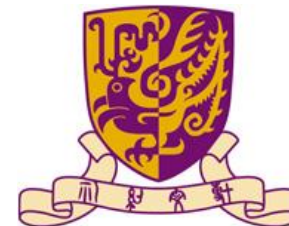


INFORMATION SECURITY

Tips in Preventing Information Leakage

Prepared by:
Information Security Section (ISS),
Information Technology Services Centre (ITSC)
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

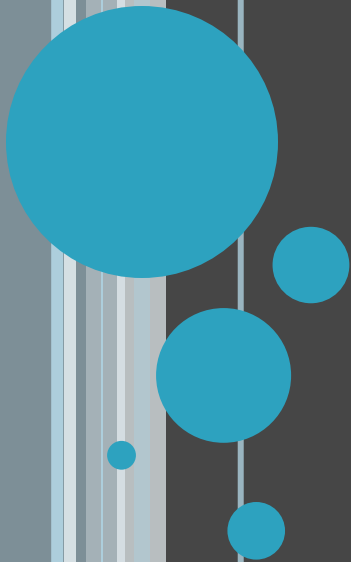
Tips to prevent data
leakage

AGENDA

- Information Security Incidents
- 4Ps to REMEMBER!!
- Tips in Preventing Information Leakage



INFORMATION SECURITY INCIDENTS



IS INCIDENTS

機場入境處電腦懷疑失竊



香港特別行政區政府
入境事務處



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。今次遺失的手提電腦是屬於一個獨立運作的電腦系統，本身並沒有與入境處其他主要電腦系統有任何連接，故事件不會影響入境處其他電腦系統。此外，有關手提電腦內的資料已獲加密處理，須利用已登記的用戶名稱和密碼進行多重認證，才能登入系統。在這些保密措施下，已獲加密的資料不能輕易讀取，因此，相信有關資料外泄的機會不大。由於遺失電腦收集的個人資料並未包括聯絡方法，本處會繼續研究如何與個別受影響旅客作進一步跟進。」

在事件發生後，入境處加強有關電腦系統的保安措施，包括重設系統的所有用戶密碼，並更新及替換電子硬體密匙(e-token)。



醫院管理局
HOSPITAL
AUTHORITY

瑪麗文員失 USB手指 洩 19病人資料

【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

...

IS INCIDENTS

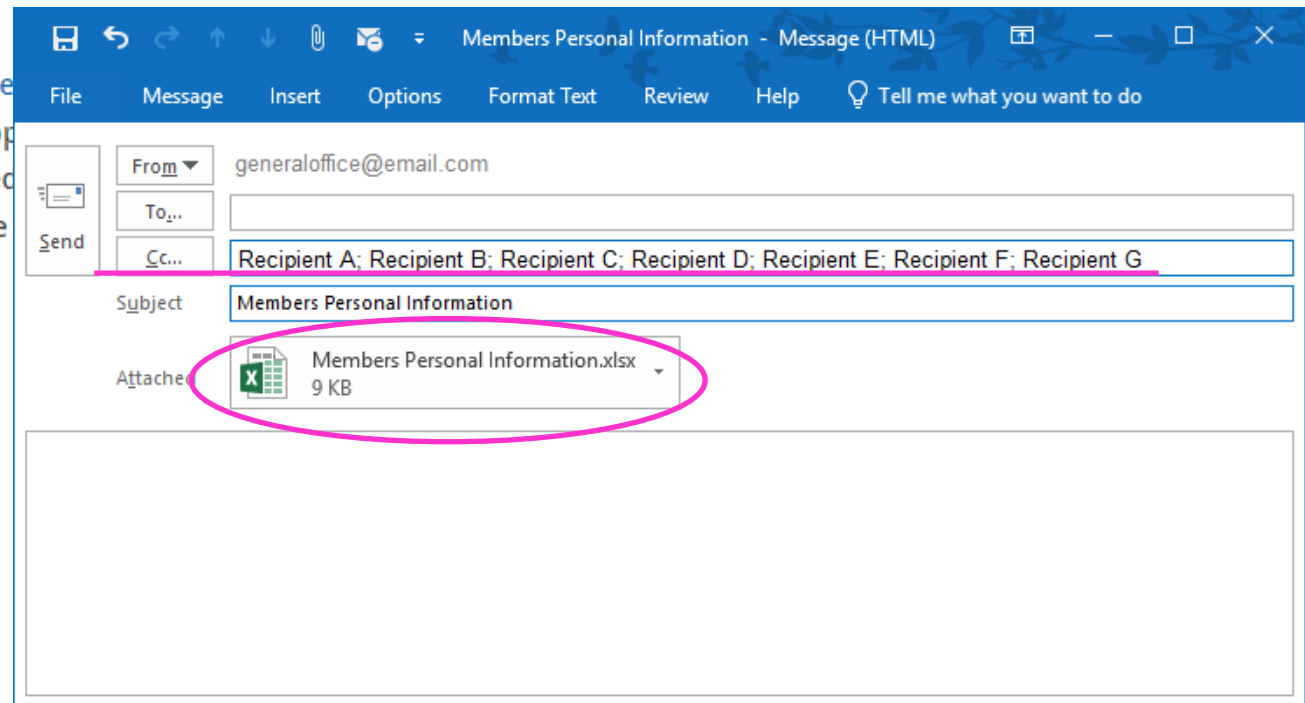


The club accidentally copied fans' details into a mass email addressed to up to 200 supporters

West Ham United could face action after accidentally leaking the details of hundreds of supporters in an email to confirm matchday tickets.

