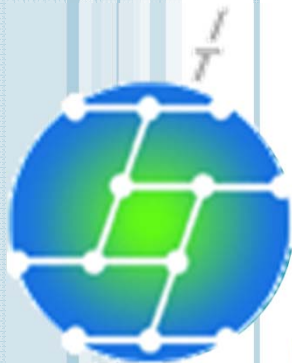


# Information Security and Protection of Personal Data & Privacy

- Incidents Sharing & Tips on Data Protection



CUHK

1

Prepared by:

Information Security Section (ISS),

Information Technology Services Centre (ITSC)

E-mail: [infosec@cuhk.edu.hk](mailto:infosec@cuhk.edu.hk)



# AIMS

## To Alert

The recent incidents and trend of cyber attacks

## To Think

What common risks of data leakage around us?

## To Learn

Tips to prevent data leakage

# AGENDA

- Information Security Incidents
- Statistic on data leakage
- 4Ps to REMEMBER!
- Tips on preventing data leakage



# INFORMATION SECURITY INCIDENTS



4

# IS INCIDENTS



8 Feb 09



香港特別行政區政府  
消防處

## Foxy又泄消防機密文件 (星島日報)

- 有市民昨日在Foxy成功下載六十多份、涉及二十多名消防員的考核報告，暴露有關消防員的月薪及職級等個人資料，其中更包括去年救人殉職的英雄蕭永方。消防處表示，對事件非常關注，會調查跟進事。

6 Dec 09



香港特別行政區政府  
香港警務處

## 警隊瘋狂洩密 177文件歷來最多

- 外洩私隱五花八門
- 指令被當「耳邊風」
- FOXY洩密個案 1 德籍夫婦離婚
- FOXY洩密個案 2 女警驗身報告
- FOXY洩密個案 3 兩名警員走犯
- FOXY洩密個案 4 警員遺失裝備
- FOXY洩密個案 5 查問死者家人

14 Feb 09

## 南華球星薪酬 Foxy 洩秘 (蘋果日報)



- 南華球員及教練由1997至2008年10個球季間，多個月份的支薪紀錄昨日被發現可透過Foxy檔案分享軟件任意下載，出糧紀錄詳細列出著名球員歐偉倫、李健和及丘建威等的私隱資料，包括月薪及銀行賬號等....

# IS INCIDENTS



香港特別行政區政府  
入境事務處

## 機場入境處電腦懷疑失竊

明報 – 2012年10月18日星期四下午8:44

入境處表示，三部於機場管制站用作執行入境管制工作的**手提電腦懷疑失竊**，已報警方處理。由於有關電腦載有外地旅客的個人資料，入境處亦已就事件向個人資料私隱專員公署作出資料外泄事故通報。

入境處發言人表示：「入境處機場管制科在本月十七日知悉遺失三部用作執行入境管制工作的手提電腦。由於事件可能涉及失竊成分，入境處於今天已報警方跟進。入境處會全力協助調查。」

發言人補充：「根據初步估計，事件涉及**約三千個外地旅客旅行證件上的個人資料**，當中並不涉及任何香港居民。...

## HSBC admits losing data of 159,000 account holders



8 May 2008

- HSBC announced **losing a computer server** containing **private data of 159,000 account holders**. HSBC admitted it lost track of the server during renovations at its Kwun Tong branch. It was claimed that the server was protected by multiple layers of security.



# IS INCIDENTS



## 瑪麗文員失 USB手指 洩 19病人資料

2011年4月21日

【本報訊】公立醫院再有員工遺失病人資料。瑪麗醫院兒科一名文員去年七月，將載有 **19名**兒科病人姓名及身份證號碼的一個檔案，從一部已設密碼的電腦，違規轉載入一隻**無密碼保護或加密系統的 USB手指**內，以作備份，但至本周一卻發現該 USB手指不翼而飛；院方已通知警方及私隱專員公署，涉事職員已被紀律處分。...

瑪麗醫院發言人指，已聯絡所有受影響病人或家屬，並向各人致歉及解釋事件不會影響其醫療服務。至今未有接獲病人資料外洩的查詢和報告。

無密碼保護及加密

...

2008年5月6日

- 醫院管理局（醫管局）行政總公布，截至四月底的過去十二個月內共有九宗**遺失電子儀器引致病人資料遺失**的呈報個案。
- 當中七宗與盜竊有關。
- 遺失的電子儀器包括四個**USB**電子儲存媒體，一部電子手帳、一部數碼音訊處理器（**MP3 player**）、一部中央處理器、一部手提電腦及一部電子照相機。
- 共**6000名病人的資料**，其中**1000人的資料沒有加密**，身分證號碼等個人資料可能會外洩。
- 有關資料主要由人手下載。

# IS INCIDENTS



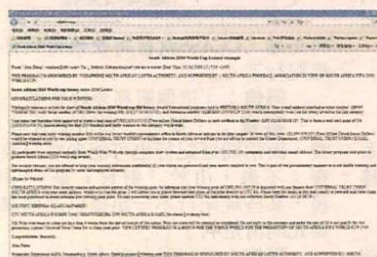
www.hkheadline.com  
25/02/2010 THU

頭條日報

## 稱可贏世界盃門券 電郵詐騙 多人「中招」

**新聞故事** 騙局處處有，今年新春特別多。農曆新年期間，有名人的電郵被不法份子盜用，訛稱在外地被洗劫急需匯款解困，企圖騙財。近日更有不少市民接獲聲稱可贏取「南非世界盃比賽入場券」及獎金的詐騙電郵，多人被騙去五百美元（約四千元）。有電腦專家指近期最流行的四大主題，包括如為海地地震籌款、世界盃門券、外遊失竊、購買電子產品。本報記者

**只**要擁有電郵地址，幾乎都曾接獲欺詐電郵，詐騙理由各式各樣，防不勝防。就讀中學的足球迷阿文於去年十一月收到英文電郵，聲稱是「美國樂透公司」經理Alex Zuma指阿文在一個足球網站登記後成功中獎，贏了二〇一〇年南非世界盃比賽入場券十張，並可與其他幸運兒瓜分二千萬美元（約一億五千六百萬港元），個人獲得十萬美元（約七十八萬港元），但要求阿文先提供詳細個人資料、足球網帳戶及密碼，以及銀行帳號等。



■ 近期最熱門的詐騙電郵，內容是訛稱贏取了世界盃門券。

「我見電郵有我的英文名，我又真是曾經在提及的足球網站登記，以為自己無端端中獎。」阿文不虞有詐回覆電郵，兩日後卻收到對方要求先匯款一萬美元（約七萬八千港元）至美國作為保證金，才會寄出入場券及將獎金轉帳。

### 科技罪案去年約1500宗

一心以為得到巨款及「一票難求」的世界盃門券的阿文未疑有詐，卻擔心沒有錢交「保證金」，遂回覆電郵表明難處。不料對方竟自動將保證金降至五百美元，阿文一心以為上天眷顧，匆匆匯款，卻呆等半個月都未有回應，阿文向同學訴苦後被譏受騙，一上網搜尋「發現外國及本港多個足球講壇均有人提及受到欺詐電郵，才確定「中招」。

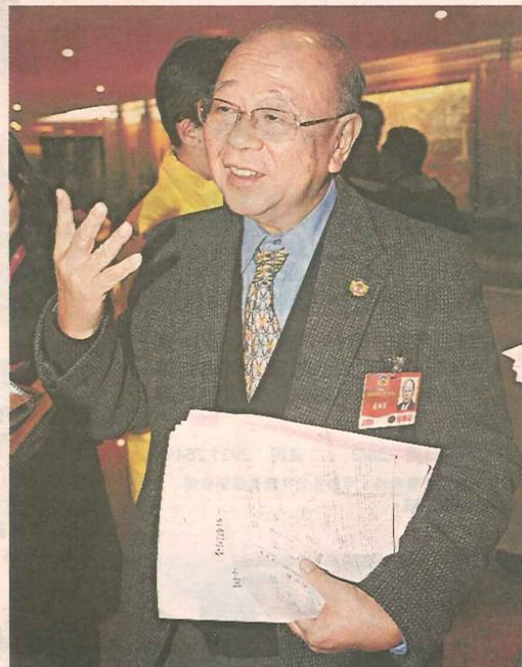
「騙子喺外國，想追都追唔到，我癩到唔敢同屋企人講。」阿文其後在討論區認識了另一名同樣被騙的球迷Hugo。Hugo去年更發現自己的電郵、足球網的帳戶均被人盜用，並懷疑有人利用他的帳戶散播病毒及含有病毒的網址。不過二人事後均沒有報警。

警方指去年共接獲約一千五百宗科技罪案，較前年增升九成，單是非法進入電腦系統案件已有四百四十一宗，較前年四十六宗勁升逾八倍。而網上商業騙案主要涉及拍賣，包括收不到貨款或付款後收不到貨物。警方科技罪案組亦特別增加人手至七十一人，打擊有關罪行。

### 借國際大事節日杜撰

曾在美國從事電腦保安工作的世維電腦公司負責人蔣光偉，歸納詐騙電郵特色，是多根據國際大事或節日，杜撰內容圖增加真實感。他指近期最為流行的四大主題，包括訛稱為海地籌款、世界盃門券中獎，又或者像前民政事務局長藍鴻震及聖雅各福群會企業拓展經理陳炳麟般，遭盜用電郵並訛稱外遊失竊騙取金錢，以及以高價向事主購買電子產品，圖騙取物品。

