Yukon Information and Privacy Commissioner

3162 Third Avenue, Main Floor
Whitehorse, Yukon, Y1A 1G3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.yukonombudsman.ca

Privacy Tips for Holiday Shoppers 2020

When shopping online…

- **Ensure your computer security is up to date.** One of the ways that cybercriminals obtain identity or payment information is by exploiting outdated computer security. Make sure that you use an up-to-date web browser (the program you use to surf the Internet), have an active and up-to-date virus scanner, and ensure your computer is receiving updates for its operating system.

- **Don't online shop while using a non-secure wireless Internet connection.** Identity thieves or fraudsters can easily capture your personal information, including card payment information, while it is being entered using public or shared WIFI.

- **Ensure any shipping notifications are real before acting on them or clicking on any links.** One example of a recent scam is Canada Post notifications that are actually phishing clones (https://www.canadapost.ca/web/en/kb/details.page?article=what_do_to_if_you_ge&cattype=kb&cat=security). There may be similar schemes targeting users of other shipping companies. (To learn more about phishing, go to https://www.getcybersafe.gc.ca/en/blogs/phishing-introduction.)

- **Beware of online vendors who only accept gift cards.** Gift cards do not have the same purchase protection as many credit cards and it may be hard for law enforcement officials to trace the transaction, if the product or service is not received.

- **Take extra measures to ensure the shopping website is real.** Identity thieves and fraudsters set up fake websites that look like legitimate online stores or marketplaces, and then collect personal and credit card information. Below are some ways to help verify if the website is legitimate or not.
    - Examine the website address. If it is unusual, it is likely fake (i.e. amason.com or amazon.shopping.com instead of amazon.com). Also, try a Google search such as "Is [website address] a scam?"

(more)

- Check if the website has a history on the Internet archive at https://archive.org/web/web.php. Having a bad reputation or no history is an indicator that the website may be fake. For more information on checking the reputation of websites, go to https://www.highya.com/articles-guides/how-to-tell-if-an-online-store-is-legit.
- Be wary of online shops that use international phone numbers, a free email service such as Gmail as their contact information or have only a "contact us" form instead of a phone number and address.
- After verifying the legitimacy of the site, search online comments or reviews related to the website or online store.
- Be suspicious of great deals on brand items; sometimes it really is too good to be true.

- **Be wary of personal information being collected**. A website should require a minimal amount of personal information to complete a purchase. When making an online purchase, it is normal to be asked to provide contact and payment information. You should never be asked to provide sensitive personal information such as your Social Insurance Number (SIN) and driver's license information. (One example is individuals being asked to provide personal information in order to receive a discount coupon, which may or may not work. This information may be used for marketing emails, phishing attempts or other purposes which are not your primary intent.)

- **Don't use the same username and password for various accounts or online stores**. If identity thieves and fraudsters are successful in hacking into databases containing credentials, they can then access other websites where you have used the same log-in information. You can check at https://haveibeenpwned.com/ to determine whether any of your accounts have been compromised and if so, stop using similar credentials for other accounts.

- **Don't share your username and passwords with others**. Sharing this information for online banking, PayPal and similar payment accounts may eliminate your ability to recover losses on these accounts. Even sharing information with people you trust can be risky because they may not take adequate precautions to protect your information and your accounts could then be compromised.

- **Educate yourself on the most common types of scams used in online shopping**. Good websites to check are https://www.priv.gc.ca/en/blog/20181217/, https://www.getcybersafe.gc.ca/en/secure-your-accounts and https://www.scamwatch.gov.au/types-of-scams/buying-or-selling.

(more)

- **Choose secure and reliable payment options when possible.** Methods such as email transfers, money-wiring (Moneygram, Western Union) or bitcoin transfers are insecure, hard to trace and uninsured by nature.

When shopping at a store…

- **Cover up your Personal Identification Number (PIN) when using debit or credit cards.** PIN codes have been compromised when others watch while people enter their PIN and then record it. Watchers could include the store clerk, other shoppers, or video surveillance, including someone recording with their smart phone.

- **Ensure automated cash machines have not been compromised**. A machine that has been tampered with may allow your bank information to be stolen. Some helpful tips to prevent this are outlined in the video found here.

- **Don't let your debit or credit card out of your sight**. Credit card information has been stolen by people who take a card when the owner isn't looking, and then record the information for future use. They may be able to replace the card before you know anything has happened or they may switch your card for one that appears to be the same.

- **Be cautious of double-swiping of your debit or credit cards**. This technique has been used to send card information someplace other than the bank, such as a personal computer. It has also been used to gain direct access to cash by debiting an account for a cash-back transaction.

- **Be wary of personal information being collected**. A store should only require personal information that is necessary to complete the payment transaction, such as a debit or credit card when being used for payment. If the clerk asks you for information such as your name, email address, mailing address, phone number, driver's license number or Social Insurance Number (SIN), ask why they are collecting this information and what their legal authority is for the collection. There are very few circumstances that would authorize a store to collect your driver's license number; this information is often sought by identity thieves or fraudsters. Any request for your SIN should be refused.

- **Keep an eye out for suspicious portable payment devices in restaurants and shops**. Identity thieves and fraudsters have been known to switch a portable debit/credit card machine with a fake one that allows them to directly collect the payment and card information. If you have any suspicions regarding a device, report it to the store manager.

(more)

General shopping and privacy tips…

- **Be careful to ensure that any charities you donate to are real.** Some cybercriminals pretend to be COVID-19 charities and ask for donations. See this federal list of 86,000 verified charities at https://apps.cra-arc.gc.ca/ebci/hacc/srch/pub/dsplyBscSrch?request_locale=en.

- **Check your bank and credit card accounts often**. Immediately report to your bank (or credit card company) any transactions that you did not make. Fraudsters have been known to make small purchases or withdraw small amounts daily to avoid detection.

- **Use auto-notification.** It is helpful to activate auto-notification of credit card charges within your banking app.

- **Use a low limit credit card to make purchases, especially online**. This eliminates the possibility of a fraudster racking up large purchases.

- **Don't provide personal information in response to an email or telephone call.** Identity thieves or fraudsters will use a technique known as phishing to obtain personal information from you, which can be used later to steal your identity and commit fraud. No legitimate company or government should request personal information directly via email or phone. It is strongly recommended that you not provide personal information in response to a phone call or email contact that you did not initiate, because there is no way for you to confirm the real source of the call or email. In general, bodies such as Revenue Canada, Kijiji, Facebook, Ebay or Microsoft will not call you. If you get a call from someone claiming to be from these entities, it is most likely a scam.

- **Don't open emails from individuals you don't recognize.** Just opening an email attachment or link can launch malware or a virus onto your computer. Malware makes it possible for personal information stored on your computer to be stolen. Malware can also corrupt or encrypt your computer files, making them inaccessible. Even if you do recognize the sender, their account could be compromised. Always be wary of emails that look suspicious and contain links or attachments.

Although these tips should be helpful, nothing is guaranteed, and new scams are being developed all the time. Shoppers should continue to use their own discretion and be vigilant when sharing personal or financial information.