Subscription Renewal Scams: Your Safety Checklist

Use this checklist whenever you receive a subscription renewal notice to verify it's legitimate and protect yourself from scams.

When You Receive a Renewal Notice

First Response (Don't React Immediately)

- ☐ Take a deep breath—you have time to verify
- ☐ Resist the urge to click any links in the email
- ☐ Don't call any phone numbers listed in the email or text
- ☐ Close the suspicious message without taking action

Check the Sender's Information

- ☐ Hover over the sender's name to see the full email address
- ☐ Verify the email ends with the official company domain (@amazon.com, @norton.com, @mcafee.com, etc.)
- ☐ Look for misspellings or extra words in the email address
- ☐ Check if the greeting uses your actual name (not "Dear Customer")

Analyze the Message Content

- ☐ Look for urgent or threatening language ("immediate action required," "account suspended")
- ☐ Check for grammar mistakes or awkward phrasing
- ☐ Verify the renewal amount matches what you normally pay
- ☐ Notice if the message creates panic or extreme urgency

Verify Through Official Channels

- ☐ Open a new browser window
- ☐ Type the company's official website address manually (don't use links from the email)
- ☐ Log into your account using your regular credentials
- ☐ Check your subscription status on the official website
- ☐ Look for your actual renewal date and payment amount
- ☐ Compare the official information with the suspicious notice

Cyber Smart Seniors
Digital Guidance for Today's Seniors

If Still Unsure

- ☐ Find the company's customer service number on their official website
- ☐ Call the number from the website (not from the suspicious message)
- ☐ Ask to verify if they sent you a renewal notice
- ☐ Take notes during the conversation

If You Think You've Been Scammed

Immediate Actions (First Hour)

- ☐ Contact your bank or credit card company immediately
- ☐ Request to freeze or cancel the compromised card
- ☐ Report the fraudulent charge or potential fraud
- ☐ Ask about fraud monitoring services

Secure Your Accounts (First Day)

- ☐ Change the password for the affected service
- ☐ Change passwords for any accounts using the same password
- ☐ Enable two-factor authentication where available
- ☐ Run a full security scan using legitimate antivirus software

Report and Document (First Week)

- ☐ File a report at ReportFraud.ftc.gov
- ☐ Report the scam to the real company whose name was used
- ☐ Document all communications (save emails, note phone calls)
- ☐ Keep records of any financial losses

Ongoing Monitoring (Next 3-6 Months)

- ☐ Review all credit card and bank statements weekly
- ☐ Watch for unauthorized charges or suspicious activity
- ☐ Check your credit report for unusual activity
- ☐ Consider placing a fraud alert on your credit file

Build Your Scam-Proof System

Organize Your Subscriptions

- ☐ Create a list of all current subscriptions
- ☐ Note the renewal date for each subscription
- ☐ Record the cost of each subscription
- ☐ List the official website for each service
- ☐ Update this list when you add or cancel subscriptions

Strengthen Your Account Security

- ☐ Enable two-factor authentication on Amazon
- ☐ Enable two-factor authentication on Microsoft accounts
- ☐ Enable two-factor authentication on antivirus software
- ☐ Use strong, unique passwords for each service
- ☐ Consider using a password manager

Establish Good Habits

- ☐ Review credit card statements monthly
- ☐ Set up account alerts for charges over a certain amount
- ☐ Never click links in unexpected renewal emails
- ☐ Always go directly to company websites to verify notices
- ☐ Share scam awareness tips with friends and family

Quick Reference: Red Flags Checklist

A renewal notice might be a scam if it has:

- ☐ A sender email that doesn't match the official company domain
- ☐ Urgent or threatening language
- ☐ Poor grammar or spelling mistakes
- ☐ A payment amount that doesn't match your usual cost
- ☐ A generic greeting instead of your name
- ☐ Pressure to act immediately
- ☐ Links or phone numbers you're urged to use right away
- ☐ Requests for unusual information (Social Security number, passwords)

Emergency Contacts to Keep Handy

Write down these important numbers and keep them accessible:

- ☐ Your bank's fraud department: ____________________________
- ☐ Your credit card company's fraud line: ____________________________
- ☐ Amazon customer service: 1-888-280-4331
- ☐ Norton support: 1-855-815-2726
- ☐ McAfee support: 1-866-622-3911
- ☐ Microsoft support: 1-800-642-7676
- ☐ Federal Trade Commission: ReportFraud.ftc.gov

Remember: When in doubt, go directly to the source. Taking five minutes to verify a renewal notice can save you from hours of stress and potential financial loss. You've got this!