



## Safe Internet Shopping

---

- Ensure that any online retailer unfamiliar to you is reputable by researching them;
- Establish a physical address and telephone contact details; Remember that the best way to find a reputable retailer is via recommendation from a trusted source;
- Remember that paying by credit card offers greater protection than with other methods in terms of fraud, guarantees and non-delivery;
- Double check all details of your purchase before confirming payment;
- Do not reply to unsolicited emails from companies you don't recognise;
- Before entering payment card details on a website, ensure that the link is secure, in three ways:
  - There should be a padlock symbol in the browser window frame, which appears when you attempt to log in or register; Be sure that the padlock is not on the page itself as this will probably indicate a fraudulent site;
  - The web address should begin with 'https://'; The 's' stands for 'secure';
  - If using the latest version of your browser, the address bar or the name of the site owner will turn green.
- Some websites will redirect you to a third-party payment service (such as WorldPay);
- Ensure that these sites are secure before you make your payment;
- Do not pay for goods when using an unsecured Wi-Fi connection;
- Safeguard and remember the password you have chosen for the extra verification services used on some websites, such as Verified by Visa;
- When making a payment to an individual, never transfer the money directly into their bank account but use a secure payment site such as PayPal, where money is transferred between two electronic accounts;
- Check sellers' privacy policy and returns policy;
- Always log out of sites into which you have logged in or registered details; Simply closing your browser is not enough to ensure privacy;
- Keep receipts;
- Check credit card and bank statements carefully after shopping to ensure that the correct amount has been debited and also that no fraud has taken place as a result of the transaction;
- Ensure you have effective and updated antivirus / antispyware software and firewall running before you go online;
- Where possible, check that the price listed by the retailer on your browser is the same as that quoted on other people's browsers, to ensure you are not being monitored and overcharged.

### **The Risks:**

- Fraud resulting from making payments over unsecured web pages;
- Fraud resulting from making payments using an unsecured Wi-Fi connection;
- Bogus online stores / shops – fake websites and email offers for goods and services that do not exist;
- Buying fake goods intentionally or unintentionally - finding they are of inferior quality and also possibly funding more serious crimes in the process;
- Losing your money when you make direct bank payments, only to find that the goods are inferior, or do not exist at all;
- Receiving goods or services which do not match the advertiser's description;
- Being offered tailored prices based on information gathered by the retailer about your online shopping habits and websites visited.