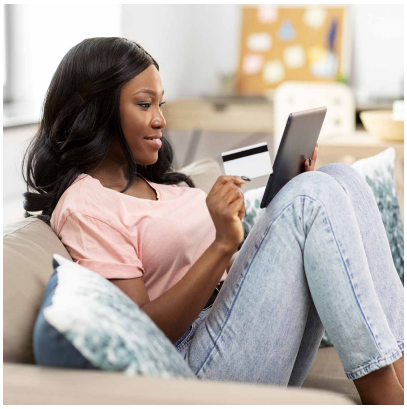


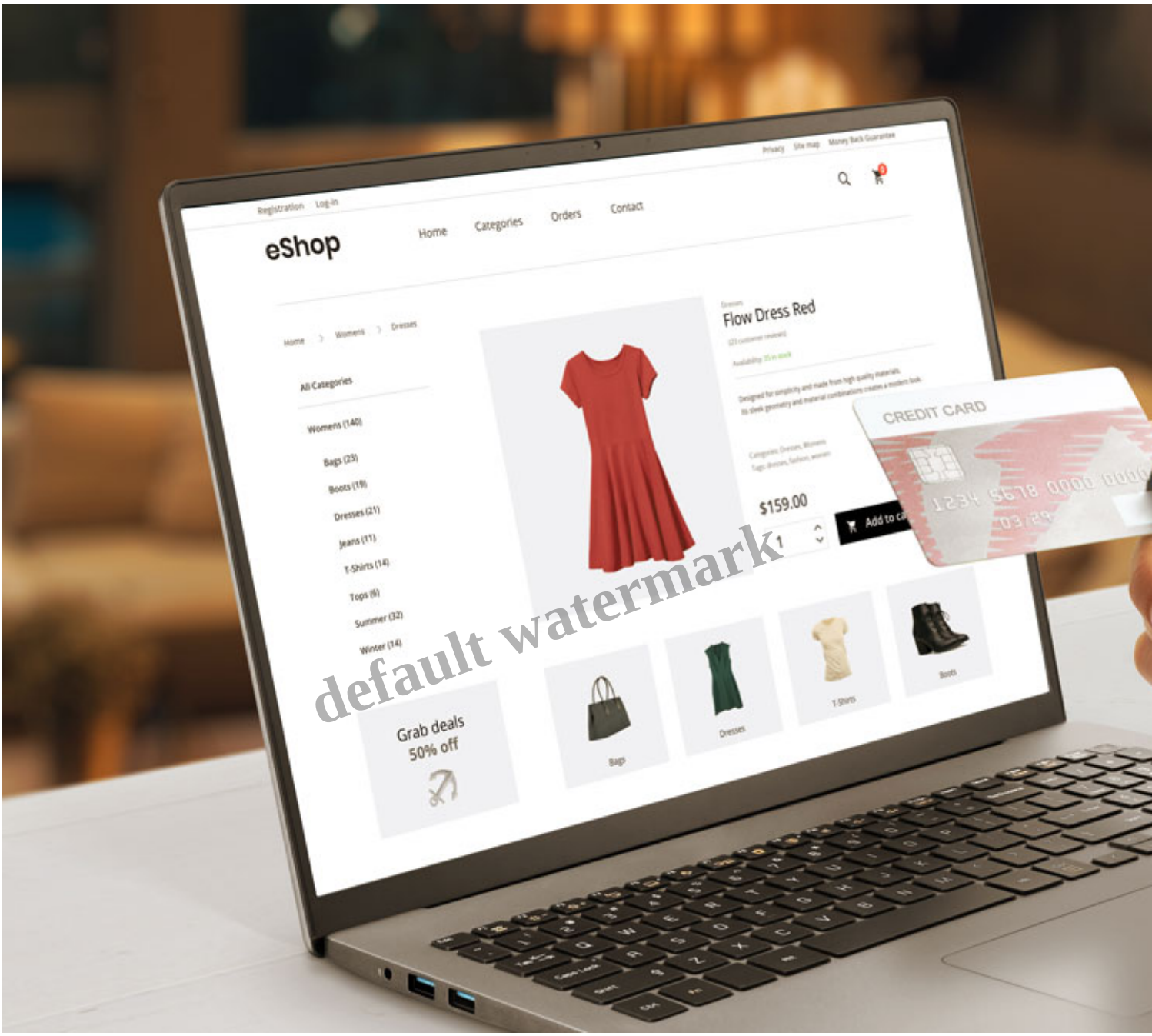
Fool me once

Description

The festive season is prime time for online shopping – and with it, cyber scams. Stay one step ahead of cybercriminals with these essential safety tips and don’t be fooled into losing your hard-earned money.

As online shopping ramps up, so do scams targeting unsuspecting consumers.Typical scams include: phishing emails mimicking trusted brands that trick you into giving away sensitive personal information; fake discount offers with too-good-to-be-true prices aimed at getting you to buy a product that will never be sent; and cloned websites designed to steal your money, personal and financial information.

Wondering how to identify a cloned site?



- Look for subtle errors in the web address when you hover your mouse over the URL, such as extra characters or unusual domain extensions (for example .shop instead of .com).
- Poor grammar, sloppy design, and suspicious payment methods are also red flags.
- Always verify a site's legitimacy by navigating to the website directly.
- Remember to check reviews on independent sites such as Trust Pilot or Hello Peter.
- If in doubt, call the company number to verify. (Top tip: Cloned sites often don't have a contact

phone number, only an email address!)

No phishing allowed

- Hover your mouse over the sender’s email address and look for small errors (for example @amazonn.co instead of @amazon.com). Fake emails often use slight changes to deceive you.
- Don’t click on suspicious links. Hover over links to preview the URL before clicking. A secure website starts with “https” and avoids strange characters.
- Beware of any urgent calls to action or emails urging you to act immediately (such as to claim prizes, benefit from limited-time deals or prevent account suspension).
- If in doubt, verify directly through official channels by contacting the organisation, brand or bank the cybercriminal is pretending to represent.

Fooled? Now what

If you fall victim to an online scam, act quickly.

1. Notify your bank to freeze or block unauthorised transactions.

2. Change your passwords for all connected accounts.
3. Report the fraud to your bank’s cybercrime/fraud unit.
4. Report the fraud to a consumer protection agency.

Remember, vigilance is your best defence. Stick to secure payment methods, avoid sharing sensitive details, and don’t click on unsolicited links. A dash of caution can save you from festive fraud!

Category

1. Our Lifestyle