The football club accidentally cc-d the email addresses of up to 200 away season ticket holders to confirm their ticket allocations for the Football League Cup second round tie against Wimbledon AFC, set to take place next Tuesday.

Because only 675 tickets had been issued, the accidental leak of personal information occurred, forcing successful supporters to provide their details again to receive tickets.



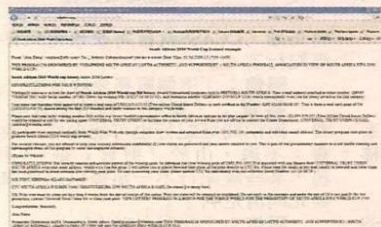
IS INCIDENTS



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識受騙，一上網搜尋「發現外國及本港多個足球論壇均有人提及受到欺詐電郵，才確定「中招」。

「騙子係外國，想追都追唔到，我睇到唔敢同屋企人講。」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，又或像前民政事務局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，多留意詐欺電郵多來自尼日尼亞，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。

IS INCIDENTS



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

Facebook再現惡意攻擊 成最危險的社交網站

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

facebook

「數萬網友遭到社交工程技術所騙，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，上面只有個連結寫著「點選此頁繼續」。但由於有個「隱形的iFrame」，點選該頁任何地方都會在使用者動態頁上散播攻擊內容及連結。「本月稍早我們看到的Fbhole也是類似情況。」Cluley說。Fbhole也會透過Facebook動態頁散播。

SophosLabs惡意程式研究中心首席技術工程師Richard Cohen說，如果你不幸中毒，可採兩步驟解決。首先，將該頁自「喜好與興趣頁」拿掉，接著，在你的動態頁上刪除該頁，它還是會留在「最近動態」頁中，但得往下拉才找得到。

IS INCIDENTS



「勒索軟件」警號再響！專家籲及時行動保護數碼資產

科技 2016-02-29 | HKITBLOG



勒索軟件我們早前都常介紹，它是一種惡意程式，當用戶「中招」，黑客多數會要求用戶通過 Bitcoins 完成付款，當用戶完成了付款後，儘管如此，但黑客通過這種手法，仍然可以獲取豐厚的收入。

近日，ESET 的研究人員便發現「勒索軟件」（Ransomware）這種科技愈趨普及，幾乎每人都會把自己的檔案，例如相片、文件等儲有有機可乘，勒索您的數碼資產。

勒索軟件屬惡意軟件的一種，一旦入侵作業系統，會使用戶無法正的控制權。簡言之，就是透過病毒鎖住檔案，並留下勒索訊息，金」。而新型態的勒索軟件，更進一步由電腦走到 Android 智能手全意識，配合防毒軟件的定時更新，才是應對上策。

如何避免

專家建議，大家可按以下方式去從心態上改變對網絡安全的危機意者。

1. 慎防可疑電郵及附件，特別是壓縮檔（zip、rar）或執行檔（exe）
2. 切勿點擊可疑電郵內的網站連結。
3. 使用可靠的防毒軟件，並定時更新。
4. 定期為電腦或手機的作業系統安裝更新軟件。
5. 定期為檔案備份，儘可能將檔案儲存至另一個安全的裝置。

Locky勒索病毒肆虐 數十校中招

經濟日報 2016年3月24日星期四上午6:55

相關內容



香港電腦保安事故協調中心高級顧問梁兆昌指，即使電腦裝有防毒軟件，也未能防止「中Locky招」。



【經濟日報專訊】提防電腦中毒！勒索病毒Locky肆虐，病毒以電郵形式，假扮收據、定單確認廣發垃圾電郵，一旦開啟附件，電腦內的文件便會被擄、不能打開。

據稱已有數以十計的學校中招，需付逾千元贖金才有機會贖回文件，但專家建議別付贖金，因會助長犯罪，呼籲市民切勿開啟有問題電郵。

入侵教師電腦 付300美元解鎖

香港生產力促進局屬下香港電腦保安事故協調中心

（HKCERT），上周五已發出保安警告，至昨午2時經累計收到27宗相關個案，當中兩宗為其網站被寄存了Locky軟件，中心透露，本港有數以十計的學校亦「中招」：「從教育界的聯繫得到的信息，使我們相信還有許多未報告的個案！」

Locky加密受害者電腦檔案，再勒索受害人0.5至1個比特幣（一個比特幣約3,200港元）以換取解密匙；據記者了解，最近有學校有多名教師電腦被Locky入侵，電腦被鎖死，被黑客要求付出約300美元（約2,300港元）解鎖，為了盡快解決事件，均決定付款。

IS INCIDENTS



有700萬個Dropbox帳號密碼被公開???

Dropbox禍不單行，曾被報導出有Bug會讓你同步的檔案消失無踪，最近還被爆出有大規模帳號遭客問題，駭客更聲稱已公開近700萬用戶的信箱及密碼，有使用Dropbox的人還是改改密碼吧。



該駭客表示成功駭入600多萬個Dropbox帳號上，並聲稱將以比特幣作為報酬，賣出更多的

不過Dropbox向the Next Web網站發聲明否認其他第三方服務害走，並不是直接從Dropbox式，他們將會停止被盜用的用戶密碼，並發被駭，大家還是換個密碼比較安全。