蔣光偉提醒網民，多留意詐欺電多來自尼日尼亞，且英文不通順或文法有誤，應切記不可向第三者透露帳戶密碼等私人資料。



■ 藍鴻震的電郵早前被不法份子盜用。



■ 近年網上罪案飆升，市民使用互聯網時須小心。



# IS INCIDENTS



## Facebook再現惡意攻擊 成最危險的社交網站

吳明宜/編譯

2010/06/4 下午3:08

Facebook用戶出現點擊綁架(clickjacking)攻擊，被誘使的人將協助攻擊散佈。

「數萬網友遭到社交工程技倆所騙，而使得點擊綁架蠕蟲周末期間在Facebook上快速蔓延，」Sophos資深技術顧問Gramham Cluley在部落格上說道。

點擊綁架蠕蟲又被稱為likejacking（按了「讚」後被綁架），它向Facebook用戶散佈像是「女生在警方讀取了她的動態後遭到逮捕」或「女生因穿著花俏而不准上學校」等垃圾郵件訊息。

點選網頁後，使用者就會連到空白頁，上面只「續」。但由於有個「隱形的iFrame」，點選該頁上散播攻擊內容及連結。「本月稍早我們我們Cluley說。Fbhole也會透過Facebook動態頁散

SophosLabs惡意程式研究中心首席技術工程師中毒，可採兩步驟解決。首先，將該頁自「喜」的動態頁上刪除該頁，它還是會留在「最近動到。」



www.mingpao.com, 更新日期: Friday, 7 January, 2011

明報新聞網

## 黑客侵電腦增六成見新高

【明報專訊】隨着愈來愈多人使用智能手機及社交網站facebook，黑客入侵個案數字上升至近年新高。香港電腦保安事故協調中心表示，去年收到382宗黑客入侵報告，比前年大幅增加六成，釣魚網站舉報亦較前年增逾一成。中心經理古煒德建議，市民在使用互聯網時要加強保安意識。

香港電腦保安事故協調中心表示，去年收到382宗黑客入侵報告，是近年新高，比前年增加六成，「釣魚」網站亦有上升趨勢，去年全年收到約300宗報告，較前年增加36宗，兩項數字均創新高。但電腦病毒方面則較去年減少，只有162宗。

智能手機facebook成攻擊目標

# IS INCIDENTS



## 涉攻擊港交所網站男子被捕



明報 - 2011年8月19日星期五下午10:40

警方於八月十日接到相關舉報，指港交所的網站遭受網絡攻擊。商業罪案調查科科技罪案組的探員進行深入調查，昨日拘捕該名男子，並檢獲17台電腦、兩部手提電話及5部數碼儲存裝置。

該名男子涉嫌「有犯罪或不誠實意圖而取用電腦」被拘捕，將會被通宵拘留調查。所檢獲的證物將會由電腦法理鑑證隊作進一步檢驗。

...

披露易網站是上星期三因為黑客入侵而出現故障，令投資者未能查閱上市公司的股價敏感資料，**7間公司下午停牌**。翌日亦有同類入侵事件，但被專家阻截，面停牌的公司亦已復牌。(即時新聞)



## 滙豐網絡「遇襲」服務大癱瘓

10 - 20 00:03

滙豐網上銀行被黑客攻擊，導致服務癱瘓數小時，英、美客戶亦受到影響。

綜合報道)(星島日報報道)滙豐全球多個網站遭黑客攻擊，影響的地區包括英國及美國等，本港網上理財服務亦一度無法使用，其後在本港時間昨日早上11點恢復正常。滙豐強調，並無客戶資料受到影響。金管局表示，滙豐已提交遭黑客攻擊相關報告。外電報道指，一個名為FawkesSecurity的黑客集團，自稱是此次攻擊的幕後黑手。

滙豐發言人表示，於英國時間10月18日，黑客通過大量訊息攻擊該行電腦系統，導致系統停止運作，令用戶無法使用網站的相關服務，滙豐全球部分網站受到影響。

滙豐全球多個網站在凌晨癱瘓，滙豐指，集團網站受到大規模阻斷服務的攻擊，令客戶不能登入網站使用網上理財，滙豐沒交代有多少客戶受影響，只強調網站被攻擊，不影響客戶數據。

...

# IS INCIDENTS



## 理大尋回USB 資料未外洩

[2009-10-17]



■理大表示，已尋回遺失的USB手指，並證實資料未有外洩。

【本報訊】理大一名研究助理早前於校內遺失一個電腦手指記憶體（USB），內涉由勞工及福利局委託進行的一項調查，牽涉2,666名市民的個人資料，包括身份證號碼、私人地址及電話等。理大昨日表示，遺失的USB手指已經尋回，並證實資料未有外洩。校方指已向警方及個人資料私隱專員公署報告有關事件，亦會成立獨立調查小組，檢討是次事件及處理個人資料的指引，以防止同類事件再度發生。

涉2666市民個人資料

...

## 港大失「手指」 洩 6800學生私隱



Apr 22, 2011

香港大學發生該校歷來最嚴重的資料外洩事件，社會科學院一名文員本周二違規將多份學生個人資料檔案下載到USB記憶體（俗稱「手指」），以便帶回家處理，卻於途中被人偷去，近6800名學生的個人資料外洩。港大已報警及通知個人資料私隱專員公署，並成立專責小組跟進調查，但兩日後才向傳媒公開事件。

涉違規帶回家 途中遇竊

...

# IS INCIDENTS



## 浸大發生洩漏個人資料事件

(明報)2009年6月2日 星期二

- 浸會大學一名職員處理聯招申請時，**不慎將附有190名申請人個人資料的電腦檔案，外傳給95名申請人。**
- 浸大已致電受影響同學致歉，並要求有關學生立即刪除檔案，又向個人資料私隱專員公署 報告，並成立調查小組調查，檢討加強個人資料處理程序，3個月內會完成調查報告。
- 浸大行政副校長李兆銓說，事件涉及一名負責英國 文學及英語教育學士課程的職員，他發電郵邀請申請人參加簡介會時犯錯，誤將其他申請人的姓名、身分證號碼、電郵、通訊地址、電話號碼，以及根據中學會考成績...



## 城大外洩數百學生私隱

21 Mar 2010 on.cc

- 城大科學及工程學院的學生近日透過協作教育中心申請 **Industrial Attachment scheme**的實習職位，向中心提供個人履歷資料，包括手提電話號碼、住址、緊急聯絡人姓名及電話號碼等，又列明自己的工作經驗及各學年的成績，以及希望申請的職位，校方會為學生轉介合適的實習職位。
- 至前日下午，數百名學生相繼收到**中心發出的電郵，內附數以百計學生及家長的個人敏感資料**，令學生極為詫異，事隔一小時，有中心職員透過電郵及電話知會學生，聲稱該郵件有毒，着學生不要打開，但在十分鐘後，中心又改稱系統出現問題，呼籲學生不要動用或傳閱有關個人資料，否則可能觸犯法例。
- 城大發言人表示，該中心因軟件出現問題而**錯誤在電郵上附有其他學生的資料**，校方發現後立即停止發放餘下的電郵，正調查事件，並會採取適當措施防止同類情況再次發生，亦會盡快將事件通知私隱專員公署。



# IS INCIDENTS



## 22機構網上泄3000個人資料 捷旅700客私隱任睇

2013-01-22 頭條

繼個人資料私隱專員公署早前揭發多間院校網站泄露個人資料後，本報在網上保安專家協助之下，以簡單的搜尋方法，便已發現多達22間來自各行各業的機構，於網上泄露逾3000名人士資料。

...

中大xxx29名學員的手機甚至個人電腦IP地址亦曝光，不法之徒可隨時盜用這些IP地址掩飾身分進行不法勾當。中心就事件致歉，並已聯絡網站設計公司立即移除有關資料，全面檢視後暫未發現其他資料外泄。發言人解釋，IP地址是有關人士提交網上表格時，由網站系統自動收集，中心無意收集和披露。

...



## 黑客入侵中大偷師生資料

2013年7月3日

【本報訊】繼早前「香港大學民意研究計劃」的電腦系統遭黑客入侵盜取敏感資料後，香港中文大學的網站昨亦發現遭黑客入侵，63名中大xxx系師生的個人資料被盜取後轉至境外網站。警方商業罪案調查科科技罪案組正追查黑客身份及動機，及事件與早前多宗黑客入侵洩密案是否有關。

被黑客入侵的中大xxx系網頁系統，主要供學生在網上遞交作業，而該校的其他學系網頁系統，校方經檢查後，暫未發現有被入侵。

被轉載至境外網站

警方商罪科探員昨晨在網上巡邏時，發現中大一個學系的網頁系統內有63名師生的個人資料，包括姓名、電郵地址、職員及學生編號、登入密碼，被轉載至另一境外網站，立即通知校方。警方初步調查，發現該網頁伺服器被人非法入侵，導致有關資料被盜取，將案件列「為有犯罪或不誠實意圖而取用電腦」。

警方稱正調查導致該學系資料被盜取的原因，並已提醒有關教育機構向個人資料私隱專員公署匯報事件及通知受影響人士。警方強調有關行為已觸犯《刑事罪行條例》，一經定罪，最高可被判處監禁5年。中大回應指，該學系已要求互聯網搜尋器移除有關搜尋項目。

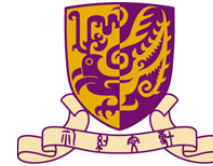
# IS INCIDENTS

## Lost of USB device:

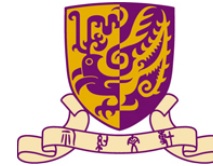
- A department staff reported that a USB was lost
- Information included: name, date of birth, HKID, phone number, address, family member's information & contact, etc. of patients
- Reported to PCPD

## Causes:

- Staff copied the information into a USB device for working at home
- The USB device was found disappeared
- Many records in the USB device are not encrypted



# IS INCIDENTS



## Personal Information leakage from a website:

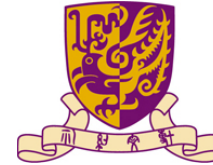
- PCPD contacted a department that personal information on their website was able to be searched from search engine
- The website of the department was developed by a outside vendor
- Use of the website: event registration for staff, student, & outside people
- Information collected: name, ID, e-mail, credit card number, etc.
- The incident was published in newspapers

