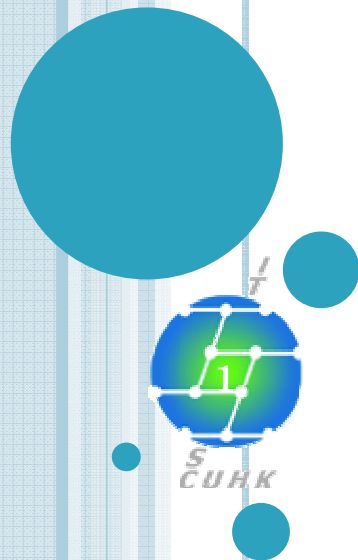


TIPS IN PREVENTING INFORMATION LEAKAGE



Presented by Christina Keing and Frankie Fu
Information Security Section (ISS), ITSC

5 Sept 2008

AIMS

To Alert

The recent incidents

To Think

What confidential data you are handling?
What are the risks?

To Learn

Tips to protect electronic data

AGENDA

- Recent incidents
- What information to protect?
- How do we handle electronic information?
- How does information leak?
- Tips in preventing information leakage



RECENT INCIDENTS

6 May 2008



Panel probes loss of 6,000 patients' details

- 9 portable computing devices containing information on 6,000 patients in public hospitals were lost or stolen over the past year.
- The 9 devices include USB drive, PDA, MP3 player, notebook and digital camera.

Source

http://www.thestandard.com.hk/news_detail.asp?pp_cat=30&art_id=65404&sid=18791577&on_type=1&d_str=20080506&sear_year=2008

RECENT INCIDENTS

27 May 2008



Cover cops hit by leaks

- An e-mail was sent to the media with 10 documents downloaded by using the peer-to-peer software Foxy.
- The documents contain highly confidential information about the undercover police operations, with the names of the agents .

Source

http://www.thestandard.com.hk/news_detail.asp?we_cat=11&art_id=66422&sid=19089930&con_type=1&d_str=20080527&fc=2



RECENT INCIDENTS

June 2007 理大成績洩漏

理大成績洩漏討論 · 香港理工大學 PolyU · 大專 · 失敗論壇 · Powered by Discuz! · Mozilla Firefox

標題: 理大成績洩漏討論

發表於 2007-6-10 04:36 PM 資料 個人空間 短消息 加為好友 #1

理大成績洩漏討論

[轉自蘋果日報] 理工大學萬名學生的個人考試成績慘遭「剝光豬」盡露人前。該校前晚透過電郵系統向學生發放期末考試電子成績表時，成績表出現大亂，學生收到別人的全份成績表，自己的資料卻收不到。不少學生網上留言促校方作出交代和道歉。個人資料私隱專員公署關注事件，或會主動介入調查。

理大學生會會長余耀東昨表示，前晚約7至8時，開始聽到有同學稱在電郵系統，收到別人的電子成績表，之後學生一窩蜂上網查電郵，導致系統癱瘓而要維修。他說，每張成績表除了學生姓名和學號外，還詳列每人本學期修讀的各科成績，以及最敏感的GPA（總成績積點，最高4分）。

學生留言要校方交代

余耀東指事件嚴重，校方必須向全校作出解釋，「個系統唔係第一年用，同學私隱都洩漏晒。」他表示，每個在學校電郵系統內的電郵會在收到後1個月自動刪除，但現時不少同學已設定將學校電郵自動傳去其他電郵戶口接收，所以校方無法立即刪除所有發出的問題電郵。

由前晚開始，陸續有理大不同學系學生在網上留言區留言，稱他們收到別人的成績表，對事件感到驚訝，「我自己仲未睇到成績，就已經俾人睇晒」、「咁大間學府，竟然咁荒唐嘅事都可以發生」、「垃圾poly（理大英文簡稱）！連個電郵系統都衰過人」。

有學生留言說，看到同學的成績不太好，「見到人哋有科肥咗佢呀！真係唔知好唔好話畀當事人知！」有學生發起寫大字報行動批評校方，促校方交代事件和向相關人士問責，又揶揄說：「冇錢就走去聽風水佬話整學校，冇事無事都裝修，又唔見整好個資訊科技系統。」有人也發起向個人資料私隱專員公署投訴。

