Identifying Whether an Email, Phone Call, Text Message, or Webpage is from Amazon

Here are some tips to determine if an email, phone call, text message, or webpage is authentic.

If you received correspondence regarding an order you didn't place, it likely wasn't from Amazon.com.

Go to **Your Orders** to review your order history.
To report suspicious communication, go to
Report a phishing Email/Call/SMS/Text Messages

If you received suspicious communication pretending to be from Amazon and you don't have an account with us, report it to us at **stop-spoofing@amazon.com**.

Don't share any personal information and report it immediately.

Visit **Report Something Suspicious** for more information.

Additional Information About Emails, Text Messages, and Webpages

Don't open any attachments or click any links from suspicious emails or text messages. If you've already opened an attachment or clicked a suspicious link, go to **Protect Your System**.To increase the security of your account, we recommend enabling Two-Step Verification. For more information, see **Enable Two-Step Verification**.

Suspicious or fraudulent emails, text messages, or webpages not from Amazon.com may contain:

- Links to websites that look like Amazon.com, but aren't Amazon.
  Note: Legitimate Amazon websites have a dot before "amazon.com" such as http://"something".amazon.com. For example, Amazon Pay website is https://pay.amazon.com/. We'll never send emails with links to an IP address (string of numbers), such as http://123.456.789.123/amazon.com/. If the link takes you to a site that is not a legitimate amazon domain, then it is likely phishing.
- An order confirmation for an item you didn't purchase or an attachment to an order confirmation.
  Note: Go to **Your Orders** to see if there is an order that matches the details in the correspondence. If it doesn't match an order in Your Account, the message isn't from Amazon.
- Requests to update payment information that are not linked to an Amazon order you placed or an Amazon service you subscribed to.

Note: Go to **Your Orders**. If you aren't prompted to update your payment method on that screen, the message isn't from Amazon.
- Attachments or prompts to install software on your device.
- Typos or grammatical errors.
- Forged email addresses to make it look like the email is coming from Amazon.com.
- When you receive an email from an @amazon.com sender and it contains the Amazon smile logo beside the email, the message is really from us. Visit **BIMI website** to find out which email providers have enabled our brand logo to be displayed.

Important: Phone Calls

While some departments at Amazon will make outbound calls to customers, Amazon will never ask you to disclose or verify sensitive personal information, or offer you a refund you do not expect.

We recommend that you report any suspicious or fraudulent correspondence. Visit **Report Something Suspicious** for more information.

Avoiding Payment Scams

Protect yourself from fraud on the internet by identifying and avoiding internet scams and phishing attempts.

When in doubt, ask the intended recipient for more information about the purpose and safety of the requested payment. Don't send the payment until you're comfortable with the transaction.

To avoid payment scams:

- Don't do business with a seller who directs you off the Amazon website. A legitimate Amazon seller transaction will never occur off the Amazon website.
- Don't send money (by cash, wire transfer, Western Union, PayPal, MoneyGram, or other means, including by Amazon Payments) to a seller who claims that Amazon or Amazon Payments will guarantee the transaction, refund your funds if you're not satisfied with the purchase, or hold your funds in escrow.
- Don't make a payment to claim lottery or prize winnings, or on a promise of receiving a large amount of money.
- Don't make a payment because you're guaranteed a credit card or loan.
- Don't respond to an internet or phone offer that you're not sure is honest.
- Don't make a payment to someone you don't know or whose identity you can't verify.
- Don't respond to emails that ask you to provide account information, such as your email address and password combination. Amazon will never ask you for personal information.