爲什麼身份盜竊竟是這樣一個問題?

身份盜竊是北美發展最迅速的、使消費者受害的罪行。此犯罪行每天每日影響更多的人們，而實際上，大多數人卻認爲不可能或不會發生在他們身上。近來這一類型犯罪行為的增加主要歸因於閱卡器的出現以及電腦黑客入侵的犯罪行爲的增加。

什麼是盜竊身份?

盜竊身份指的是一個人使用另一個人的身份為了達到詐騙或謀取經濟利益的目的。使用諸如姓名、地址、社會保險號碼此類最基本的個人信息資料，身份盜竊犯用其申請貸款、按揭、信用卡、租賃汽車或公寓以及從事其它犯罪行為，所以這一切均使用被盜的身份。這經常導致無辜的受害者去負責處理由此產生的經濟和法律糾葛以及面臨著重新建立他們良好信譽的困難。

罪犯是如何盜用您個人的信息資料的?

肩窺法: 身份盜賊置隱形照相機於銷售點終端機的鍵盤或自動提款機上方爲了對無戒心顧客的個人身份號碼(PIN)、信用卡號碼或密碼進行拍照。

光顧垃圾和回收桶: 衆所周知，身份盜賊在垃圾桶裏尋找丟棄的貸款申請書、信用卡賬單或財務記錄以便獲取個人信息資料。

盜竊個人財產: 罪犯會從錢包、皮夾和汽車雜物箱下手獲取個人信息資料。電腦也是极佳的信息資源，因爲他們可獲取所訪問過的網址記錄、個人電子郵件以及網上銀行業務信息。

不正當的閱卡或僞造行爲: 此行爲經常發生在自動提款機和銷售點終端器。閱卡器通過數據儲存器能使身份盜賊讀取信用卡或銀行卡（debit card ）號碼以及個人身份號碼。這些裝置旨在儲存個人信息以便後來複製這些卡用於他們自己的盜騙活動。

買賣信息: 如果不誠實的職工讀取了個人信息資料和信用卡號碼，他們通過互聯網聊天室傳播或銷售這些信息。

光顧信箱: 身份盜賊偷竊個人郵件或使其改寄另一通信地址或郵政信箱。竊賊尋找新的信用卡、預先核准的信用卡通知書、保險陳述書、收入報稅資料、投資文件和顧主福利表。

獲取個人信息資料的其它手段

網絡釣魚騙術（Phising） (與"fishing"讀音相同) – 這是通過現代技術加以更新的故伎重演。網絡釣魚騙術包括竊賊假冒合法企業的代表通過郵件、電話或互聯網進行促銷。他們向您提供令人煩惱或令人興奮的信息，該信息需要立刻回應，依此騙取使用者所披露的私人信息。這種騙術常見於欺騙性的比賽以及幾乎所有的活動；受害者不會得到他們被承諾的東西。

科技農民騙子（Pharmers） – 身份竊賊只不過使互聯網用戶從合法的網站改為使用欺騙性的網站，該網站已被僞裝成如同原來那個合法的網站。這騙術是通過使用嵌入的鏈接，聲稱會使您連接到一個安全的網站。當用戶輸入他們的登錄姓名以及密碼，身份竊賊能夠讀取這一信息以便將來之用。

電腦使用的安全提示

- 決不可使用公共電腦從事財務活動;
- 安裝抗病毒軟件，確保定期更新;
- 訪問以 http://為前綴的網站;
- 在螢幕的底部尋找表示安全網站的鎖或未破損鑰匙的標示符號。

Guard your personal information and documents.

Phising – essentially this is an old con game updated to take advantage of new technology.
Phising means using mail, phone or internet promotions in which thieves falsely claim to be representatives of legitimate enterprises. They provide you with upsetting or exciting information which demands an urgent response in an attempt to scam the user into disclosing private information.
Example – receiving a bogus e-mail from a company that appears to look legitimate asking for account or PIN numbers.

Pharmers – simply redirect as many internet users as possible from legitimate commercial web sites and lead them to malicious sites that are made to look legitimate.
This is done by a "imbedded link" which claims to bring you to a secure site. When users enter their login name and password, criminals are able to capture this information.

Tips for Computer Use

- Never use a public computer for financial transactions.
- Install virus protection software and update it regularly.
- Be careful what e-mails you open
- Look for web sites that begin with http://
- Look for an icon of a lock or an unbroken key.

CRIME PREVENTION

TORONTO POLICE SERVICE

EMERGENCY

9-1-1

POLICE NON – EMERGENCY

(416) 808-2222

For more information regarding IDENTITY THEFT contact the Crime Prevention Officer at your local Police Division

Working Together to Prevent Crime…

SP - E, 2005/08

IDENTITY THEFT