理大認錯已緊急搶修

理大發言人承認發放電子成績表系統出現故障，有關方面知悉後已關閉電郵系統，教務處、資訊科技處和服務供應商昨日緊急研究故障成因和進行搶修，以盡快解決問題。發言人說，高級文憑生和學士學位學生的成績資料，都是經同一電腦系統發放。資料顯示，該兩類學生人數約有12,000人。

私隱公署或介入調查

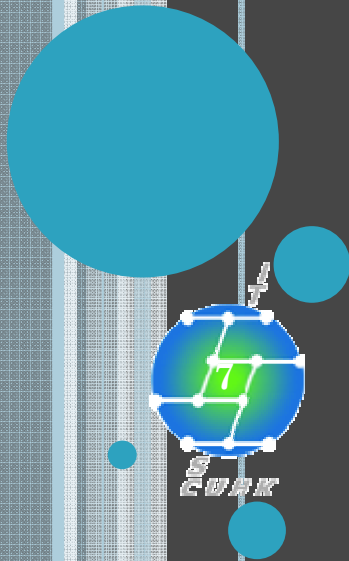
私隱專員公署發言人表示，初步看來理大有洩漏個人資料問題，情況就如銀行將某位客戶資料錯寄另一客戶。該發言人說若事件影響廣泛，公署可主動調查，毋須等候受害人投訴，這次涉及萬名學生，公署有可能會主動介入，也希望受影響學生可主動提供資料。公署調查後一般會要求有關機構改善，然後評核是否令人滿意；若對方拒絕執行，才會作出檢控。

各位理大同學們有沒有遇到這情況？
如有，你收到的分數中的學生你又是誰？
您又希望校方做些甚麼補救？
若非理大同學，您又怎樣看此事件？

Source: "Fail Forum"

<http://failforum.net/forum/viewthread.php?tid=563585&extra=page%3D1>

WHAT INFORMATION TO PROTECT?



WHAT INFORMATION TO PROTECT?



- “Confidential data” means data which are sensitive, restricted and top secret.
- Examples include but not limited to :
 - Password, credit card numbers, salary, student academic record and medical history, etc.
- Staff may also judge by themselves based on the regular practice and their experience.

WHAT INFORMATION TO PROTECT?

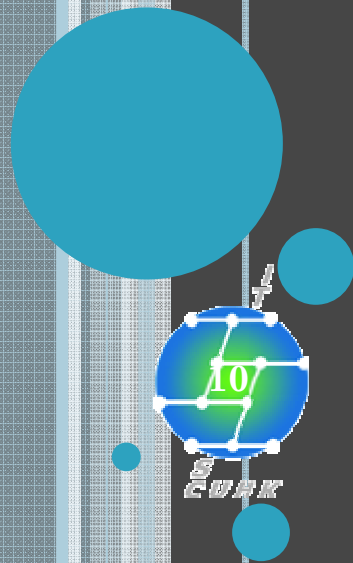
The
Ordinance



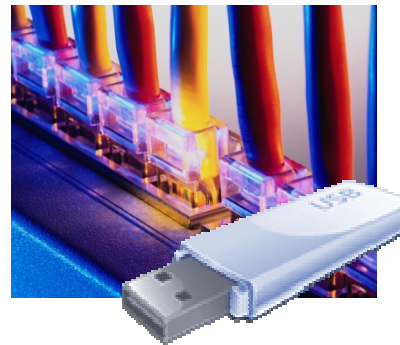
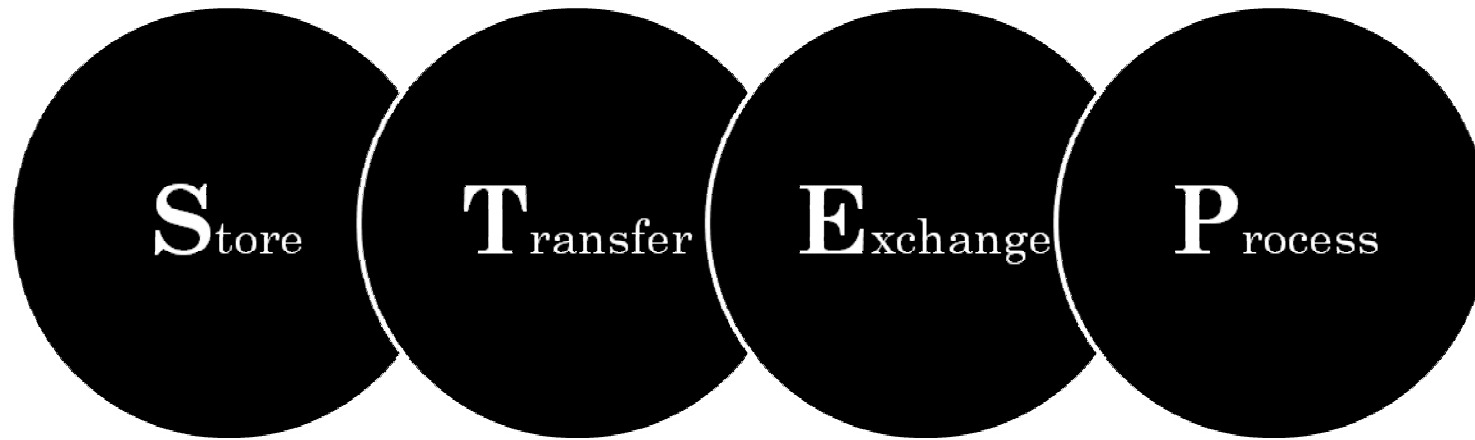
- “personal data” means any data
 - relating directly or indirectly to a living individual
 - from which it is practicable for the identity of the individual to be directly or indirectly ascertained
 - Example: name + address
- For more information:
 - Personal Data Controlling Committee at CUHK
<http://www.cuhk.edu.hk/policy/pdo/>
 - Personal Data (Privacy) Ordinance
 - <http://www.pcpd.org.hk/english/ordinance/down.html>