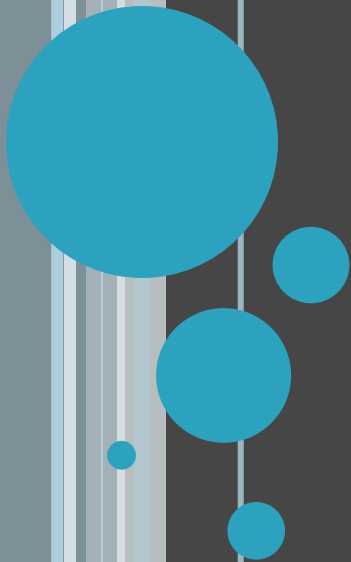
iCloud疑遭入侵 歷來最大規模密照外洩 逾百女星名人遭殃

[全部 > 新聞](#)

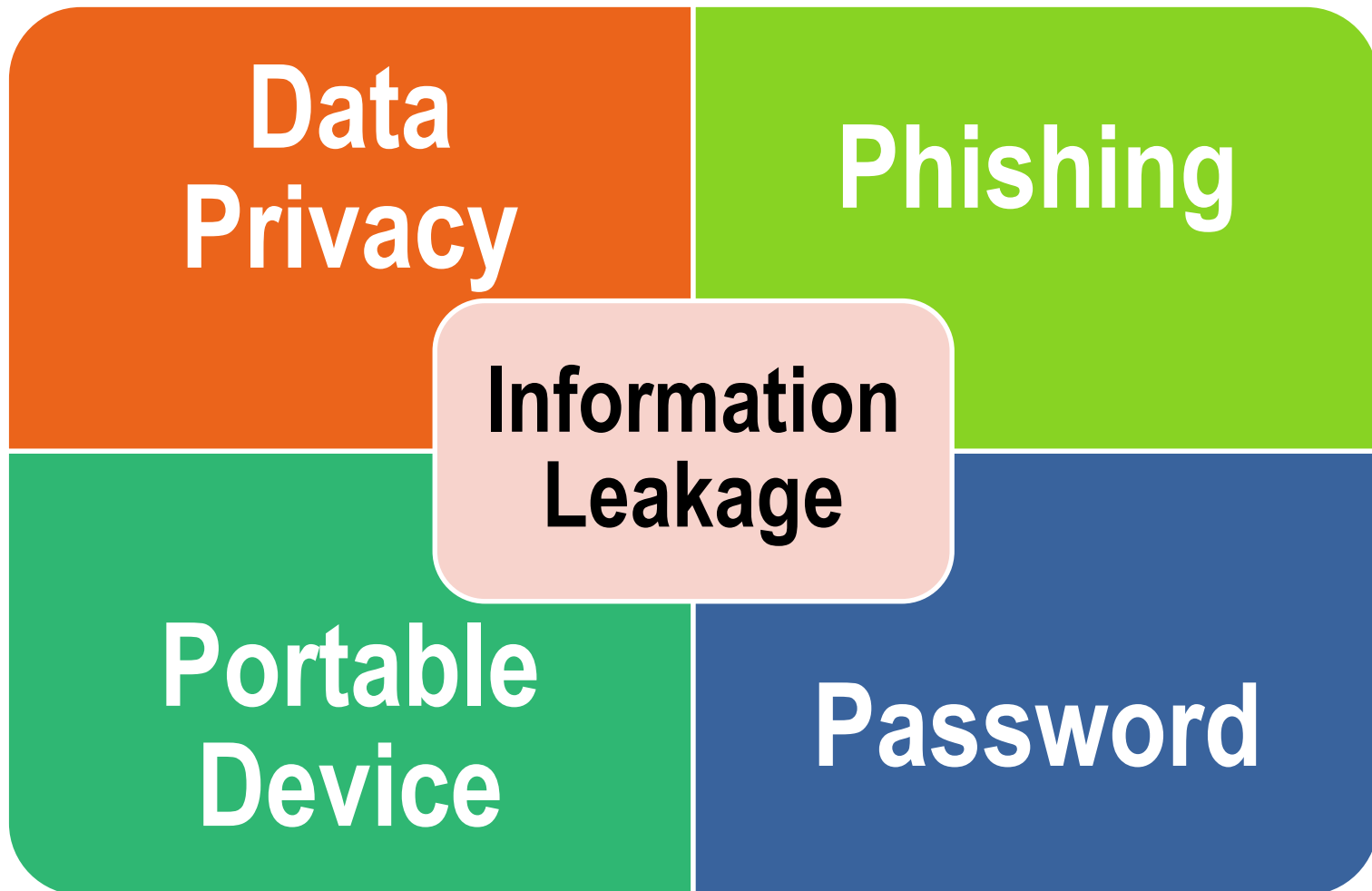
[f 推介](#) [分享](#) [0](#)

《飢餓遊戲》女星珍妮花羅倫絲(Jennifer Lawrence)、美國水著模特兒Kate Upton及英國名模Cara Delevingne等逾百名歐美女星名人，疑遭黑客入侵她們的蘋果雲端儲存iCloud帳戶，盜取多張裸照，部分檔案日前於網站4chan公諸於世，隨即在網上瘋傳，有傳媒形容是史上最大規模密照外洩事件。蘋果暫未回應事件，專家呼籲用戶在上傳敏感資料至雲端前應三思。

4Ps to REMEMBER!!



