CYBERCRIMINALS LIKE ONLINE SHOPPING TOO

cyber.gov.au

Secure online shopping checklist:

1. **Shop using secure devices.**
   Make sure the devices you use for online shopping have the latest updates installed and are connected to a trusted network. For example, use your home Wi-Fi or cellular (4G/5G) connection rather than public Wi-Fi.

2. **Protect your payment information and accounts.**
   Be careful saving payment information on an online shopping account. If you do save payment information to an account, you should turn on multi-factor authentication (MFA) to protect it. Where this is not possible, set a long, complex and unique passphrase as the account's password to help keep cybercriminals out. You could also use a password manager to generate and store passphrases for you.

3. **Use trusted sellers.**
   Research online shopping websites before you buy and stick to well-known, trusted businesses.

4. **Know the warning signs.**
   Extremely low prices, payments through direct bank deposits, and online stores that are very new or have limited information about delivery, return and privacy policies can all be signs of a scam.

5. **Use secure payment methods.**
   Never pay by direct bank deposits, money transfers or digital currencies such as Bitcoin as it is rare to recover money sent this way. You should pay by PayPal or with your credit card. You may want to set up a second card with a low credit limit and keep it specifically for online shopping. This will help minimise financial losses if your card details are compromised after shopping online.

6. **Don't engage, and report suspicious contact.**
   Be aware of any strange phone calls, messages or emails you get about online orders. It could be someone trying to get you to share your personal or financial details. If someone contacts you about an order you don't remember placing, it could be a scam. Stop contact and reach out to the store using the details on their official website to check.

7. **Watch out for fake delivery scams.**
   Don't let your guard down while you're waiting for your goods to arrive. Cybercriminals can send fake parcel delivery notifications with links that could trick you into downloading malware or giving away your personal details. If you receive such a message, do not click on the link. Delete the message immediately. You can contact the seller or the courier company using the details on their official website. Scamwatch has examples of what these fraudulent text messages may look like.

8. **Take additional precautions**
   It is always a good idea to limit the amount of personal information that you use on websites. Ask yourself if the website really needs this extra information or an account to complete the transaction.

WHAT TO DO IF THINGS GO WRONG

If you've been the victim of a cybercrime:

VISIT
cyber.gov.au for more advice on how to be secure online.

SIGN UP
To our free alert service **cyber.gov.au/acsc/register** and follow us on Facebook **facebook.com/cybergovau**

REPORT
Cybercrime to REPORTCYBER: **cyber.gov.au/report**

CONTACT
Call **1300 CYBER1** or visit **cyber.gov.au**

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre