Information Security and Protection of Personal Data & Privacy

- Incidents Sharing & Tips on Data Protection

Prepared by:
Information Security Section (ISS),
Information Technology Services Centre (ITSC)
E-mail: infosec@cuhk.edu.hk
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
IS INCIDENTS

8 Feb 09

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的英雄盧永成。消防處表示，對殉職的英雄盧永成事件非常關注，會調查跟進。

6 Dec 09

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洩密 (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....
機場入境處電腦懷疑失竊

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.
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
• 医院管理局（医管局）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

稱可贏世界盃門券
電郵詐騙 多人「中招」

騙局處處有，今年新春特別多。農曆新年期間，有名人電郵被不法份子盜用，詐騙手法千變萬化， david@123.com 轉發至 several@456.com，收件人名稱為“恭喜賀年”，附上主題為“恭喜賀年”的附件，附件為一個偽造的下載連結。

【專家警示】

警方警告：

1. 不要輕信來電或電郵，特別是那些沒有姓名和電話號碼的来電或電郵。
2. 不要回覆任何來電或電郵，特別是那些要求提供個人資料的來電或電郵。
3. 不要點擊任何附有的連結或附件。
4. 保持警惕，對於不明來源的來電或電郵，先電話徵詢警方意見。
5. 安裝防詐騙軟體，並保持軟體更新。

警方提醒市民：

1. 不要輕信來電或電郵，特別是那些沒有姓名和電話號碼的來電或電郵。
2. 不要回覆任何來電或電郵，特別是那些要求提供個人資料的來電或電郵。
3. 不要點擊任何附有的連結或附件。
4. 保持警惕，對於不明來源的來電或電郵，先電話徵詢警方意見。
5. 安裝防詐騙軟體，並保持軟體更新。

警方同時呼籲：

1. 當收到來電或電郵時，要仔細核實來電或電郵的內容。
2. 如果有懷疑，應立即向警方報案。
3. 當出現詐騙情況時，應立即停止交易，並向警方報案。
4. 如果已經受騙，應立即報告給警方。
5. 安裝防詐騙軟體，並保持軟體更新。

警方提醒市民：

1. 不要輕信來電或電郵，特別是那些沒有姓名和電話號碼的來電或電郵。
2. 不要回覆任何來電或電郵，特別是那些要求提供個人資料的來電或電郵。
3. 不要點擊任何附有的連結或附件。
4. 保持警惕，對於不明來源的來電或電郵，先電話徵詢警方意見。
5. 安裝防詐騙軟體，並保持軟體更新。

警方同時呼籲：

1. 當收到來自不明來電或電郵時，要仔細核實來電或電郵的內容。
2. 如果有懷疑，應立即向警方報案。
3. 當出現詐騙情況時，應立即停止交易，並向警方報案。
4. 如果已經受騙，應立即報告給警方。
5. 安裝防詐騙軟體，並保持軟體更新。

警方提醒市民：

1. 不要輕信來電或電郵，特別是那些沒有姓名和電話號碼的來電或電郵。
2. 不要回覆任何來電或電郵，特別是那些要求提供個人資料的來電或電郵。
3. 不要點擊任何附有的連結或附件。
4. 保持警惕，對於不明來源的來電或電郵，先電話徵詢警方意見。
5. 安裝防詐騙軟體，並保持軟體更新。

警方同時呼籲：

1. 當收到來自不明來電或電郵時，要仔細核實來電或電郵的內容。
2. 如果有懷疑，應立即向警方報案。
3. 當出現詐騙情況時，應立即停止交易，並向警方報案。
4. 如果已經受騙，應立即報告給警方。
5. 安裝防詐騙軟體，並保持軟體更新。
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圍期間在Facebook上快速蔓延，」Sophos資深技術顧問Graham 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「女生在警方誘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，上面只有一個按鈕，但由於有個「隱形的iFrame」，點選該按鈕後也無法再看到攻擊內容及連結。「本月稍早我們我們的Cluley說。Fbhole也會透過Facebook動態頁散播，Sophos Labs惡意程式研究中心首席技術工程師表示，適用於和中毒，可採兩步驟解決。首先，將該頁自喜愛列表中移除，它還是會留在「最近動態」。

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

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，比上年大幅增加六成，並有機會接連數年增加。中心經理古偉德建議，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，比前年增加六成，「釣魚」網頁亦有上升趨勢，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
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部數碼儲存装置。

該名男子涉嫌「有犯罪或不誠實意圖而取用電子」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。

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滙豐行電腦系統，導致系統停止運作，令客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，滙豐及交存有多少客戶受影響，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。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

浸大發生泄漏個人資料事件
(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，聲稱該電郵有毒，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，否則可能觸犯刑例。

○ 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。
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。
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
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
**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
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 realize that the file contains personal data, and these applications can embed other applications in the backend
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
Incident Reporting and Handling

1. Submit Incident Reporting Form to dir-itsc@cuhk.edu.hk or 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.
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
STATISTICS ON DATA LEAKAGE

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

Source: KPMG International. October 2010
Main Causes of Data Leakage

- Classified as 4 types:
  - Negligence cause
  - Phishing e-mail / website
  - Password stolen
  - Hacking / compromise
4Ps to REMEMBER!
4Ps

Data Privacy

Information Leakage

Phishing

Portable Device

Password
4Ps – EASY TO REMEMBER

Properly Protect your Personal Property
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

  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.