## Causes:

- Staff download the registration records, these records were placed in a temporary folder which should be deleted immediately after the download
- No access right implemented to the temporary folder
- The temporary folder can be searched by the search engine

# IS INCIDENTS

## Website being hacked:



- HKPF found in the hacker site that a department's website was being hacked
- Hacker posted the personal information collected from the website in the hacker site
- The department's website was developed by a outside vendor
- Use of the website : for a project which will collect student's research topics
- Information collected: student's name, ID, e-mail, research topics, etc.
- The incident was published in newspaper

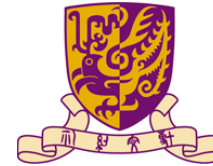
## Causes:

- Linux server which didn't install security patches for several years



# IS INCIDENTS

## Personal information leakage from a PPT file:

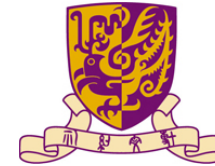


- PCPD received complaints that a site is leaking personal data
- A PowerPoint prepared by a presenter in a conference was uploaded to department's website
- Some charts in the PowerPoint are generated by an Excel data file embedded in the backend
- Information contains: patient's personal information

### Causes:

- The staff uploading the PowerPoint does not realized that the file contains personal data, and these applications can embed other applications in the backend

# IS INCIDENTS



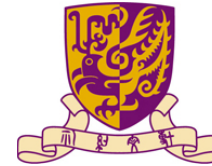
## Phishing e-mails:

- Many hackers send phishing e-mails to university members
- Purpose: steal account information, or other confidential information in the computers
- The phishing e-mails contains some executable attachments (e.g. \*.zip, \*.exe) or URL(links) in the e-mail
- Some systems were infected by some Trojan, also some abnormal network activities in the odd hours

## Causes:

- Victims may click on the URL, or double-click the attachment embedded in the phishing e-mail
- The URL or attachment embedded in the e-mail will immediately install some virus / Trojan to the computers when you open it
- These virus / Trojan cannot be detected by anti-virus program because:
  - The virus signature of the anti-virus program is not up-to-date
  - They are new virus(zero-day)
- The computers were not shutdown when not in use

# IS INCIDENTS

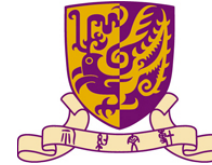


- **Involved parties**

- Incident reporter
- Data Source owner
- ITSC – Information Technology Services Centre
- PDCC – Personal Data Controlling Committee
- SEC, CPR
- AAPC – Administrative & Planning Committee
- PCPD – The Office of Privacy Commissioner for Personal Data
- The Hong Kong Police Force
- Funding Source

# IS INCIDENTS

## Incident Reporting and Handling



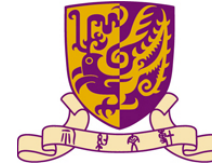
1. Submit Incident Reporting Form to [dir-itsc@cuhk.edu.hk](mailto:dir-itsc@cuhk.edu.hk) or [infosec@cuhk.edu.hk](mailto:infosec@cuhk.edu.hk) and PDCC (<http://www.cuhk.edu.hk/itsc/security/isreport/index.html>)
2. ITSC will help to evaluate the incident and do investigation.
3. PDCC convener may call up an ad-hoc meeting to review the incident, assess the impacts and risks, discuss remedial actions, prepare press release etc.
4. Reporting party may need to report to the Hong Kong Police Force and setup all necessary remedial actions.
5. PDCC may report the incidents to AAPC and the Office of Privacy Commissioner for Personal Data.
6. CPR will prepare script for press enquiry.



# IS INCIDENTS

- **Remedial actions**

- Contact impacted individual data subjects
- Setup Telephone hotline and Voice Mail
- Post the incident in departmental website
- Send email to notify incident happening and express apologies.
- Staff disciplinary actions



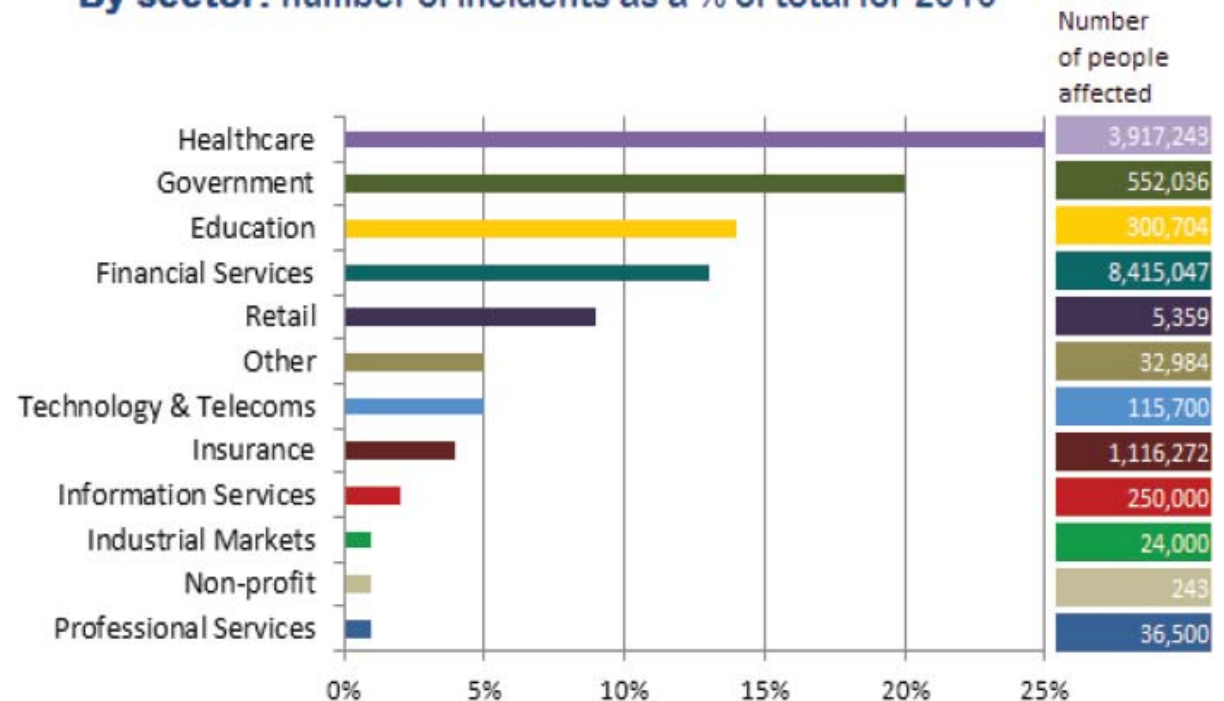
# STATISTICS ON DATA LEAKAGE



22

# STATISTICS ON DATA LEAKAGE

By sector: number of incidents as a % of total for 2010



Source: KPMB International. October 2010

## Why Universities?

- Hacking for challenge/ **fun**  
(external and student hackers / professional and script kiddies)
- Universities' computers - a great candidate for **zombie** machines
- Relatively **weak** security perimeter
- **Enormous** personal information
- **Valuable** research data

# Main Causes of Data Leakage

- **Classified as 4 types :**
  - Negligence cause
  - Phishing e-mail / website
  - Password stolen
  - Hacking / compromise



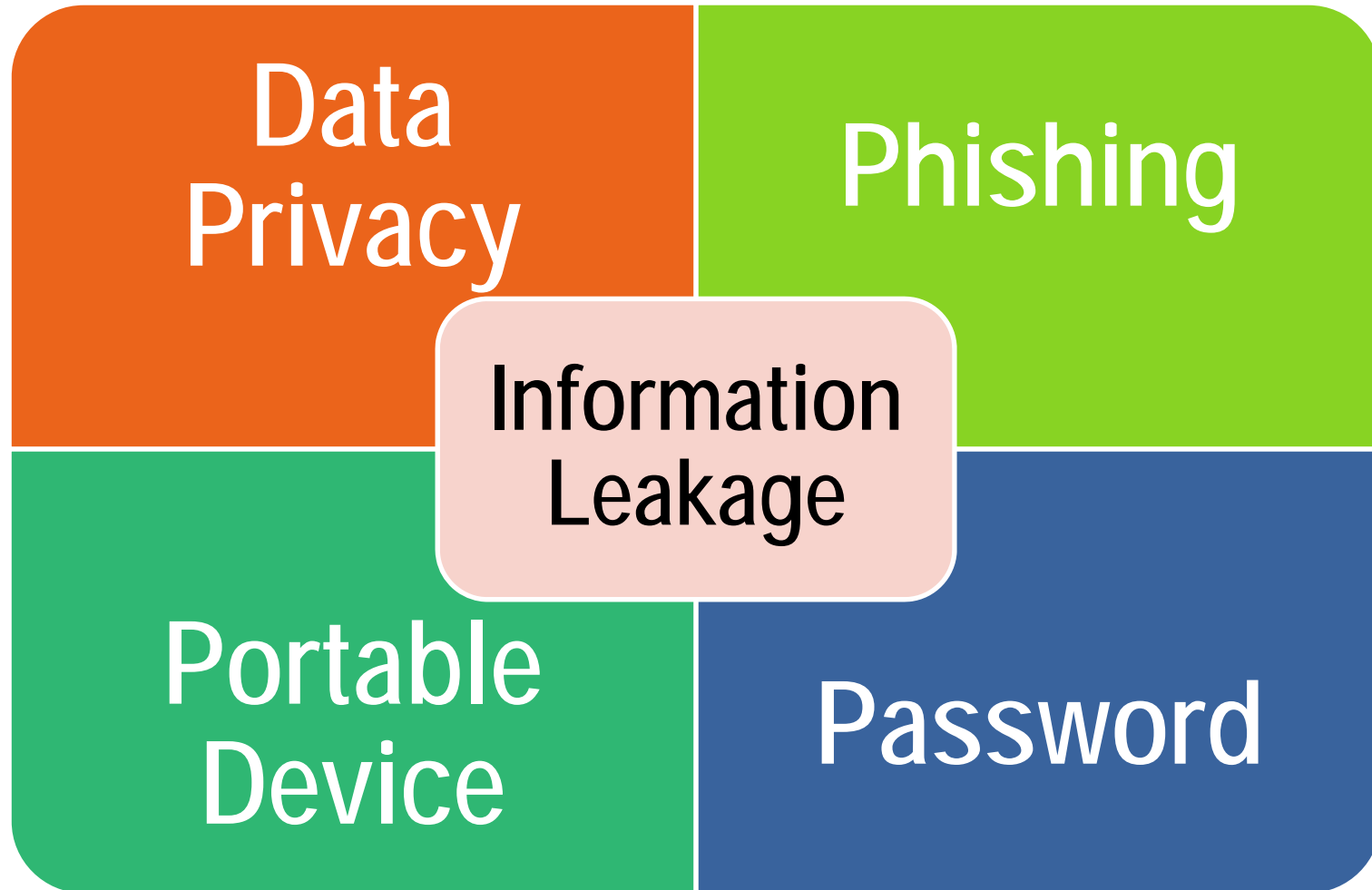
# 4Ps to REMEMBER!