4Ps to remember



1. DATA PRIVACY



DATA PRIVACY COMPLIANCE IN CUHK



Policy in protection of personal data (privacy) - Personal Data 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 1 - Purpose and Manner of Collection
- Principle 2 - Accuracy and Duration of Retention
- Principle 3 - Use of Data
- Principle 4 - Data Security
- Principle 5 – Openness and Transparency
- Principle 6 - Access and Correction



DATA PRIVACY COMPLIANCE IN CUHK



○ Principle 4 – Data Security

- **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 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 measures)



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

DATA PRIVACY COMPLIANCE IN CUHK



- What is Personal Data?
- relating directly or indirectly to a living individual
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained

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

2. PHISHING



PHISHING



- Phishing / Fraud E-mail
- Phishing Website

PHISHING



- **Aim:**
 - To steal / collect **personal / sensitive information**
 - To ask for **money**

- **Purpose:**
 - For sale
 - For stealing your money
 - For sending more phishing e-mails
 - For controlling your computer, e.g. kidnapping
 - 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 which contains virus

- an **attachment** which contains virus

- Tempt you to reply / Claim to be urgent

PHISHING EMAIL



How to differentiate?

- Key phrases:
 - “Verify your account.” / “If you don’t respond with 48 hours, your account will be closed.”
 - “You have won the lottery.”
 - “To unsubscribe, click here...”
- Reply address is different from sender’s.
- Doubtful link / attachment embedded.
- Spelling mistakes



PHISHING EMAIL



Security Vulnerability Alert! - Message (HTML)

File Message Adobe PDF

Ignore X Reply Reply All Forward Meeting IM More Move Rules OneNote Actions Mark Unread Categorize Follow Up Translate Find Related Select Zoom

From: ITSC Service Desk <servicedesk@cuhk.edu.hk> Sent: Sat 1/9/2016 5:25 AM

To: ITSC Service Desk

Subject: Security Vulnerability Alert!

Two 'i' in the word "servicedesk"

Security Vulnerability Alert! *Subject draw your attention: **Alert!*** *Suspicious URL embedded*

We in service desk detected spam activities on your CU webmail account. Kindly Click Here or click/copy and paste the link below on your web browser and follow the verification process to assist us effect the necessary quarantine & resolve the spam issues on your account.

<http://goo.gl/Ukr6LX> *Suspicious URL embedded*

ITSC Service Desk


(c) All Rights Reserved. Information Technology Services Centre, CUHK

PHISHING EMAIL



April Salary Update - Message (HTML)

File Message Tell me what you want to do...

 CUHK-HR <employeehrpayroll@cuhk.edu>
April Salary Update

Hello, *Attractive subject*

Sequel to last week notification, find enclosed hereunder the letter summarizing your 14.89 percent salary increase starting April 2018.

****For authentication purpose, ensure your login information are correctly entered****

All documents are enclosed hereunder:


[Access Documents Here](#) *Suspicious URL embedded*

Human Resources & Employee Relations
The Chinese University of Hong Kong *Department not exist.*

Incorrect email address, CUHK email address should be xxx@cuhk.edu.hk

Abnormal sender address, CUHK email address should be xxx@cuhk.edu.hk

Mon 28-Jan-19 12:22 PM

 [Redacted]@gmail.com>

Are you on campus

To [Redacted]

Available?

PHISHING EMAIL



- When you receive a suspicious e-mail, you should:
 - **NEVER** reply any information to the e-mail.
 - **NEVER** click on any hyperlink or open any attachment in the e-mail.
 - Check if it's a reported phishing case via [ITSC homepage > News](#).
 - Report to [ITSC Online Service Desk](#) > Information Security > Report Phishing Email, if it is a new case.
 - Delete the e-mail.

ITSC and CUHK
NEVER
ask for your PASSWORD

PHISHING WEBSITE



- **Tactics:**

- Embedded a hyperlink 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**



Fri 29-Dec-17 7:57 PM

CUHK Library <libraries@cuhk.com>

Library Notifications

To undisclosed-recipients

Dear Library User,

Our records show that your access to CUHK Library System is about to expire. Due to security precautions established to protect University Libraries System, you have to renew your library account on a regular base, so please use the following link

sts.cuhk.edu.hk/authn/redirect/libraries/access/reactivation.htm

Mouse over the URL, suspicious URL embedded!

<https://library.llic.tk/data/access/lib/stscuhkeduhk>

Thank you,

Chinese University of Hong Kong
Sino Building, Chung Chi Rd, Sha Tin
libraries@cuhk.edu.hk

PHISHING WEBSITE

- This is the phishing webpage

The screenshot shows a web browser window with the title 'Sign In'. The address bar displays the URL `https://sts.cuhk.edu.hk.lit.cf/adfs/authenticate.html.ver=3&url=httpsaffshib.i`. Two red boxes highlight the domain `sts.cuhk.edu.hk` and the subdomain `.lit.cf`. A red callout box with the text 'Suspicious!!' points to the `.lit.cf` subdomain. The website content includes a 'Welcome to CUHK' banner with a campus illustration, a 'CUHK LOGIN' header, and login instructions for students, staff, and alumni. There are input fields for 'Login ID' and 'OnePass Password', a 'Sign in' button, and links for 'Login Help', 'Change Current / Expired Password', 'Maintenance Schedule', and 'Contact ITSC'. The footer contains copyright information for 2016 and the CADS logo.

Sign In

https://sts.cuhk.edu.hk.lit.cf/adfs/authenticate.html.ver=3&url=httpsaffshib.i

Suspicious!!