HOW DO WE HANDLE ELECTRONIC INFORMATION?



HOW WE HANDLE ELECTRONIC INFORMATION?



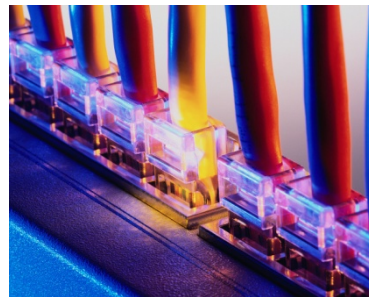
HOW WE HANDLE ELECTRONIC INFORMATION?

4. Portable
Device

3. Network

2. Email

1. PC



**HOW INFORMATION
LEAKS?**

TIPS OF PREVENTION?

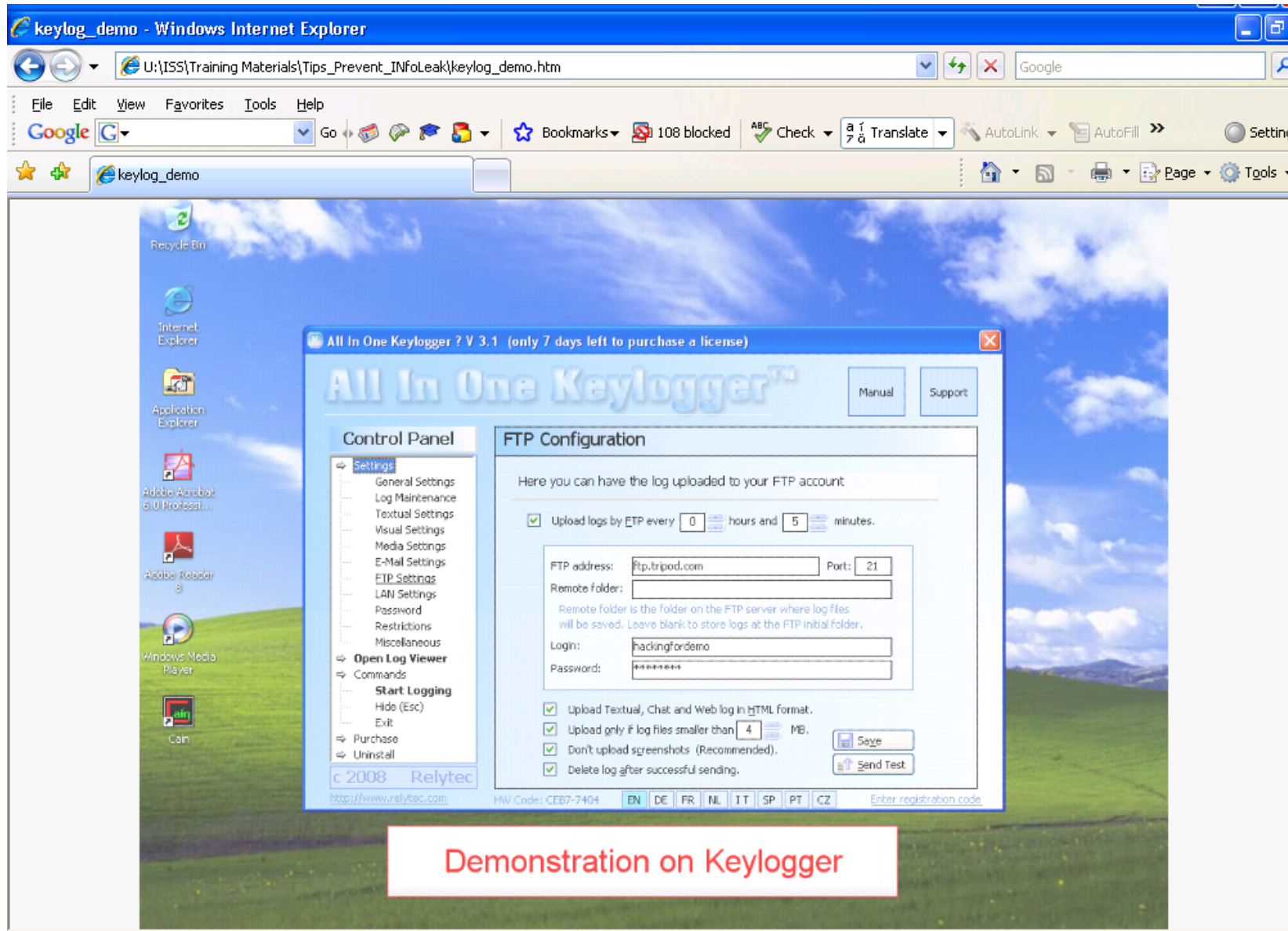
HOW INFORMATION LEAKS FROM

1. PC

- a. Unaware of software installed (e.g. keystroke logger).