25



# 4Ps



# 4Ps – EASY TO REMEMBER

Phishing

Password

Data  
Privacy

Portable  
device

Properly

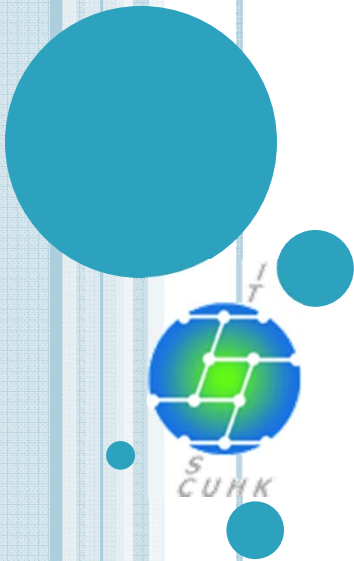
Protect

Personal

Property

**P**roperly **P**rotect your **P**ersonal **P**roperty

# 1. DATA PRIVACY



# Personal Data (Privacy) Ordinance



- Brought into force on 20 December 1996.
- Protect the privacy interests of living individuals' personal data.
- Controls the collection, holding, processing or use of personal data.
  
- Amendments of the Personal Data (Privacy) Ordinance relating to direct marketing and the legal assistance scheme take effect from 1 April 2013.
- Data user is required to take specified action before using personal data in direct marketing and data user must not use or provide personal data to others for use in direct marketing without data subject's consent or indication of no objection.

# DATA PRIVACY COMPLIANCE IN CUHK



- Policy in protection of personal data (privacy) - Personal Data Controlling Committee of CUHK (保障個人資料 (私隱) 政策 - 個人資料管理委員會)
  - All staff members and students of the University who handle **identifiable personal data** should take extra precaution to ensure that the **relevant laws on personal data (privacy)** and **University Guidelines are complied** with and that effective security measures are adopted to **protect personal and sensitive data** concerning a wide spectrum of data subjects such as staff, students, alumni, patients, clients, donors, job applicants and other data subjects involved in research/experiments/surveys
  - 所有教職員和同學處理可供**辨認的個人資料**時務須提高警惕，確切遵守有關**個人資料 (私隱)**的法例和**大學的指引**，並採取有效的保安措施，確保**個人及敏感資料**受到保障，當中包括教職員、學生、校友、病人、服務對象、捐款者、職位申請人、以及研究、實驗及調查所涉及的資料當事人的資料。
- <http://www.cuhk.edu.hk/policy/pdo/en/>



# DATA PRIVACY COMPLIANCE IN CUHK



- The University's Guidelines in Protection of Personal Data (Privacy) - 6 Data Protection Principles
  - Principle 2 - Accuracy and Duration of Retention - personal data should be accurate, up-to-date and **kept no longer than necessary**.
  - Principle 3 - Use of Personal Data - personal data should be **used for the purposes for which they were collected or a directly related purpose**.
  - Principle 4 - Security of Personal Data - **appropriate security measures** to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).



# DATA PRIVACY COMPLIANCE IN CUHK



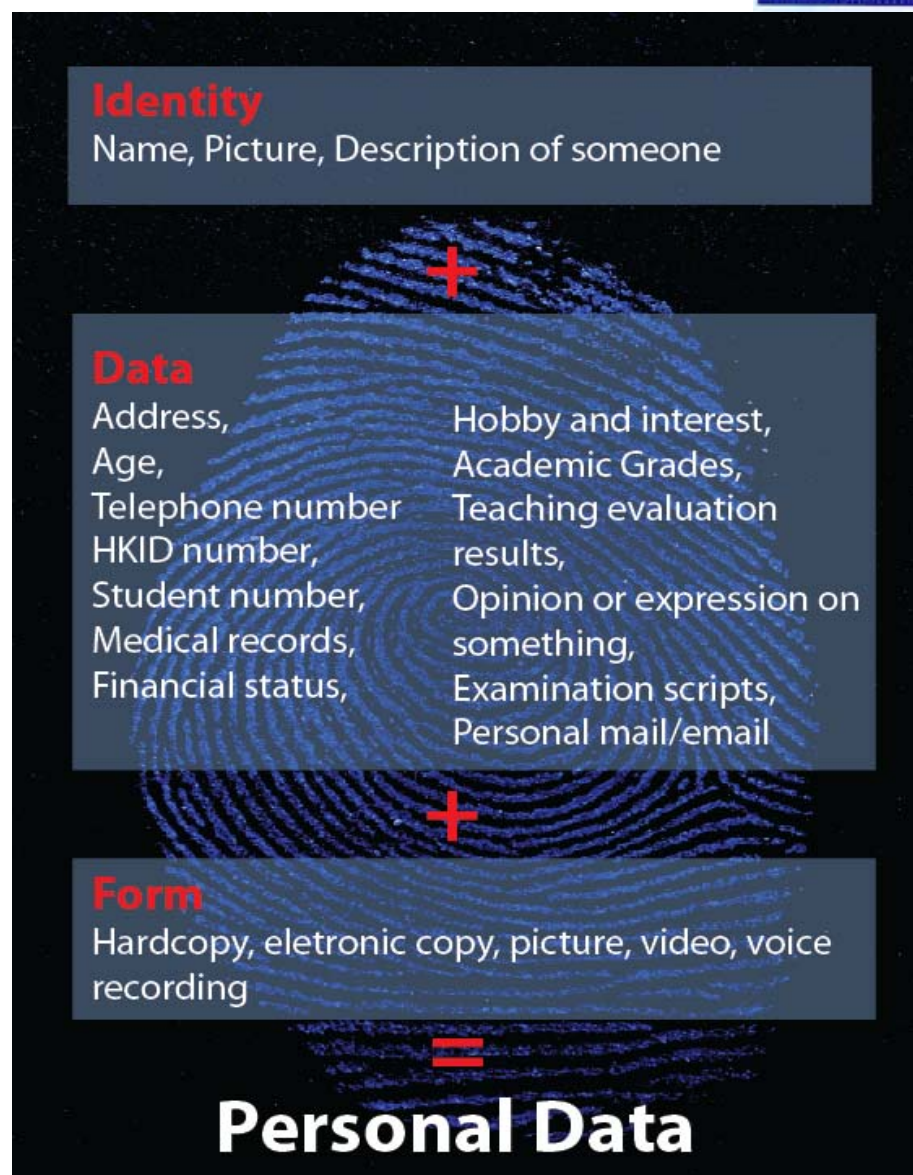
- Principle 4 - Data should be **protected against unauthorized or accidental access, processing**, erasure or other use having particular regard to:
  - Access (physical or logical)
  - Transfer
  - Process
  - Storage:
    - Physical location
    - Security measure



# DATA PRIVACY COMPLIANCE IN CUHK



## ○ What is Personal Data?

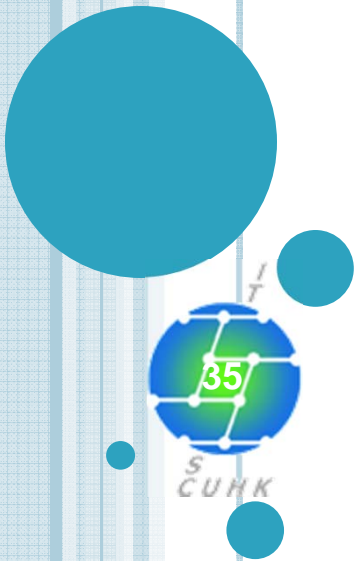


# DATA PRIVACY COMPLIANCE IN CUHK



- Please take extra care and possible security measure when you are handling personal data!!!

