

# 歲晚呢錢變招 冒公營機構及銀行套資料

# 市民誤按「釣魚」Link

# 慘遭騙徒擄住拎



年近歲晚，又是騙徒搵食旺季，在網上廣布「釣魚」騙局，不少市民失財！近期不少港人包括多名立法會議員，紛紛收到欺詐短訊或電郵連結（Link），假冒港燈、煤氣公司、香港郵政，以及銀行等，十分逼真，一「擊」（點擊）即「上釣」。

參看警方統計數字，去年11月至今年7月的「釣魚電郵騙案」舉報涉及損失達320萬元，最大一宗的事主被誘騙至假銀行損失275萬元。網絡騙案層出不窮，年關將至，警方呼籲市民提高警惕，收到各種不明來歷的超連結時，務必三思而後「擊」。

大公報記者 盛德文、賴振雄、黃山

「好彩及時醒覺，無輸入個人同銀行資料去，如果唔係就慘啦！」，上月險被假冒港燈的退款電郵超連結而「中招」的陳女士，近日接受大公報記者電話訪問時猶有餘悸。

## 假冒港燈及香港郵政

在港島西區居住的陳女士，上月中旬在手機收到聲稱「港燈」的短訊，指發票計算錯誤，向其退還213元，並附上一個超連結，要求客戶點擊該連結以驗證身份。陳女士手快按入該超連結，發現要輸入個人資料，因眼花叫家人代輸入資料，被女兒發現可疑而作罷，截圖後即時將該連結刪除。事後，發現是假冒港燈的詐騙連結。

記者日前按陳女士提供的資料登入該超連結，跳出「港燈」的「客戶登錄」網頁，見到：「可再生能源證書申請狀態跟蹤」欄目，按指示填寫客戶資料及驗證碼再提交，網頁顯示「驗證碼不正確，請修改重試」，顯示網頁已無法登入，相信網站已被警方查封。記者發現連結的偽冒網站，完全照抄港燈的網頁格式，頂部印有港燈標誌和特區區徽，非常逼真。

港燈公共事務部昨日對《大公報》表示，上月21日已在公司網頁提醒市民慎防帶有惡意連結或附件的詐騙電郵，並已就事件向警方報案，對於事件涉及多少客戶及影響範圍，暫未有補充。

騙徒除了假扮港燈退款外，還扮成香港郵政或其他公用事業機構，以釣魚形式超連結「請君入籠」。市民莫女士昨日向《大公報》表示，上月底收到一則聲稱是香港郵政的短訊通知，寫有「由於欠缺資料，我們無法

交付您的包裹」，短訊附有一個超連結，由於她不懂得如何處理，找女婿代為處理，其女婿按指示，登入網頁後，即見看似香港郵政「寄投易ec-ship」服務的網站，要求輸入名稱、地址和電話等個人資料，並支付運輸費。

莫女士輸入相關資料後，網站跳往另一頁面，要求輸入信用卡資料作付款。她頓覺奇怪，懷疑被騙，即時停止輸入資料，退出連結，後來證實是一宗騙案。她和女婿至今仍擔心輸入的個人資料，會被不法之徒反覆使用。記者昨日按莫女士提供資料登入該連結，發現該詐騙連結已被警方查封。

## 扮銀行職員套PayMe密碼

除以上的犯案手法外，PayMe亦是騙徒瞄準的目標，騙徒通過非法途徑獲取市民個人信息後，假冒銀行職員致電，準確說出受害者姓名及身份證號碼，增加可信性，以銀行戶口出現異常等藉口，誘使受害人按內附的超連結進入假網站，或更新電子支付平台「PayMe」戶口，騙取受害者的「一次性密碼」及「交易密碼」後，登入並騎劫其「PayMe」戶口，將存款轉走。

今年6月12日，有女事主接到假冒銀行職員的騙徒電話，被對方以上述手法，誘使其交出密碼及驗證碼，受害人其後發現PayMe戶口瞬間損失三千元。



## 漁翁撒「網」 「釣」走個人資料

不法分子會從不同途徑（如系統漏洞、暗網等）收集個人信息後，以所謂「釣魚」方式，即漁翁撒網向市民廣發電郵或手機短訊，誘使市民點入釣魚網站，輸入信用卡資料等，然後利用其信用卡資料購買貴價物品或將款項轉走。

今年1至9月，警方共接獲735宗電騙報案，比去年同期下跌18%。不過，今年最高單一損失案件就高達2.3億元。

## 六旬漢中招失275萬

警方去年11月至今年7月接獲共183宗釣魚電郵騙案報案，損失達320萬元。今年6月14日及24日，警方先後拘捕一名34歲本地男子及一名35歲突尼斯籍男子，兩人涉案19宗共騙款33萬元，主要假冒香港郵政奪取事主信用卡資料，當中一名商人被騙28萬元。