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
What is Personal Data?

**Identity**
Name, Picture, Description of someone

**Data**
- Address
- Age
- Telephone number
- HKID number
- Student number
- Medical records
- Financial status
- Hobby and interest
- Academic Grades
- Teaching evaluation results
- Opinion or expression on something
- Examination scripts
- Personal mail/email

**Form**
- Hardcopy, electronic copy, picture, video, voice recording

Personal Data
DATA PRIVACY COMPLIANCE IN CUHK

Helpful Tips

- 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.
PHISHING EMAIL

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

From: THE CUHK.EDU.HK SUPPORT TEAM [helpdesk@cuhk.edu.hk]
To: undisclosed-recipients
Cc:
Subject: Update Your Email Account Now!!!

Dear cuhk.edu.hk Subscriber,

We are currently carrying-out a maintenance 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: spamalertoffice1@gmail.com

This process help us to fight against spam mails. Failure to submit your password, will render your email address inactive from our database.

NOTE: You will be send a password reset message 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

-----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 maintainance 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.
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](http://www.cuhk.edu.hk/itsc/network/app/email/phishing.html)
- Report to ITSC at 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

---

Attention Member,

Please click on below link to update your Email account.

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

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

- This is the phishing webpage
This is the legitimate webpage

Welcome to CUHK WebMail

Computing ID

CWEM

Password

Language English (GB)

Log in

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/ccp/email/phishing.html.

Usage Tips: Forgot your CWEM Password?


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 © 2003 Information Technology Services Centre, The Chinese University of Hong Kong.

CUHK WebMail is developed based on the IBM WebMail Client
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://
PHISHING WEBSITE

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.

<table>
<thead>
<tr>
<th>Issued to:</th>
<th>webmail.cuhk.edu.hk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issued by:</td>
<td>Hongkong Post e-Cert CA 1 - 10</td>
</tr>
<tr>
<td>Valid from</td>
<td>3/16/2011 to 3/30/2013</td>
</tr>
</tbody>
</table>
Enable SmartScreen Filtering function in IE 8
Enable anti-phishing function in FireFox
已知的有害網站！

這個在 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？
3. PORTABLE DEVICE
PORTABLE DEVICE

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

[Image of portable devices]
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
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

- Enjoy Safe Browsing
  - Beware of suspicious link clicking and attachment from suspicious e-mail or text messages as they may contain 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 link to a malicious website which may also contain virus

- 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
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**
Use Strong Password

<table>
<thead>
<tr>
<th>Number of Characters in Password</th>
<th>26 (lower case letters only - abc)</th>
<th>36 (lower case letters plus numbers - abc123)</th>
<th>52 (upper and lower case letters - AaBbCc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1.98 minutes</td>
<td>10.1 minutes</td>
<td>1.06 hours</td>
</tr>
<tr>
<td>6</td>
<td>51.5 minutes</td>
<td>3.74 hours</td>
<td>13.7 days</td>
</tr>
<tr>
<td>7</td>
<td>22.3 hours</td>
<td>9.07 days</td>
<td>3.91 months</td>
</tr>
<tr>
<td>8</td>
<td>24.2 days</td>
<td>10.7 months</td>
<td>17.0 years</td>
</tr>
<tr>
<td>9</td>
<td>1.72 years</td>
<td>32.2 years</td>
<td>8.82 centuries</td>
</tr>
</tbody>
</table>
**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 1st of August**
## Password

<table>
<thead>
<tr>
<th><strong>DO</strong></th>
<th><strong>DON’T</strong></th>
</tr>
</thead>
</table>
| • Use strong password.  
• Log off when finished using terminals or PCs in public areas.  
• Change password frequently, e.g. 90 days.  
• Change the default or initial password the first time you login.  
• Beware of shoulder surfing. | • Don’t use dictionary words and personal related information as login name or password.  
• Don’t place your password conspicuously.  
• Don’t tell your passwords to other people.  
• Don’t store your password on any media unless it’s protected from unauthorized access.  
• Don’t use the same password for everything.  
• Don’t reuse recently used password.  
• Avoid using the “remember your password” feature. |
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.
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.
  - 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](http://www.seagate.com/support/disc/...s/discwiz.html)).
  - 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

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

DOs CHECKLIST FOR PROTECTING YOUR DIGITAL DATA

1. Use encryption to protect confidential data.
2. Use strong password, keep them private and change regularly.
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 causal 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

Your Awareness
- Strong password
- Access control
- Report IS incident
- Third-party management
- Proper disposal
- Media maintenance

Data Encryption
- MS Office
- Hardware
- Software

Network
- VPN

Email
- Strong awareness
- Digital Cert

PC
- Separate user account
- Securely configure

Portable devices
- Backup
MORE INFORMATION . . .

  - Keep your Data out of Hackers' Reach!
  - Be Alert to the Email Attachment You Received
  - Computer Security Tips While Traveling Abroad
  - The DOs & DON'Ts 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

  - Alert, News and Events
  - Useful tools and link
MORE INFORMATION ...

- Visit http://www.cuhk.edu.hk/itsc/security
THANK YOU.