infosec@pjlhuillier.com
ICT GROUP
INFOSEC 101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

**December 19, 2014  Release # 297**

-- Begin Transmission --

# How to buy online safely

## Can you trust your common sense and intuition?

Unfortunately, it is not practical for users to determine if a website is safe or not with the naked eye. Purchasing from a secure computer or device running the latest antivirus software, firewalls and security patches will significantly decrease your chances of becoming a victim. Never follow links from unsolicited online communications, such as email messages, social media posts, or instant messages.

### Familiarize yourself with the Terms of Use and the Data Protection Policy

Read the fine print. Terms can sometimes detail hidden and unexpected costs or obligations.

### Only purchase through websites using encryption

URLs that start with https:// rather than http:// (the “s” stands for secure) are encrypting information during transfer. Another indicator of a website using encryption is a small padlock icon displayed in the Internet browser. However, there is no guarantee that these sites are safe, as hackers can create websites that use encryption but are designed to steal personal information.

### Provide the minimum amount of personal information

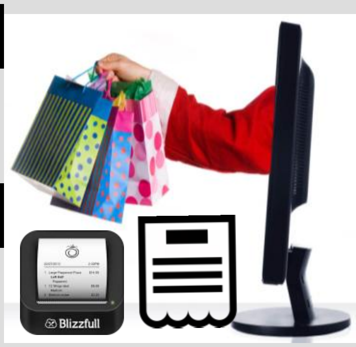
Leave optional fields blank: Middle name, date of birth, mobile phone number, hobbies. Many website operators request optional information alongside required information to process a business transaction. Compulsory fields are often identifiable by an asterisk.

### Never share your password

Even if someone else is making the purchase for you, you should enter the password yourself and never share it with others. To stop subsequent users from accessing your account without authorization, never select the “remember my password” option on a shared computer.

### Buy local where possible

When the seller is based in a different country, it can be much more difficult and expensive to resolve any issues and to enforce consumer rights legislation.



### Check your bank statements

Check your bank account transactions regularly, particularly after making purchases over the Internet, to be sure that all payments are legitimate. If you discover payments that you cannot identify, inform your bank immediately.

### Keep your order confirmations and receipts

Always retain important information relating to a purchase in either printed or electronic format. This information will be very useful in resolving any issues relating to the purchase.

-- End of Transmission –

**Information Security:** It’s a Shared Responsibility

REFERENCE(S): Sophos Ltd. (2012). *Threatsaurus: The A-Z of computer and data security threats.* Boston, USA | Oxford, UK

**INTERNAL USE ONLY:** For circulation within the PJ Lhuillier Group of Companies only.

**Document Code: 2014ICT_15SECA040**