## Verification Steps When in Doubt

- ☐ Hang up and call Amazon customer service directly at 1-888-280-4331
- ☐ Log into your Amazon account through the official website
- ☐ Check your order history for any unauthorized purchases
- ☐ Review your payment methods for any changes
- ☐ Look for any official notifications in your account messages
- ☐ Contact your bank if you suspect any financial compromise

## If You Think You've Been Scammed

- ☐ Change your Amazon password immediately
- ☐ Check all your financial accounts for unauthorized activity
- ☐ Contact your bank and credit card companies
- ☐ Place a fraud alert on your credit reports
- ☐ Report the scam to Amazon at [stop-spoofing@amazon.com](mailto:stop-spoofing@amazon.com)
- ☐ File a report with the Federal Trade Commission at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
- ☐ Document all details of the scam attempt (time, phone number, what they said)

## Protecting Your Family and Friends

- ☐ Share this checklist with family members and friends
- ☐ Establish a family code word for verifying suspicious calls
- ☐ Discuss common scam tactics with your loved ones
- ☐ Show them how to verify Amazon communications independently
- ☐ Encourage them to ask for help when they're unsure about any contact

## Seasonal Shopping Safety (Back-to-School & Holidays)

- ☐ Be extra vigilant during busy shopping periods
- ☐ Keep track of your actual Amazon purchases

Visit [www.CyberSmartSeniors.com](https://www.CyberSmartSeniors.com) to access premium guides, personalized checklists, and expert podcasts for less than the cost of a cup of coffee each month!

- ☐ Set up account notifications for real purchase confirmations
- ☐ Review your account regularly during heavy shopping seasons
- ☐ Be aware that scam attempts increase during peak shopping times

## Monthly Security Maintenance

- ☐ Review your Amazon account activity monthly
- ☐ Check your payment methods for any unauthorized changes
- ☐ Update your passwords regularly
- ☐ Review your account security settings
- ☐ Remove any old or unused payment methods
- ☐ Verify your contact information is current

## Emergency Contact Information

**Amazon Customer Service:** 1-888-280-4331

**Report Amazon Scams:** [stop-spoofing@amazon.com](mailto:stop-spoofing@amazon.com)

**Federal Trade Commission:** ReportFraud.ftc.gov

**Identity Theft:** IdentityTheft.gov

---

**Remember:** When in doubt, hang up and verify independently. Legitimate companies will never pressure you to act immediately without giving you time to verify their identity through official channels.

Visit [www.CyberSmartSeniors.com](http://www.CyberSmartSeniors.com) to access premium guides, personalized checklists, and expert podcasts for less than the cost of a cup of coffee each month!

**Cyber Smart Seniors**   
Digital Guidance for Today's Seniors