- b. Unaware of the inherited settings under a shared environment (e.g. via Foxy).
- c. Infection of virus and some malicious attack.



a. UNAWARE OF SOFTWARE INSTALLED (E.G. KEYSTROKE LOGGER)





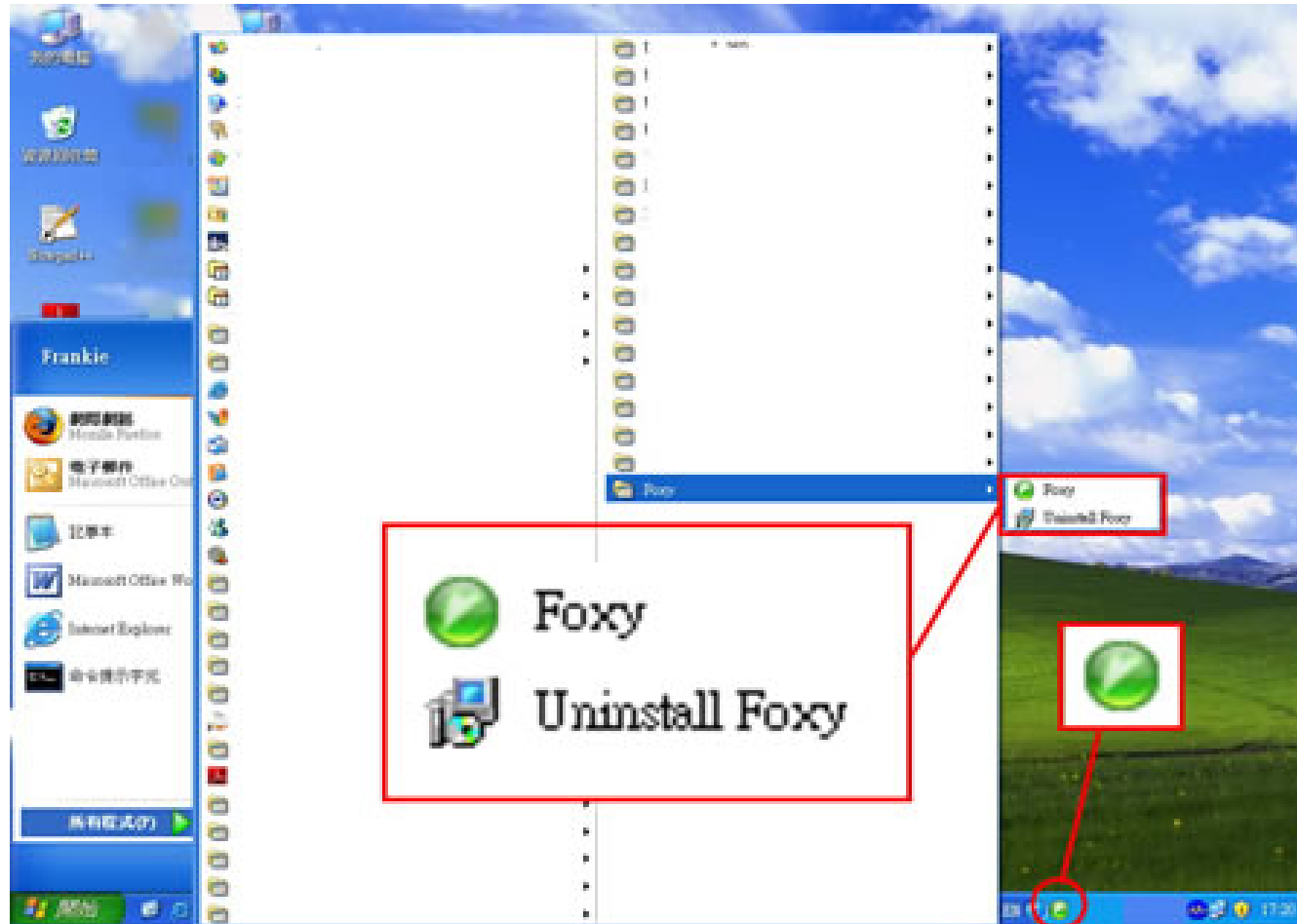
- The Best Protection is:
 - Don't process and save confidential information in unfamiliar computers (e.g. computer in cyber café or public area)

