



Black Friday: Spot the Deals, Avoid the Scams!

Beware of offers that seem too good to be true!

During the Black Friday sales period, attractive discounts can conceal online scams. Cybercriminals exploit the increased interest in online shopping and use various tactics to obtain personal and financial information.

The most common types of online fraud include:

- Creating fake or cloned websites that impersonate legitimate online retailers;
- Sending phishing text messages and emails that appear to originate from well-known companies, banks, or public institutions;
- Promoting fraudulent advertisements on social media featuring unusually large discounts;
- Selling counterfeit products falsely advertised as genuine, branded goods;
- Requesting payments through insecure methods that may expose or compromise banking information.

How can you protect yourself from online fraud?

✓ **Verify the website** – Check that the web address is correct, the online retailer is legitimate, and the merchant's identification and contact details are clearly displayed.

✓ **Be cautious of unusually large discounts** – If an offer seems too good to be true, verify its authenticity before making a payment.

✓ **Avoid suspicious links** – Do not click on links received via text message, email, or social media, especially those concerning blocked parcels, outstanding payments, or exclusive offers. Access official websites directly by entering their addresses in your browser.

✓ **Protect your financial information** – Never disclose your PIN, passwords, or authentication codes, and avoid entering your card details on unfamiliar or unverified platforms.

✓ **Use secure payment methods** – Choose trusted payment options and check customer reviews before placing an order.

✓ **Monitor your bank account** – Enable transaction notifications and promptly report any suspicious activity to your bank.

 **If you become a victim of fraud, contact your bank immediately and report the incident to the police.**

 **Do not let messages such as “Offer expires in 5 minutes!” pressure you into making hasty decisions.** Creating a false sense of urgency is a common tactic used by scammers to prevent victims from verifying an offer before acting.

 **Stay informed, verify before you pay, and protect your money and personal data!**