



News Release

December 16, 2011

Christmas shopping tips to protect your privacy

WHITEHORSE –

Shopping Privacy Tips for Consumers

- Cyber-crooks are gearing up for the holidays so stay alert against fraudsters who will make merry with your online personal information. Some **privacy tips for online shopping** are as follows:
 - Research your merchant – look at the merchant’s privacy and security policy and customer ratings prior to making any purchases on line.
 - Make sure when entering personal information that the website is secure.
 - Reputable merchants usually send you an e-mail confirming your order. If you don’t receive an email confirmation you should follow up immediately.
 - Use a low limit credit card for online purchases and one that provides you with specific guarantees, such as 100% coverage for any losses due to fraud when shopping on the web.
 - Make sure your computer security is up to date to protect against spyware, adware, malware and other internet attacks.
 - Do not use the same username and password at every website. If your personal information is compromised, a thief will not get very far if you use different passwords and usernames on different websites.
 - Never share your website passwords and online banking account information with anyone.
 - Do not get fooled by extraordinary offers. If a product or service looks too good to be true, it probably is.

News Release

Page 2 of 3

- Beware of emails asking for personal information even if they appear to be from a reputable source. Fraudsters will often send “phishing” emails trying to steal your personal information or install malware.
- Do not click on links if you do not know or trust the source.
- Thieves and fraudsters are also present in stores. Some **privacy tips for in-store shopping** are as follows:
 - Do not provide your personal information, such as name, address, telephone number, and postal code, when asked to do so by a retailer unless they can provide a reasonable purpose for the collection, use and length of retention.
 - Keep your credit card receipts to check against your monthly credit card statement.
 - Shred sales receipts and other paper that displays your credit/debit card number or bank account numbers – thieves are known to sort through residential trash to find these items which may be used to commit identity fraud.
 - Be cautious about clerks that double swipe your debit or credit card. Ask for cancelled sales receipts.
 - Don’t give your debit or credit card PIN to anyone or write the number down (e.g. on your debit card).
 - Cover the PIN pad with your hand when entering your PIN into a point-of-sale terminal or ATM.
 - Keep an eye on your debit or credit card when you give it to the store clerk or waiter – make sure it’s not out of your sight.
 - If you see something suspicious relating to point-of-sale terminals or ATMs, report it to the store merchant.
- Additional privacy tips:
 - Do not leave purses or wallets in your vehicle, or unattended in a store.
 - Do not carry your SIN card or birth certificate in your wallet in case of loss.

News Release

Page 3 of 3

Shopping Privacy Tips for Merchants

Retailers are reminded to protect customer and employee personal information.

- Do not collect personal information if you do not need it.
- Do not record driver's licenses or other forms of ID used to verify the identity of a credit card user.
- Limit access to personal information to only those employees that need to see the personal information to do their job.
- Make sure that credit card numbers are properly obscured or truncated by point-of-sale terminals.
- Make sure point-of-sale terminals are visible to consumers throughout the transaction: credit and debit cards should not disappear under the counter to be swiped.
- Find out if your point-of-sale terminals collect and store customer credit and debit card information. If so, make sure you protect the device against theft. Advise your staff to keep it stored when not in use and not give it any person except for the purposes of conducting a sale.
- Protect personal information on your premises – store paper records securely; ensure information on your computers is protected with adequate safeguards including proper physical security, locked doors and alarms, and technical security, such as passwords; shred or securely dispose of all customer information once it is no longer needed.
- Train and retrain staff about their obligation to protect privacy and provide your staff with the information they need to inform customers about your privacy policies and procedures, including why you collect consumer personal information. Example, your staff should be able to explain to a customer why you collect personal information as part of processing a refund.

For more information contact:

Tracy-Anne McPhee

Information and Privacy Commissioner

867-667-8468

info@ombudsman.yk.ca