Welcome to
CUHK

CUHK LOGIN
For Office 365, @Link, LibrarySearch and more

Login with
Student: *Student-ID@link.cuhk.edu.hk*
Staff: *alias@cuhk.edu.hk*
Alumni: *alumni-ID@link.cuhk.edu.hk*
Password: OnePass Password

Login ID

OnePass Password

Sign in

? Login Help

Change Current / Expired Password

Maintenance Schedule

Contact ITSC


Copyright 2016. All Rights Reserved.
Information Technology Services Centre The Chinese University of Hong Kong

CADS
(CADS Reference Number: 233)

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

- This is the legitimate webpage



Sign In

https://sts.cuhk.edu.hk/adfs/ls/?wa=wsignin1.0&wtrealm=urn:federation:Micros

Welcome to
CUHK

CUHK LOGIN
For Office 365, @Link, LibrarySearch and more

Login with
Student: *Student-ID@link.cuhk.edu.hk*
Staff: *alias@cuhk.edu.hk*
Alumni: *alumni-ID@link.cuhk.edu.hk*
Password: OnePass Password

Login ID

OnePass Password

Sign in

Login Help

Change Current / Expired Password

Maintenance Schedule

Contact ITSC

Copyright 2016. All Rights Reserved.
Information Technology Services Centre - The Chinese University of Hong Kong

PHISHING WEBSITE

1. Secure communication (https://)
2. Digital Certificate

A screenshot of a web browser displaying a phishing website. The browser's address bar shows the URL 'https://www.security.online-banking.hsbc.com.hk/gsa?idv_cmd=idv.SaaSSecurityCommand'. A red box highlights the 'https' part of the URL, with a red arrow pointing to a green padlock icon in the browser's status bar. A red box also highlights the 'https' part of the URL. A security warning overlay is visible on the right side of the browser window. The overlay has a title 'Website identification' and contains the following text: 'VeriSign has identified this site as The Hongkong and Shanghai Banking Corporation Limited HONG KONG, HONG KONG HK'. Below this, it says 'Your connection to the server is encrypted. Should I trust this site?'. The overlay also has a section titled 'Website permissions' which says 'You haven't set any permissions for this site yet. Allow Adobe Flash'. The background of the browser shows the HSBC logo and the text '登入網上理財' (Log in to online banking) and '網上理財' (Online banking). There is a red button labeled '繼續' (Continue) at the bottom right of the browser window.

登入網上理財：用戶名稱 X

← → ↻ 🏠 **2** **1** https://www.security.online-banking.hsbc.com.hk/gsa?idv_cmd=idv.SaaSSecurityCommand

HSBC 滙豐

登入網上理財

網上理財

請輸入您的用戶名稱

繼續

Website identification

VeriSign
has identified this site as
The Hongkong and Shanghai Banking Corporation Limited
HONG KONG, HONG KONG
HK

Your connection to the server is encrypted.
[Should I trust this site?](#)

Website permissions

You haven't set any permissions for this site yet.
[Allow Adobe Flash](#)

PHISHING WEBSITE



Sign In

https://sts.cuhk.edu.hk/adfs/ls/?wa=wsignin1.0&wtrealm=urn:federation:Micros

Welcome to CUHK

Website identification

Hongkong Post Root CA 1
has identified this site as
sts.cuhk.edu.hk
HK

Your connection to the server is encrypted.
[Should I trust this site?](#)

Website permissions

You haven't set any permissions for this site yet.
[Allow Adobe Flash](#)

CUHK LOGIN
For Office 365, @Link, LibrarySearch and more

Login with
Student: *Student-ID@link.cuhk.edu.hk*
Staff: *alias@cuhk.edu.hk*
Alumni: *alumni-ID@link.cuhk.edu.hk*
Password: OnePass Password

Login ID

OnePass Password

Sign in

[Login Help](#)

[Change Current / Expired Password](#)

[Maintenance Schedule](#)

[Contact ITSC](#)

Copyright 2016. All Rights Reserved.
Information Technology Services Centre The Chinese University of Hong Kong

PHISHING WEBSITE



- Enable **Anti-Phishing / SmartScreen** filtering features on your browsers, e.g. Edge, Chrome, Firefox, etc.



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？

忽略此警告

3. PORTABLE DEVICE



PORTABLE DEVICE

- USB Storage Device
- Notebook
- Tablet
- Smartphone
- ...

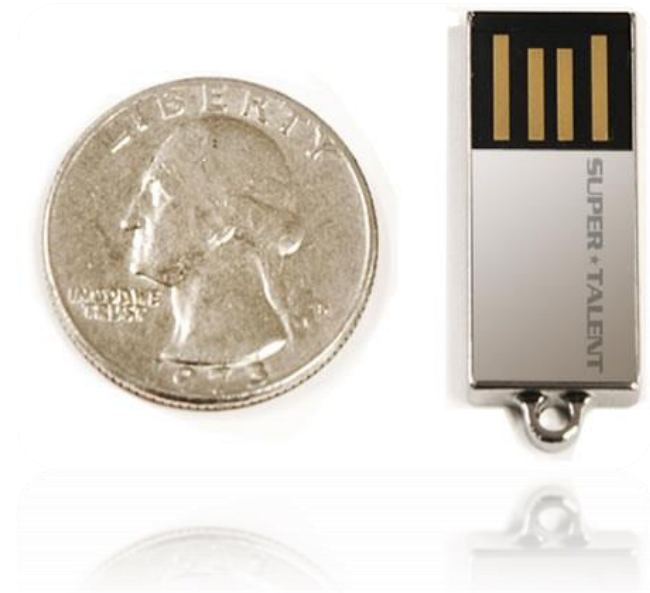


PORTABLE DEVICE



○ 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

- Software Encryption

- e.g. BitLocker, bundled in Win 8 / 10

- Hardware with Encryption

- With security functions e.g. encryption, password, fingerprint, etc. embedded
- Convenient and fast but more expensive



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
(<https://www.itsc.cuhk.edu.hk/user-trainings/information-security-best-practices/guidelines-for-securely-managing-mobile-removable-devices/>).