## 2. PHISHING





# PHISHING



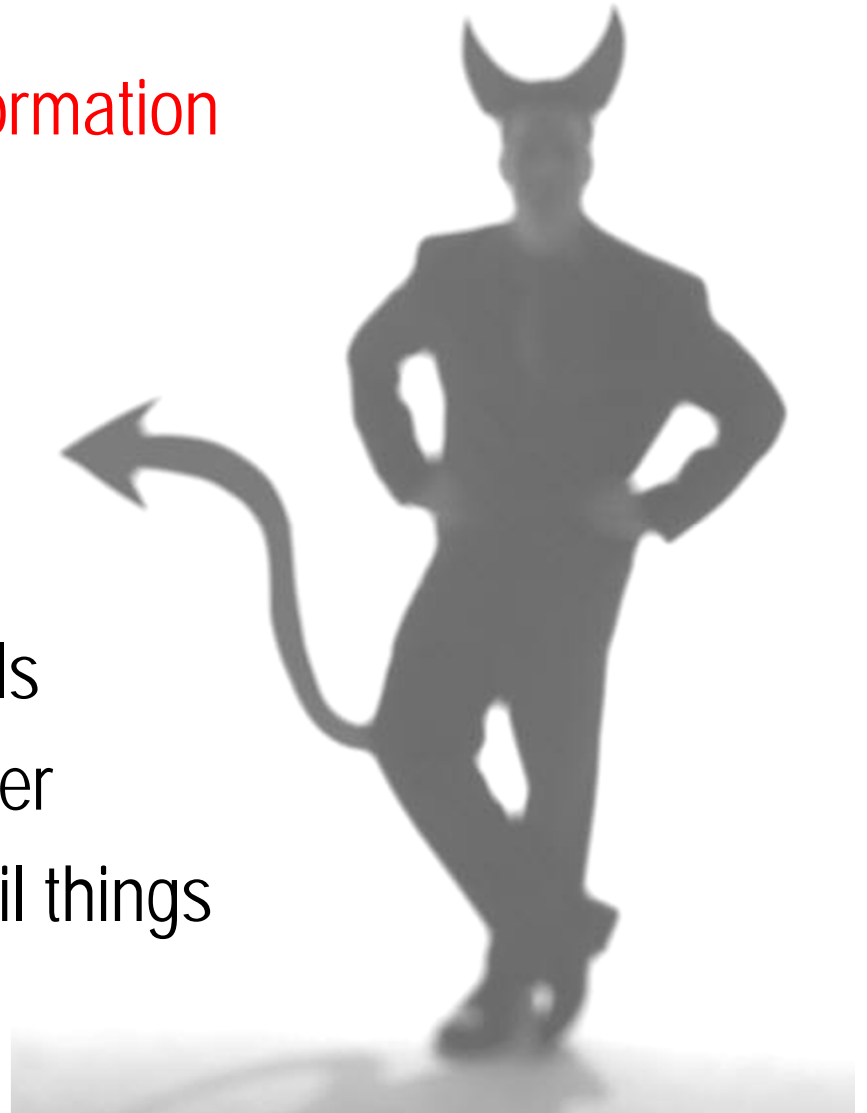
- Phishing / Fraud E-mail
- Phishing Website



# PHISHING



- Aim:
  - To steal / collect **private information**
- Purpose:
  - For sale
  - For stealing your money
  - For sending phishing e-mails
  - For controlling your computer
  - For doing other illegal or evil things



# PHISHING EMAIL



- Tactics:
  - Use legitimate email's look and feel
  - Embedded with a hyperlink which will redirect you to a phishing website
  - Embedded with an attachment which contains virus
  - Tempt you to reply
  - Claim to be urgent

# PHISHING EMAIL



## How to differentiate?

- Key phrases:

- "Verify your account."
- "You have won the lottery."
- "If you don't respond with 48 hours, your account will be closed."
- "To unsubscribe, click here..."



- Reply address is different from sender's.
- Doubtful link / attachment embedded.

**URGENT**

# PHISHING EMAIL



Update Your Email Account Now!!! - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

SnagIt Window

Extra line breaks in this message were removed.

From: THE CUHK.EDU.HK SUPPORT TEAM [helpdesk@cuhk.edu.hk] Sent: Mon 11/8/2008 17:48  
To: undisclosed-recipients  
Cc:  
Subject: Update Your Email Account Now!!!

Dear cuhk.edu.hk Subscriber,

We are currently carrying-out a mentainace process to your cuhk.edu.hk account, to complete this process you must reply to this email immediately,Your email address here (\*\*\*\*\*) and enter your password here (\*\*\*\*\*) if you are the rightful owner of this account.

Reply to Email: spamalertofficer1@gmail.com

This process we help us to fight against spam mails.  
Failure to summit your password, will render your email address in-active from our database.

---

NOTE: You will be send a password reset messenge in next seven (7) working days after undergoing this process for security reasons.

Thank you for using cuhk.edu.hk!  
THE CUHK.EDU.HK SUPPORT TEAM



# PHISHING EMAIL



- Reply address is different from sender's

RE: Update Your Email Account Now!!! - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

Send [Icons] [Dropdown] [Dropdown] A B I U [List Icons]

SnagIt [Icon] Window [Dropdown]

To: spamalertofficer1@gmail.com

Cc:

Subject: RE: Update Your Email Account Now!!!

-----Original Message-----  
From: THE CUHK.EDU.HK SUPPORT TEAM [mailto:helpdesk@cuhk.edu.hk]  
Sent: Monday, August 11, 2008 5:48 PM  
To: undisclosed-recipients  
Subject: Update Your Email Account Now!!!

Dear cuhk.edu.hk Subscriber,

We are currently carrying-out a maintainace process to your cuhk.edu.hk account, to complete this process you must reply to this email immediately,Your email address here (\*\*\*\*\*) and enter your password here (\*\*\*\*\*) if you are the rightful owner of this account.

Reply to Email: spamalertofficer1@gmail.com

This process we help us to fight against spam mails.  
Failure to summit your password, will render your email address in-active from our database.

# PHISHING EMAIL



- When you receive a similar suspected e-mail, you should:
  - **NEVER** reply any information to the e-mail.
  - **NEVER** click on any hyperlink in the e-mail.
  - **NEVER** open (double-click) on any attachment in the e-mail.
  - **Check** whether it is a reported case through our page on Phishing: <http://www.cuhk.edu.hk/itsc/network/app/email/phishing.html>
  - **Report** to ITSC at [infosec@cuhk.edu.hk](mailto:infosec@cuhk.edu.hk) if it is a new case.
  - **Delete** the e-mail.

**ITSC and CUHK**

**NEVER**

**ask for your PASSWORD**

# PHISHING WEBSITE



- Tactics:
  - Embedded a link in a phishing e-mail
  - Use legitimate webpage's look and feel
  - Embedded and install virus, trojan, or malicious software

# PHISHING WEBSITE



- Doubtful link embedded

Account Update - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W) | [Print] [New] [Reply] [Forward] [Close] [Up]

寄件者: Chinese University of Hong Kong [secureteam@cuhk.edu.hk]  
收件者: undisclosed-recipients  
副本:  
主旨: Account Update

Attention Member,

Please click on below link to update your Email account.

<http://webmail.cuhk.edu.hk/>

Chinese University of Hong Kong

blocked::http://www.1025.ru/js/webmail.cuhk.edu.hk/

# PHISHING WEBSITE




- This is the phishing webpage

A screenshot of a phishing website for CUHK WebMail. The browser address bar shows the URL http://www.1025.ru/js/webmail.cuhk.edu.hk/. The page features the CUHK logo and the text 'WEBM@IL A Web Interface to the CWEM System'. A login form is centered on the page with fields for 'Computing ID', 'CWEM Password', and a 'Language' dropdown menu set to 'English (US)'. A 'Log in' button is below the form. Below the login form, there is a 'CADS' logo and the text '(CADS Reference Number: 041)'. A warning message reads: 'Beware of Phishing E-mail! ITSC or CUHK never ask for your account and/or personal information through e-mail. Check out more information at http://www.cuhk.edu.hk/itsc/network/app/email/phishing.html.' Below this, there are links for 'Usage Tips: Forgot your CWEM Password?' and 'Next Maintenance Sessions: Check http://www.cuhk.edu.hk/itsc/sys\_ava/outage.html'. At the bottom, there is a 'Need Help?' section with links to the User Manual and the ITSC Electronic Helpdesk. The page number '45' is visible in the bottom right corner.

Mail :: Welcome to CUHK... x

http://www.1025.ru/js/webmail.cuhk.edu.hk/

 **WEBM@IL**  
A Web Interface to the CWEM System

No e-mail in INBOX but still prompting Quota exceeded?  
ITSC or CUHK never ask for your account and/or personal information through e-mail

**Welcome to CUHK WebMail**

Computing ID

CWEM Password

Language

**CADS**  
(CADS Reference Number: 041)

**Beware of Phishing E-mail! ITSC or CUHK never ask for your account and/or personal information through e-mail.**  
Check out more information at <http://www.cuhk.edu.hk/itsc/network/app/email/phishing.html>.

**Usage Tips:** [Forgot your CWEM Password?](#)

**Next Maintenance Sessions:** Check [http://www.cuhk.edu.hk/itsc/sys\\_ava/outage.html](http://www.cuhk.edu.hk/itsc/sys_ava/outage.html)

**Need Help?**

You can browse the User Manual **NET105 Access to the CUHK WebMail System** in [English](#) and [Chinese](#).

For comments and enquiries about the CUHK WebMail system, please write to the ITSC Electronic Helpdesk at <https://helpdesk.itsc.cuhk.edu.hk/group/postmaster>.

Copyright © 2008 Information Technology Services Centre, The Chinese University of Hong Kong.  
CUHK WebMail is developed based on the IMP Webmail Client

45

# PHISHING WEBSITE



- This is the legitimate webpage


Mail :: Welcome to CUHK WebMail - Windows Internet Explorer

https://webmail.cuhk.edu.hk/login.php?new\_lang=en\_GB

File Edit View Favorites Tools Help

Google 搜尋 分享 網頁註解 拼字檢查 翻譯 自動填入

Mail :: Welcome to CUHK WebMail

 **WEBM@IL**  
A Web Interface to the CWEM System


No e-mail in INBOX but still prompting Qu  
ITSC or CUHK never ask for your account and/or personal information

**Welcome to CUHK WebMail**

Computing ID

CWEM Password

Language

  
(CADS Reference Number: 041)

Beware of Phishing E-mail! ITSC or CUHK never ask for your account and/or personal information through e-mail. Check out more information at <http://www.cuhk.edu.hk/itsc/network/app/emails/phishing.html>.

**Usage Tips:** Forgot your CWEM Password?

**Next Maintenance Sessions:** Check [http://www.cuhk.edu.hk/itsc/sys\\_ava/outage.html](http://www.cuhk.edu.hk/itsc/sys_ava/outage.html)

**Need Help?**

You can browse the User Manual **NET105 Access to the CUHK WebMail System** in English and Chinese.

