How do I know if a call was from Amazon?

If you receive a suspicious phone call claiming to be from Amazon, here are some things you can look out for:

- Amazon will never ask for payment or offer you a refund you do not expect.
- Amazon will never ask you to make a payment outside of our website (e.g. via bank transfer, e-mailing credit card details, sharing gift card details over the phone, etc.)
- Amazon will never ask you for remote access to your device e.g. by asking you to install an app.

Please do not share any personal information, and disconnect the call immediately.

How do I know if an SMS was from Amazon?

Smishing scams are becoming increasingly advanced: Scam messages can be inserted into a thread of legitimate messages that you might have received from Amazon. If you receive a suspicious SMS claiming to be from amazon (sometimes called Smishing), here are some things you can look out for:

- Scam texts will often say there is a problem with your account, ask you for sensitive information like passwords, or state that you are owed a refund. Amazon will never ask for your password or personal information by text Message.
- Amazon will never ask for your personal information, or ask you to make a payment outside of our website (e.g. via bank transfer, e-mailing credit card details, etc.) and will never ask for remote access to your device e.g. by asking you to install an app.

How do I know if an e-mail is from Amazon?

Spoof or phishing emails are fraudulent emails attempting to get your personal information. They are generally made to look like they are coming from Amazon. If you receive an e-mail claiming to be from Amazon, and you suspect it is a spoof or phishing e-mail, here are some things you can look out for:

- Amazon e-mails will always come from an address that ends @amazon.co.uk (e.g. shipment-tracking@amazon.co.uk, auto-confirm@amazon.co.uk, no-reply@amazon.co.uk).

  Note: If you purchase from another Amazon international website, the e-mail domain will reflect the country you are purchasing from (e.g. Amazon.de will have all communication coming from @amazon.de.)

- Links to legitimate Amazon websites start with https://www.amazon.co.uk or the equivalent if you're visiting an international Amazon site (e.g. https://www.amazon.fr if viewing the French site). Legitimate Amazon websites also have a dot before "amazon.co.uk" such as https://www."something".amazon.co.uk or "something".amazon.co.uk. For example, Amazon Pay is pay.amazon.co.uk. The

wording before the dot will never be IP address (string of numbers), such as http://123.456.789.123/amazon.co.uk/

Note: Never click on a link, open an attachment or respond to an email you suspect to be fraudulent. If you click on a link or a button by mistake, before entering any information please check using the tips above if the web address is a legitimate Amazon URL.

- Amazon will never ask for personal information to be supplied by e-mail.
- Amazon will never request to update payment information that is not linked to an Amazon order you placed or an Amazon service you subscribed to.

Note: Go to My Orders. If you aren't prompted to update your payment method on that screen, the message isn't from Amazon.