PORTABLE DEVICE

For Smart Phones & Tablets



- Lock your devices.
- Use Secure Network, e.g. VPN
 - DO NOT connect to untrusted Wi-Fi networks and access personal data.
 - Turn off Wi-Fi, Bluetooth & location service when not use .
- Enjoy Safe Browsing:
 - Use SSL (https://)
 - Beware of the Quick Response (QR) code
 - Disable link preview function
- Protect Your Operating System (OS):
 - DO NOT jailbreak / root the device
 - Keep the OS updated and install anti-virus software
- Mind Your Apps, DO NOT download apps from untrustworthy sources.



PORTABLE DEVICE

For Smart Phones & Tablets



- Securely erase / wipe all the data before discarding or selling your device.
 - Use the 'remote wipe' function to erase data if the device is lost.
- Setup below functions to locate your device in case it is lost:
 - “Find My iPhone” for iPhone / iPad.
 - “Lost Phone” for Android devices.
- Read the security guidelines for smart phones and tablets
(<https://www.itsc.cuhk.edu.hk/user-trainings/information-security-best-practices/security-tips-while-using-smart-phones-and-tablets/>).

4. PASSWORD



PASSWORD



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

PASSWORD



WEAK

123456

91557730

20080801

frankie

STRONG

p@trick1101

We@rthch7730

li08_ly01

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

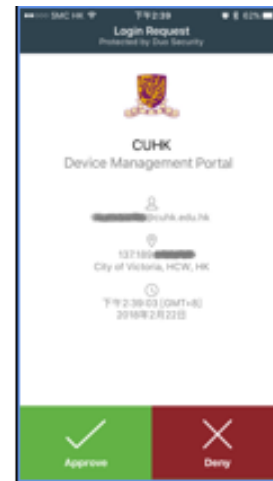
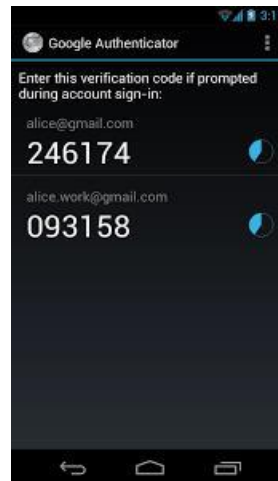
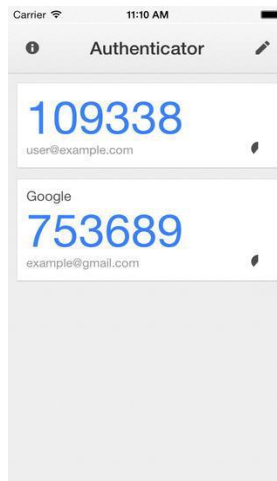
lily births on 1st of
August

PASSWORD

○ 2 Factor Authentication (2FA):

- Combination of:

- Something you know, e.g. password
- Something you are, e.g. fingerprint
- Something you have, e.g. one-time password / token



- Duo 2FA (<https://www.itsc.cuhk.edu.hk/all-it/information-security/two-factor-authentication-2fa/>)

PASSWORD



Information to protect your accounts:

- OnePass Password
- CU Link Card:
 - CU Link PIN
 - MiFare ID / Serial No



NEVER

Disclose / Collect all of these information

PASSWORD



DO	<ul style="list-style-type: none">• Use strong password.• Change password frequently, e.g. 6 months, annually, etc.• Change the default or initial password the first time you login.• Beware of shoulder surfing.• Log off when finished using terminals or PCs in public areas.
DON'T	<ul style="list-style-type: none">• Don't use dictionary words / personal information as login name / password.• Don't place your passwords conspicuously.• Don't tell your passwords to other people.• Don't store your passwords on any media unless it's protected from unauthorized access.• Don't keep your passwords in any unprotected file with an easy to guess filename, e.g. password.txt• Don't use the same password for everything.• Don't reuse recently used password.• Avoid using the "remember your password" feature.

PASSWORD

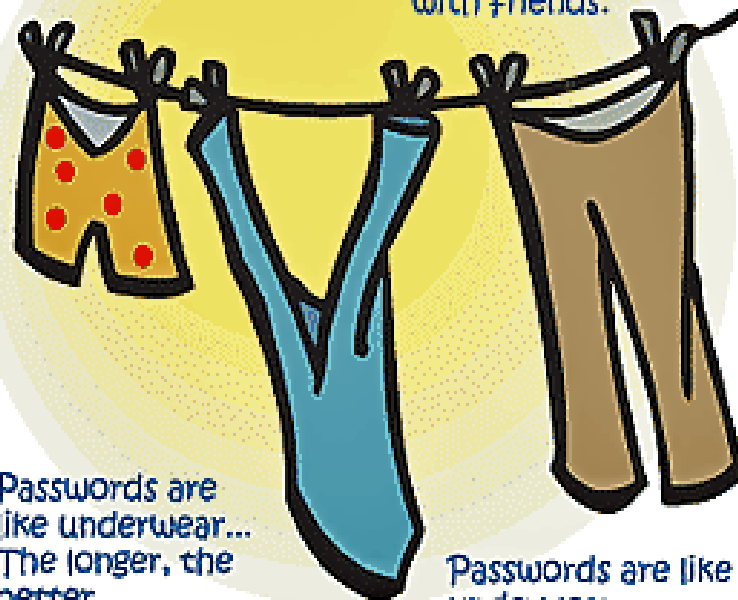


Passwords Are Like Underwear

Passwords are like underwear...
Change yours often.