For comments and enquiries about the CUHK WebMail system, please write to the ITSC Electronic Helpdesk  
at <https://helpdesk.itsc.cuhk.edu.hk/group/postmaster>.

Copyright © 2008 Information Technology Services Centre, The Chinese University of Hong Kong.  
CUHK WebMail is developed based on the IMP Webmail Client

46



# PHISHING WEBSITE



- Tips to prevent phishing website
  - **DO NOT click** the link provided in the e-mail or provide personal data to the e-mail or website.
  - **Reset** your password **IMMEDIATELY** in case you have input your account information to the phishing website.
  - **Verify** digital certificate.
  - **Use SSL (https://)** when browsing any website that may process sensitive data.
  - **Enable** anti-phishing website function.

# PHISHING WEBSITE



## ○ Verify Digital Certificate

- A lock
- https://

The screenshot shows a Windows Internet Explorer browser window with the title "個人網上理財 - 香港匯豐 - Windows Internet Explorer". The address bar contains a long, complex URL starting with "https://www.ebanking.hsbc.com.hk/1/2/!ut/p/kcxml/04\_Sj9SPykssy0xPLMnMz0vM0Y\_QjzKLN443NjECSZnFm8Ybm-". A red box highlights the "https://" part of the URL. The page content includes the HSBC logo and a navigation menu with items like "安全和保密的網上理財", "網上特別優惠", "系統提升時間表", and "常見問題". A digital certificate dialog box is open in the foreground, titled "憑證". It displays the following information:

- 憑證資訊**
- 這個憑證的使用目的如下:
  - 確保遠端電腦的識別
- \*請參照憑證授權敘述中的詳細資訊。\*
- 發給:** www.ebanking.hsbc.com.hk
- 發行者:** www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
- 有效期自 20/8/2008 到 21/8/2009

Buttons at the bottom of the dialog include "安裝憑證(I)...", "發行者聲明(S)", and "確定". A lock icon is visible in the top right corner of the browser window.

# PHISHING WEBSITE



Mail :: Welcome to CUHK WebMail - Windows Internet


https://webmail.cuhk.edu.hk/login.php?new\_lang=

File Edit View Favorites Tools Help

Google

Favorites Suggested Sites Free Hotmail

Mail :: Welcome to CUHK WebMail




**WEBM@IL**  
A Web Interface to the CWEL

Beware of Phishing  
<http://www.cuhk.edu.hk>

### Certificate

General Details Certification Path

 **Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer

\* Refer to the certification authority's statement for details.

**Issued to:** webmail.cuhk.edu.hk

**Issued by:** Hongkong Post e-Cert CA 1 - 10

**Valid from:** 3/16/2011 **to:** 3/30/2013

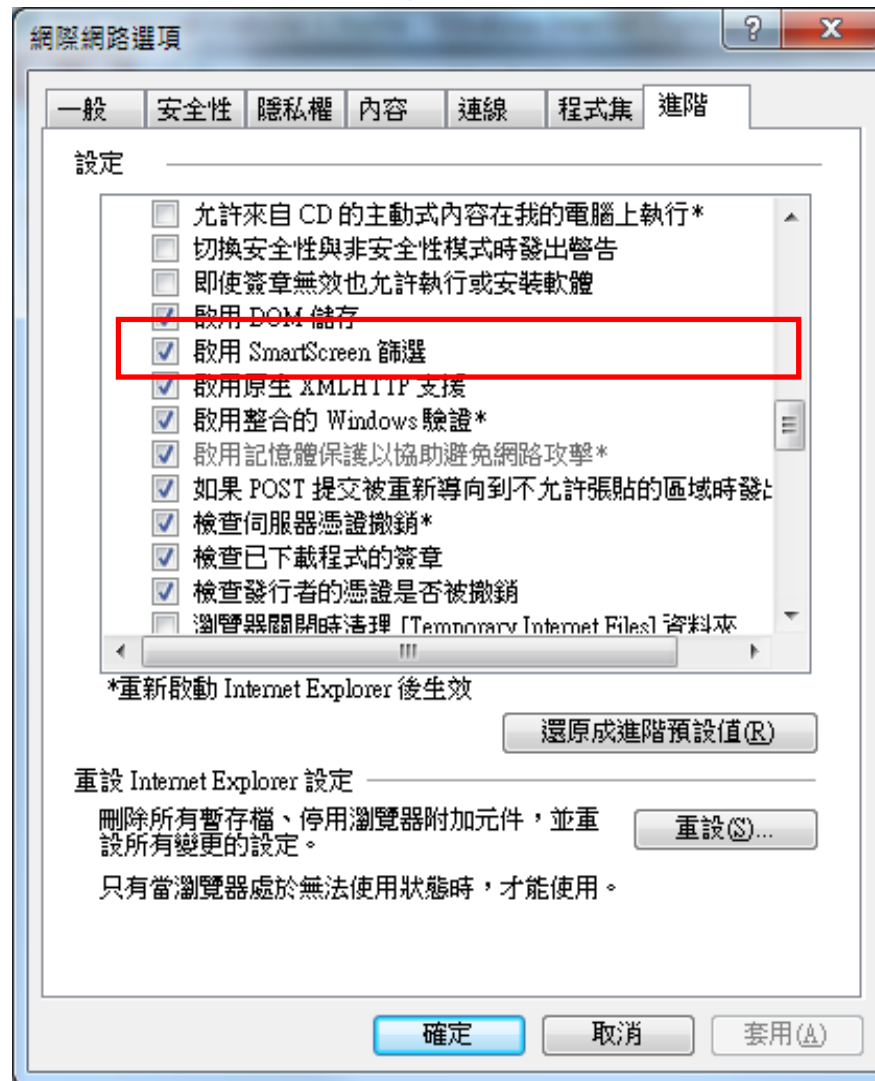
Install Certificate... Issuer Statement

OK

# PHISHING WEBSITE



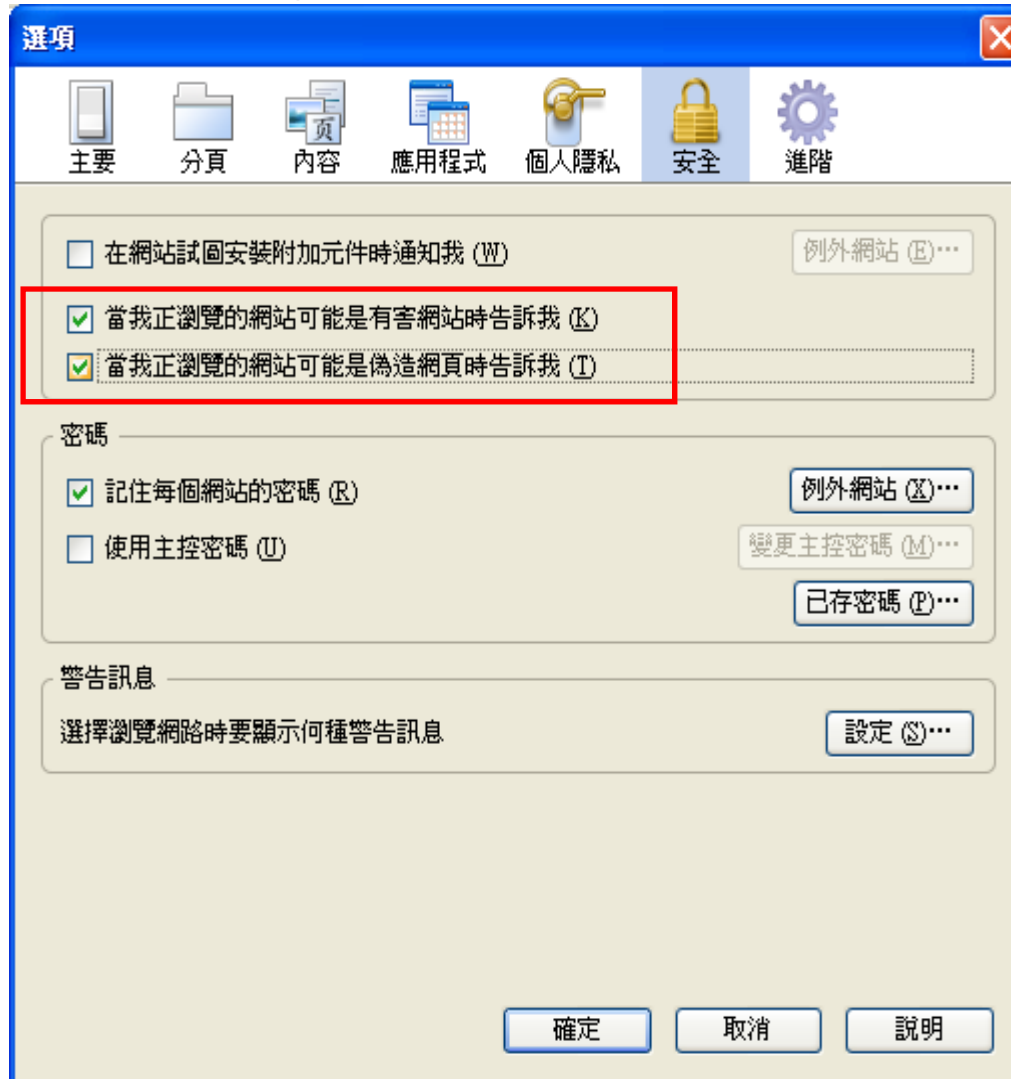
- Enable SmartScreen Filtering function in IE 8



# PHISHING WEBSITE



- Enable anti-phishing function in FireFox



# PHISHING WEBSITE



已知的有害網站！ - Mozilla Firefox

檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)

http://www.mozilla.com/firefox/its-an-attack.html

最常瀏覽的網站 新手上路 即時新聞

SiteAdvisor



## 已知的有害網站！

這個在 [www.mozilla.com](http://www.mozilla.com) 的網站已被回報是有害網站，依據你所選擇的安全設定予以阻擋。

有害網站會嘗試安裝能竊取隱私資訊、利用你的電腦攻擊他人或破壞作業系統等的惡意軟體到你的電腦上。

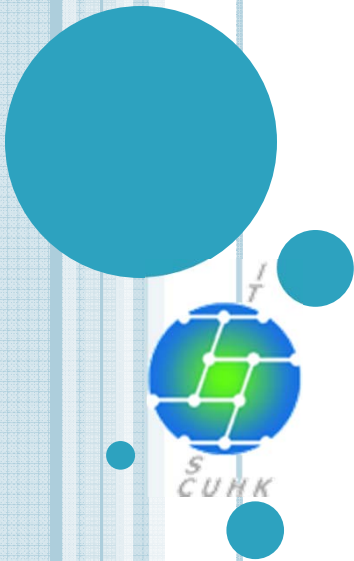
某些有害網站會故意安裝有害軟體到電腦上，但更多網站是在連網站擁有者都不知情的情況下，成為有害軟體散佈的溫床。

[帶我離開這裡！](#) [為什麼要封鎖此網站？](#)

忽略此警告



# 3. PORTABLE DEVICE



# PORTABLE DEVICE

- USB Storage Device
- Notebook
- Tablet
- Smart Phone
- ...



