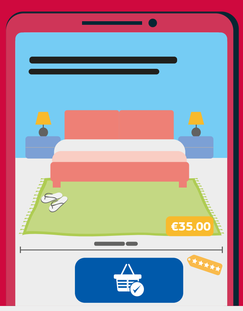
Have you been scammed?

Still waiting for something you purchased online? Or does the product you received not match what you ordered? Then you may have fallen for a scam.

Scams are increasingly sophisticated and we all make mistakes. An online shopping scam is when you make a purchase online unknowingly from a fake website or a fake ad on a genuine site. The product may not really exist, may be counterfeit or may be of inferior quality.



What to do?

1. Try to **contact the retailer,** there may be a genuine reason for the problem.

2. **Contact your financial institution** immediately if:

- your bank account has been compromised
- you notice unusual activity on your credit card account
- you do not receive a response or you are not satisfied with the response from the retailer

You may be able to prevent further theft.

3. **Change your passwords.** The scammer may have your password so change it to a strong password with at least 15 characters including upper and lower case letters, numbers and symbols.

A **passphrase** may be easier to remember. This could be a sentence that includes unusual words, or words from different languages.

You should also **change login details** for any of your other accounts that use the same or similar username and password.

Use a **unique password** for each account.

4. **Update** your antivirus software in order to fight new viruses and protect your device.

5. **Report** the fraud. Your information may help catch the fraudster and prevent further incidents.

To find out where to get advice and to report the crime in your country, visit **https://cybersecuritymonth.eu/cyber-first-aid**

6. Make sure to **keep any evidence** you have of the theft, e.g. emails, invoices, receipts, copy of the advertisement, etc.

7. **Share** your experience with family and friends to help protect them.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth

#ThinkB4UClick