Helpful
Tips

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

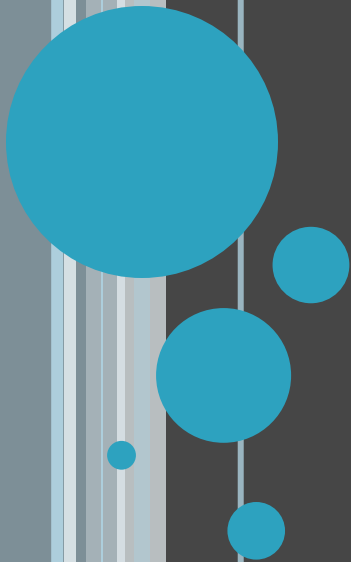


Passwords are
like underwear...
The longer, the
better.

Passwords are like
underwear...
Be mysterious.

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

MORE TIPS IN PREVENTING INFORMATION LEAKAGE



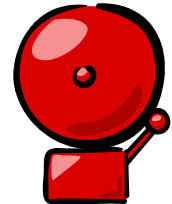
TIPS IN PREVENTING INFORMATION LEAKAGE

○ Your Awareness



○ Report IS incidents

- In case of leakage highly sensitive and confidential information in electronic format, report it **IMMEDIATELY**.
- Details reporting procedures can be found at <http://www.itsc.cuhk.edu.hk/en-gb/all-it/information-security/is-incident-handling>.





TIPS IN PREVENTING INFORMATION LEAKAGE

○ Data Protection

- Protect files with encryption, e.g., [Microsoft Information Protection \(MIP\)](#), Window's BitLocker, etc. if it contains any confidential / sensitive information.

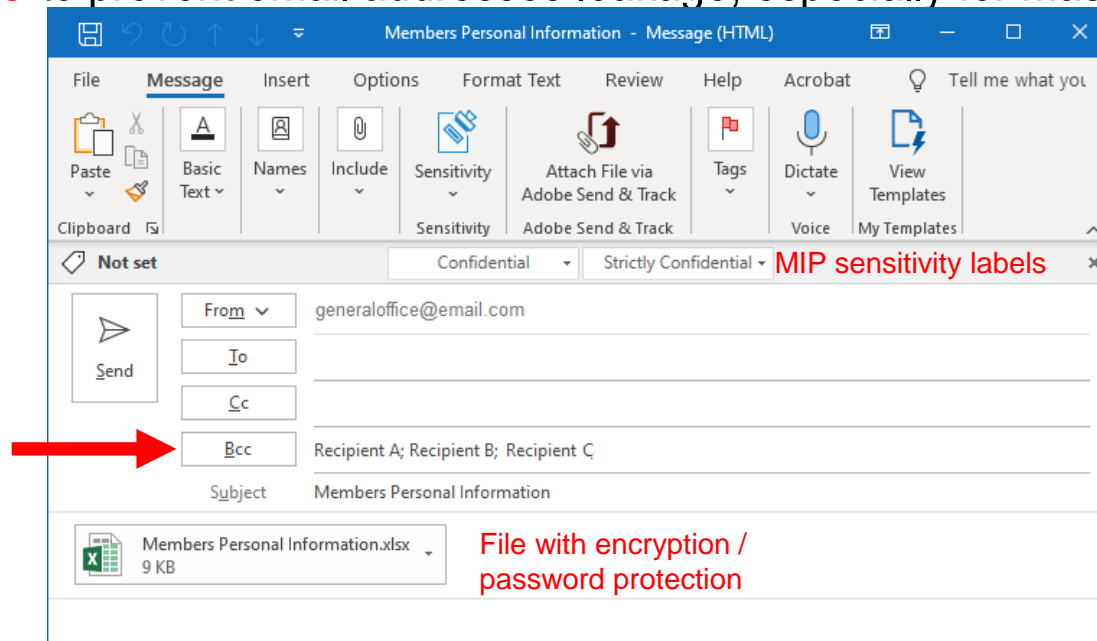
Confidential ▼

Strictly Confidential ▼

TIPS IN PREVENTING INFORMATION LEAKAGE

○ Email Protection

- Use Microsoft Information Protection (MIP) to protection confidential email content and email attachments.
- Use **BCC** to prevent email addresses leakage, especially for mass email:



- Use **Mailing List** - a single email address that points to a number of email addresses. An email sent to a mailing list will be automatically forwarded to members who subscribe the list.

(<https://www.itsc.cuhk.edu.hk/all-it/email-messaging-and-collaboration/mailing-list/>)



TIPS IN PREVENTING INFORMATION LEAKAGE

- Proper disposal - hardware
 - Zero-filled (<http://www.seagate.com/support/by-topic/downloads/>).
 - Data Purging (<http://www.dban.org/>).
 - Degaussing the devices.
 - Physically destroying them.

- Proper disposal – hardcopy
 - Use paper shredder.