# PORTABLE DEVICE



## ○ Benefit

- Small size
- Large storage capability



## ○ Risk

- Easy to lose
- Unauthorized person can get enormous stored data in if no protection

# PORTABLE DEVICE

For USB storage device / Notebook

- Use Data encryption (Hardware)

- e.g. Stealth MXP USB device about \$2000 for 4GB
- e.g. Dell Latitude D630 Notebook about \$7500

- This solution is most convenient and fast but expensive



# PORTABLE DEVICE

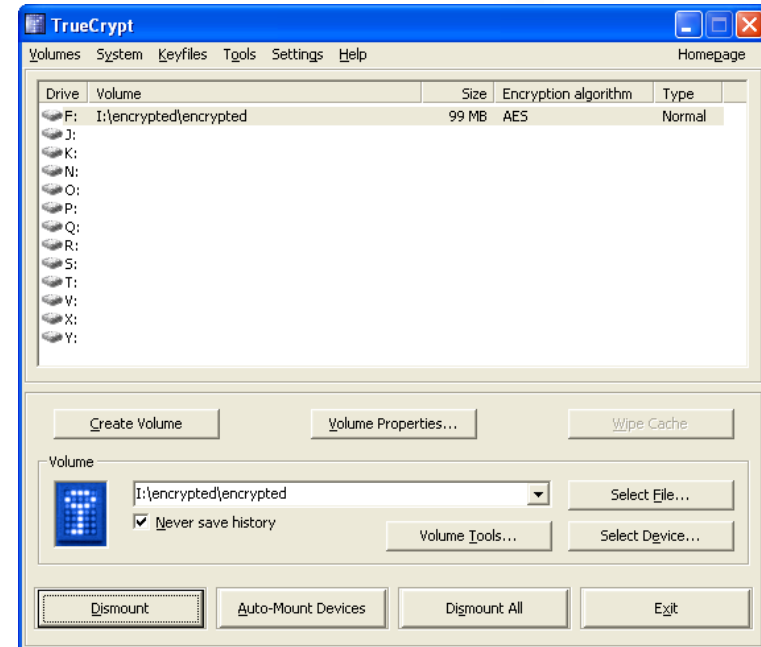


- Data encryption (Software)

- e.g. TrueCrypt

(<http://www.truecrypt.org/downloads.php>)

- e.g. BitLocker, Bundled in Win 7



- This is a cheaper but slower solution.

- It can be used for PC, notebook and storage device.

- It supports to encrypt entire partition, drive or storage device

# PORTABLE DEVICE



## For USB storage device / Notebook

- **DO NOT** store sensitive data into portable device.
- Store **minimal** data if storing into portable device is unavoidable.
- Take all necessary **security measure** to protect the data in the portable device, e.g. encryption, password, finger print ...
- Read guidelines in securely managing mobile computing devices and removable storage media (<http://www.cuhk.edu.hk/itsc/security/gpis/guide.html>).



# PORTABLE DEVICE

## For Smart Phones & Tablets



### ○ Lock Your Mobile Device

- Enable passcode
- Auto screen lock after a short period of inactivity

### ○ Use Secure Networks

- Turn off Wi-Fi, Bluetooth and location service when not use
- DO NOT connect to untrusted Wi-Fi networks
- DO NOT access personal data with public Wi-Fi networks
- Use secure network e.g. VPN

# PORTABLE DEVICE

## For Smart Phones & Tablets



### o Enjoy Safe Browsing

- Beware of suspicious link clicking and attachment from suspicious e-mail or text messages as they may contains virus
- Use SSL (<https://>) when browsing any website that may process sensitive data
- Beware of the Quick Response (QR) code you scan as it might links to a malicious website which may also contain virus



### o Protect Your Operating System (OS)

- DO NOT jailbreak or root the device
- Keep the OS updated
- Install anti-virus software

# PORTABLE DEVICE

## For Smart Phones & Tablets



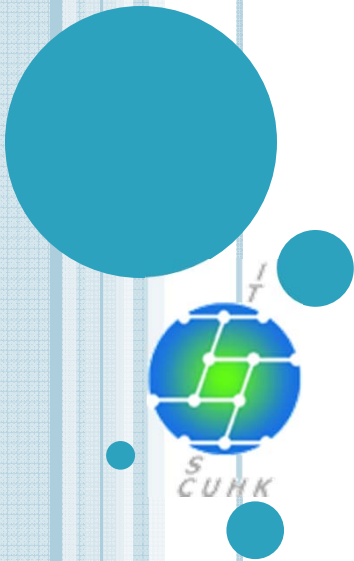
### ○ Mind Your Apps

- **DO NOT** download apps from untrustworthy sources
- **Review and update** apps regularly
- **Remove unused** apps

### ○ Protect Your Sensitive Data

- **Avoid storing** confidential / sensitive data
- **Encrypt** confidential / sensitive data
- **Back up** the data to another secure storage media regularly
- **Securely erase / wipe** all the data before discarding or selling your device
- **Report any lost or stolen** university-owned devices that contain sensitive or restricted data of the University to the Director of IT Services at [dir-itsc@cuhk.edu.hk](mailto:dir-itsc@cuhk.edu.hk)

# 4. PASSWORD



# PASSWORD



- **Strong password**

- at least 8 characters
- mix of random
  - mixed-case alphabetic characters
  - numerals, and
  - special characters (e.g. #, \$, !)

- **2 Factor Authentication**

# PASSWORD



- Use Strong Password

Number of Characters in Password	26 (lower case letters only - abc)	36 (lower case letters plus numbers - abc123)	52 (upper and lower case letters - AaBbCc)
5	1.98 minutes	10.1 minutes	1.06 hours
6	51.5 minutes	3.74 hours	13.7 days
7	22.3 hours	9.07 days	3.91 months
8	24.2 days	10.7 months	17.0 years
9	1.72 years	32.2 years	8.82 centuries



# PASSWORD



## WEAK

- 123456
- 91557730
- 20080801
- frankie

## STRONG

- p@trick1101
- We@rthch7730
- li08\_ly01

We are the champion + last 4 digit of mobile no.

lily births on 1<sup>st</sup> of August

# PASSWORD



<b>DO</b>	<ul style="list-style-type: none"><li>• Use strong password.</li><li>• Log off when finished using terminals or PCs in public areas.</li><li>• Change password frequently, e.g. 90 days.</li><li>• Change the default or initial password the first time you login.</li><li>• Beware of shoulder surfing.</li></ul>
<b>DON'T</b>	<ul style="list-style-type: none"><li>• Don't use dictionary words and personal related information as login name or password.</li><li>• Don't place your password conspicuously.</li><li>• Don't tell your passwords to other people.</li><li>• Don't store your password on any media unless it's protected from unauthorized access.</li><li>• Don't use the same password for everything.</li><li>• Don't reuse recently used password.</li><li>• Avoid using the "remember your password" feature.</li></ul>

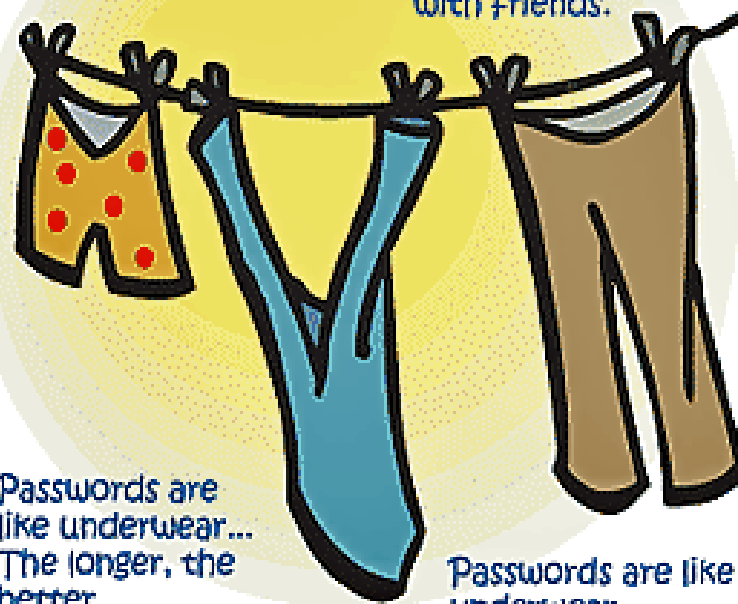
# PASSWORD



## Passwords Are Like Underwear

Passwords are like underwear...  
Change yours often.

Passwords are like underwear...  
Don't share them  
with friends.