而今年1月至9月，警方共接獲86宗涉電子支付平台及假冒銀行網站的騙案，損失1780萬元。其中最大宗的銀行釣魚網絡騙案的受害者是一名六旬男子，被誘騙點擊假冒滙豐銀行的「網絡釣魚」短訊，輸入賬戶資料及密碼後，損失275萬港元。

## 銀行短訊電郵 不會附超連結

近年假借銀行、快遞、公共事業機構之名行騙愈來愈多，警方及有關部門多次提醒市民要警惕，見到不明網頁的連結，需三思而後「點擊」，如有懷疑，應致電有關機構查詢，或打警方反詐騙協調中心的「防騙易」熱線，避免上當。

按照金融管理局的要求，銀行不會透過短訊或電郵超連結，引領客戶到其網站或流動應用程式進行交易，更不會透過超連結要求客戶提供任何敏感的個人資料（包括登入密碼和一次性密碼）。換言之，公眾若收到任何短訊或電郵超連結，要求輸入網上銀行個人登入資料，該等短訊或電郵並非由銀行發出的，必須提防。

## 有懷疑致電客服查真偽

警方亦多次呼籲市民，切勿透過電話短訊或電郵內的超連結登入任何可疑網頁，以及隨意打開可疑電郵內的任何連結或附件。警方提醒大家留意超連結的英文串法，小心檢查該連結和相關機構的網址有否不同，從而辨別真偽。另外，市民勿將信用卡資料及保安碼，輸入到不明來歷的應用程式或網站，及向陌生人透露銀行登入資料或一次性密碼。市民如收到自稱PayMe等支付公司職員來電，應掛線並直接聯絡客戶服務，查證真偽。

## 防騙小貼士

- 定期更改電子錢包交易密碼
- 若發現電子錢包有可疑交易或變更，應主動向供應商查證
- 勿向陌生人透露電子錢包供應商發出的「驗證碼」或「交易密碼」
- 切勿將個人資料輸入可疑訊息的內附連結



## 釣魚騙局



陳女士按入短訊超連結顯示的假冒港燈網頁。

## 市民有Say



### 唔好貪 免上當

楊伯：有朋友收到類似信息，包括有中電同銀行的，並及時轉發提醒自已。以前都收過澳門、內地等領獎信息，但自己從來不信。防詐騙，記住唔好貪就唔得。

大公報記者陳詠韶



### 停一停 想一想

張小姐：自己就暫時未收到，但平時亦會提醒家人不要上當。如果收到類似信息，我會先停一停、想一想，再謹慎應對，自己冇辦理過相關業務，冇無交過那些費。

## 職員貪平出事 港商訂貨遇騙

### 慎防陷阱

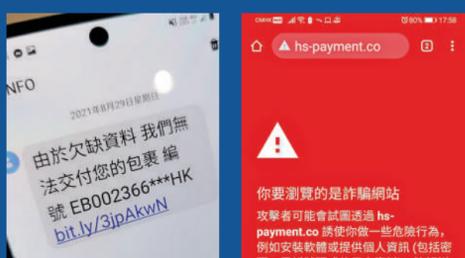
釣魚短訊可謂無處不在，有港商亦遇上。香港中小企協會創會會長余繼泉表示，有在內地設廠的港商吩咐職員購買文具之類物資，有職員貪貪平，選購標價較低但不熟悉的供應商，卻不知墮入騙局。不久後，職員收到對方短訊通知，因缺貨無法如期交付，騙徒要求他再次輸入信用卡資料確認，以作退款，職員不虞有詐，令公司招致財務損失。

立法會議員葛珮帆表示，以往也曾經收到有中小企向她反映訂貨時被騙，更有騙徒扮成客戶，表示合作上出現問題，過程中要求匯錢解決。由於牽涉的金額不算很多，騙徒可以清楚說出客戶的資料，職員信以為真。

今年5月，葛珮帆與立法會議員陳恒鏞及劉國勳幾乎同時收到可疑PayMe驗證碼短訊，三人隨即向金管局作出投訴及向警方報案，並公開提醒市民慎防騙徒。



假冒港燈網頁要求輸入個人資料。



市民莫女士收到假冒香港郵政的短訊。



大公報記者事後按入莫女士提供的郵政包裹連結，發現已被移除及加上詐騙網站的警告。

## 防騙電話

- 防騙易熱線：18222
- 衛生防護中心熱線：2125 1111/2125 1122
- 港燈客戶中心電話：2887 3411
- 香港郵政熱線：2921 2222
- 滙豐個人客戶服務熱線：2233 3000
- 順豐香港客戶熱線：2730 0273