b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY)



Age Group	Probability of Foxy installed (%)
○ Children of P4 – S3	> 30%
○ Children of P4 – S3 ○ Have MP3 player	> 60%
○ Children of P4 – S3 ○ Have MP3 player ○ Have lot of new songs	> 90%

- b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY).



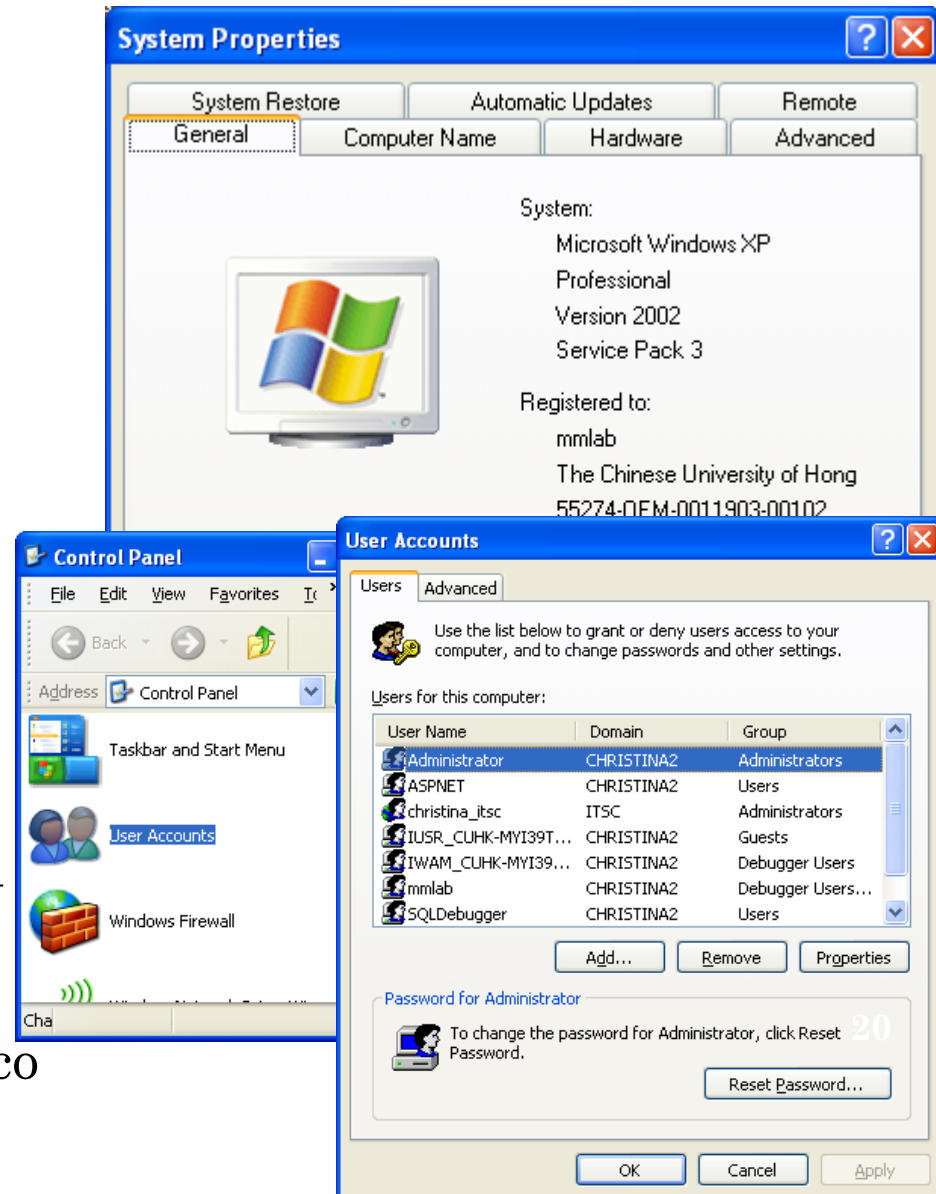
b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY)