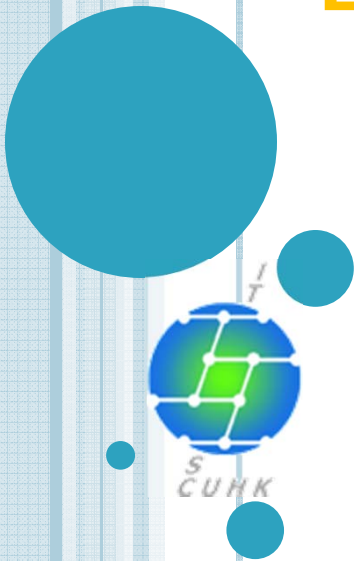
Passwords are  
like underwear...  
The longer, the  
better.

Passwords are like  
underwear...  
Be mysterious.

Passwords are like  
underwear...  
Don't leave yours  
lying around.

Helpful  
Tips

# MORE TIPS ON PREVENTING DATA LEAKAGE





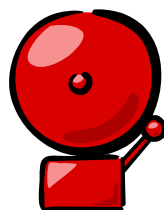
# TIPS ON PREVENTING DATA LEAKAGE

- Your Awareness



- Report IS incidents

- In case of leakage confidential information in electronic format, report it immediately to [infosec@cuhk.edu.hk](mailto:infosec@cuhk.edu.hk).
- Details can be found at <http://www.cuhk.edu.hk/itsc/security/isreport>.





# TIPS ON PREVENTING DATA LEAKAGE

- Proper disposal - hardware
  - Zero-filled (<http://www.seagate.com/support/disc/...s/discwiz.html>).
  - Data Purging (<http://dban.sourceforge.net/>).
  - Degaussing the devices.
  - Physically destroying them, or by using a data cleaner to erase data inside.
- Proper disposal - hardcopy
  - Use paper shredder.



# TIPS ON PREVENTING DATA LEAKAGE

- Media maintenance
  - Buy device which supports hardware data encryption.
  - Remove hard disk before repairing.
  - Clean up hard disk.
- Third-party management
  - Sign Non-Disclosure Agreement (NDA).





# GUIDELINES FOR SECURELY CONFIGURING YOUR COMPUTERS

Guideline	Done
1. Follow the University Software Standards	
2. Install anti-virus software – Kaspersky ( <a href="http://www.cuhk.edu.hk/itsc/security/antivirus/index.html">http://www.cuhk.edu.hk/itsc/security/antivirus/index.html</a> )	
3. Update latest virus signatures for the anti-virus software	
4. Perform regular scanning, e.g. full scan, on your computer	
5. Turn on personal firewall	
6. Update Windows and update latest patches	
7. Set strong passwords	
8. Separate user accounts with no admin right in a shared computer	
9. Disconnection from the Internet when it is not in use, i.e. shutdown	
10. Further suggestion.	

<http://www.cuhk.edu.hk/itsc/security/protectpc/index.html>

# DOs CHECKLIST FOR PROTECTING YOUR DIGITAL DATA



1. Use encryption to protect confidential data.
2. Use strong password, keep them private and change regularly.
3. Beware of suspicious e-mails.
4. Configure your computer securely.
5. Backup important data and test the backup regularly.
6. Activate password protection for unattended computing devices, e.g. screensaver.
7. Run a VPN connection over CUHK Wi-Fi connection.
8. Turn off unnecessary wireless connections.
9. Observe and comply with the "Data Protection Principles".
10. Report information security incident immediately.



# Security Tips while Travelling Abroad

- DO NOT connect to untrusted Wi-Fi networks.
- DO NOT access personal data with public Wi-Fi networks.
- Use ONLY your own personal computer to access any system / website that require your passwords.
  - Enable a secure network connection, e.g. VPN.
  - Use SSL (<https://>) when browsing any website that may process sensitive data.

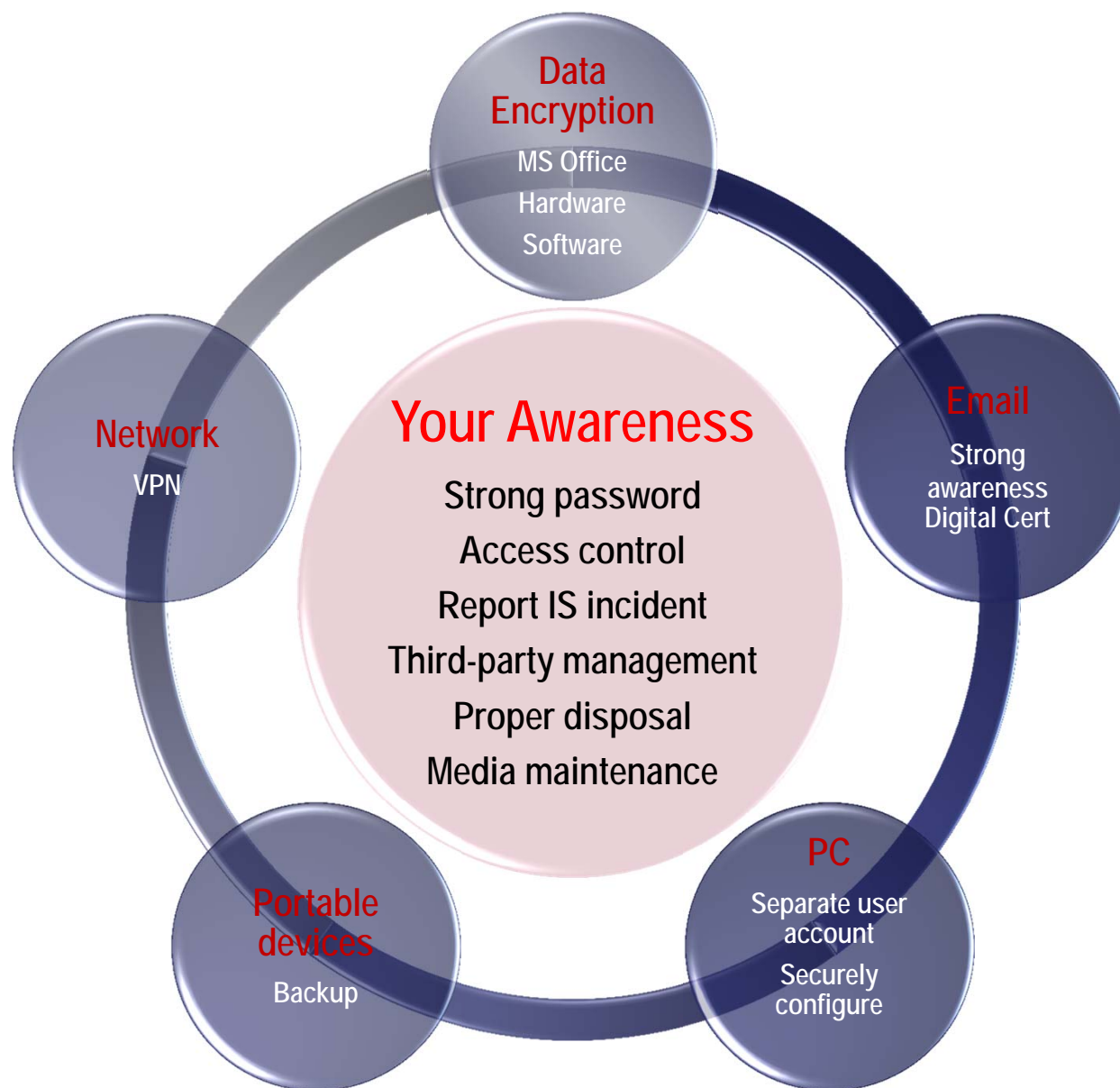


# Security Tips while Travelling Abroad

- Be cautious when using public computers
  - Use public computers **for casual browsing ONLY**.
  - Public computers are insecure, they might have been compromised by virus or malware.
  - **DO NOT enter** passwords and any personal data.
  - **DO NOT access** CUHK IT systems, e.g. CUHK VPN, CUSIS, CWEM, eLearning, Staff Self-Service Enquiry System, etc. to avoid private information and CWEM password leakage.



# TIPS ON PREVENTING DATA LEAKAGE





# MORE INFORMATION ...

- For General User (<http://www.cuhk.edu.hk/itsc/security/gpis/index.html>)
  - Keep your Data out of Hackers' Reach!
  - Be Alert to the Email Attachment You Received
  - Computer Security Tips While Traveling Abroad
  - The DOs & DONT's checklist for protecting your digital data
  - Guidelines for securely configuring your computers (home and office)
  - Security Guidelines for Smart Phones and Tablets
  - Guidelines to Secure USB Devices
  - Guidelines for securely managing mobile computing devices and removable storage media
  - Guidelines for setting a strong password
  - Good practice in using Internet
- For IT Professional (<http://www.cuhk.edu.hk/itsc/security/restricted/isgptech/index.html>)
- Alert, News and Events
- Useful tools and link



# MORE INFORMATION ...

- Visit <http://www.cuhk.edu.hk/itsc/security>

The screenshot shows the website for the Information Technology Services Centre at The Chinese University of Hong Kong. The browser address bar displays <http://www.cuhk.edu.hk/itsc/index-en.html>. The website header includes navigation links for Home, Site Index, Policies and Guidelines, and Contact Us, along with a search bar for ITSC. The main navigation menu lists various services such as About Us, Accounts, Applications, Departmental IT, Information Security, Network Services, Research & Teaching, and User Areas. A 'Useful Links' dropdown menu is open, listing categories like Alerts, News and Events, Good Practices for General Users, LAN Admin Resources, and Information Security Policies. On the left, a 'What's New' section features news items from September and August, including a phishing alert. A prominent banner advertises 'Install Free Anti-Virus Software for Your PC' with a 'Learn More' button. Other sections include 'Network Connection @ Student Hostels' and a note about accessing 2012-13 course sites via MyCUHK.





THANK YOU.