

Amazon Alexa, Echo & Fire TV | Medium | 2 min read

Alexa scams and unexpected purchases: how to stop them

Please note: independent guidance. Vision Tech is not affiliated with the maker. Menus differ between models and software versions, so check the manual or on-screen help.

Echo devices can order from Amazon by voice, and scammers sometimes pretend to be Amazon. A few settings and habits keep you safe.

Set a voice purchase code

You can set a 4-digit voice code to confirm purchases. In the Alexa app:

1. Tap **More**, then **Settings**.
2. Go to **Account Settings**.
3. Choose **Voice Purchasing**.
4. Select **Purchase Confirmation**, then **Manage**.
5. Switch on the voice code and create a 4-digit number.

Menu names in the Alexa app change from time to time, so if yours looks slightly different, look for the closest wording rather than worrying.

Keep the code private. Do not say it when visitors are around. In the same area you can also switch voice purchasing off if you never want it.

Check your orders

Look at your Amazon orders for anything you did not expect, and at your voice history in the Alexa app. If a child or a TV advert could have triggered an order, you may find it there. See our guide on voice recordings first, as deleting history removes the evidence.

Cancel or return

On the Amazon website or app, go to your orders and cancel or return the item if it has not been sent. The website walks you through it.

Spotting scams

- Amazon will not phone and ask you to confirm a payment, or tell you to buy gift cards.
- Do not install software or remote control tools on request from a caller.
- Emails and texts about an Echo order you did not make may be fake. Do not click the link. Go to Amazon's website or app yourself.
- Never give out your password or one-time codes.
- Do not turn off security features at the request of anyone.

If you have been caught out

Change your Amazon password at once, turn on two-step verification, and contact your bank if you gave out card details.

When to get more help

If you think you have been scammed, contact your bank first and report it to Action Fraud. Vision Tech can help secure your accounts and devices afterwards.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.