TIPS IN PREVENTING INFORMATION 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)
(<https://www.itsc.cuhk.edu.hk/all-it/information-security/data-privacy-and-protection/>)

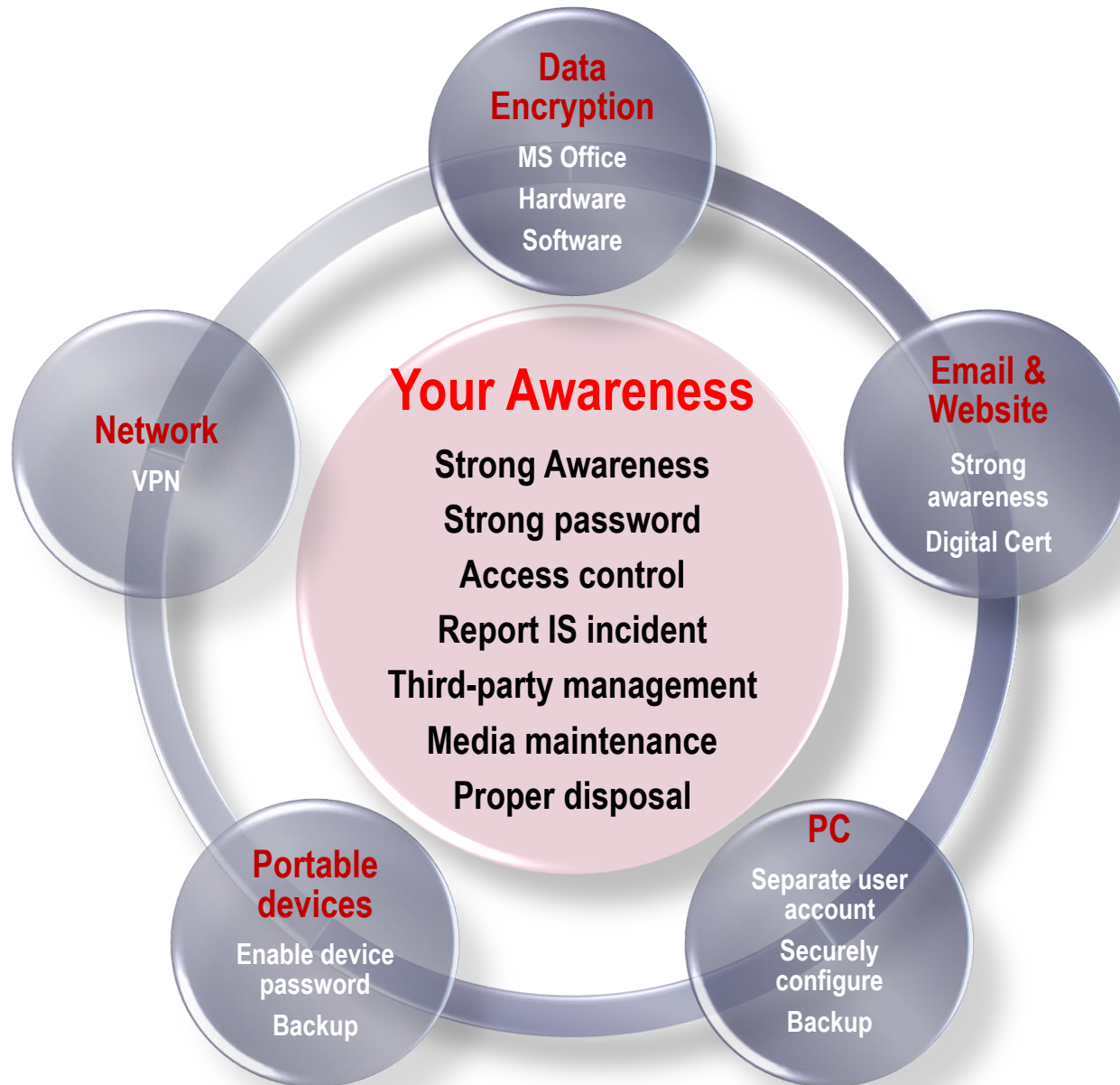


GUIDELINES FOR SECURELY CONFIGURING YOUR COMPUTERS

Guideline	Done?
1. Follow the University Software Standards	
2. Update Windows and update latest patches	
3. Install anti-virus software – Kaspersky (https://www.itsc.cuhk.edu.hk/all-it/information-security/anti-virus-on-pcs/)	
4. Update latest virus signatures for the anti-virus software	
5. Perform regular scanning, e.g. full scan, on your computer	
6. Turn on personal firewall	
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.	

Details: <https://www.itsc.cuhk.edu.hk/user-trainings/information-security-best-practices/guidelines-for-securely-configuring-your-computers/>

TIPS IN PREVENTING INFORMATION LEAKAGE





DOs CHECKLIST FOR PROTECTING YOUR DIGITAL DATA

1. Encrypt confidential / sensitive data.
2. Use strong password, keep them private & change regularly.
3. Beware of suspicious e-mails.
4. Configure your computer securely.
5. [Backup important data & test the backup regularly.](#)
6. Activate password protection for unattended computing devices.
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.



MORE INFORMATION ...

Information Security homepage

(<https://www.itsc.cuhk.edu.hk/all-it/#information-security>)

- Major Projects:
 - DUO Two Factor Authentication (2FA)
 - Microsoft Information Protection (MIP)
- Information Security Policies
 - 2FA Policy for All University Accounts
 - Revise OnePass Password Expiry Policy from 400-day Expiry to Annual Expiry
- Information Security Best Practices for
 - General User
 - IT Professional
- News & Alerts
- etc.

A decorative graphic on the left side of the slide. It consists of several vertical stripes of varying widths and shades of blue and grey. Overlaid on these stripes are five solid blue circles of different sizes, arranged in a cluster that tapers towards the bottom.

THANK YOU.