b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY).

Use separate user accounts with no administrator right under a shared environment.

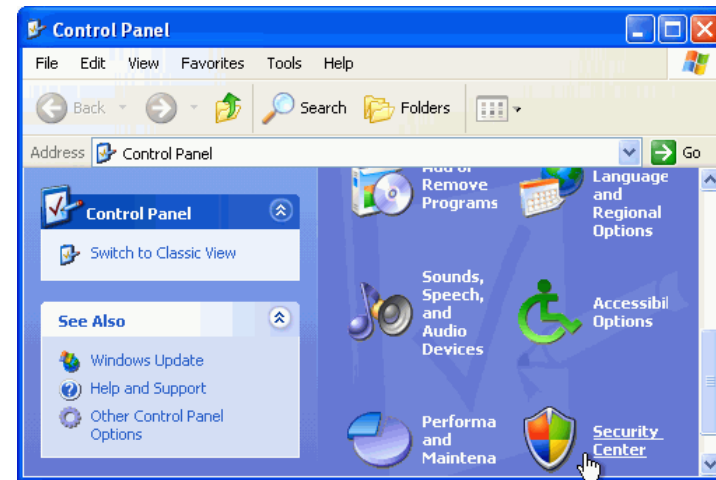
- However, this is useful only under Windows XP **Professional Edition** but not Home edition.
- For staff, you are entitled upgrade your Windows XP Home Edition. More info can be found at “Work at Home Use Rights” at <http://www.cuhk.edu.hk/itsc/compenv/license/ms.html>



c. INFECTION OF VIRUS AND SOME MALICIOUS ATTACK

○ Installation of

- Firewall
 - e.g. CUHK anti-virus centre
<http://www.cuhk.edu.hk/itsc/security/antivirus/index.html>
- Anti-virus
 - e.g. CUHK anti-virus centre
<http://www.cuhk.edu.hk/itsc/security/antivirus/index.html>
- Anti-spyware
 - e.g. spypot
<http://www.safer-networking.org/en/index.html>



TIPS TO PREVENT INFORMATION LEAKAGE FROM

1. PC

a. Unaware of software installed (e.g. keystroke logger)

b. Unaware of the inherited settings under a shared environment (e.g. Foxy)

c. Infection of virus and some malicious attack

TIPS TO PREVENT INFORMATION LEAKAGE FROM

1. PC

a. Don't use unfamiliar computer to process confidential data.

b. Use Windows XP Professional Edition; separate user accounts with no admin right.

c. Securely configure your computer; install firewall, anti-virus and anti-spyware

TIPS TO PREVENT INFORMATION LEAKAGE FROM

1. PC

- **Office PC** is relatively safe assuming you to follow the guidelines at

- More information can be found:



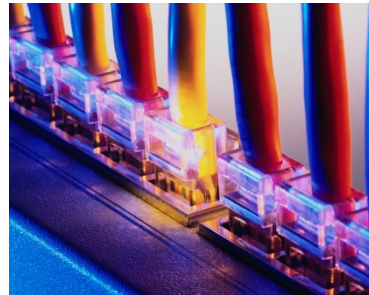
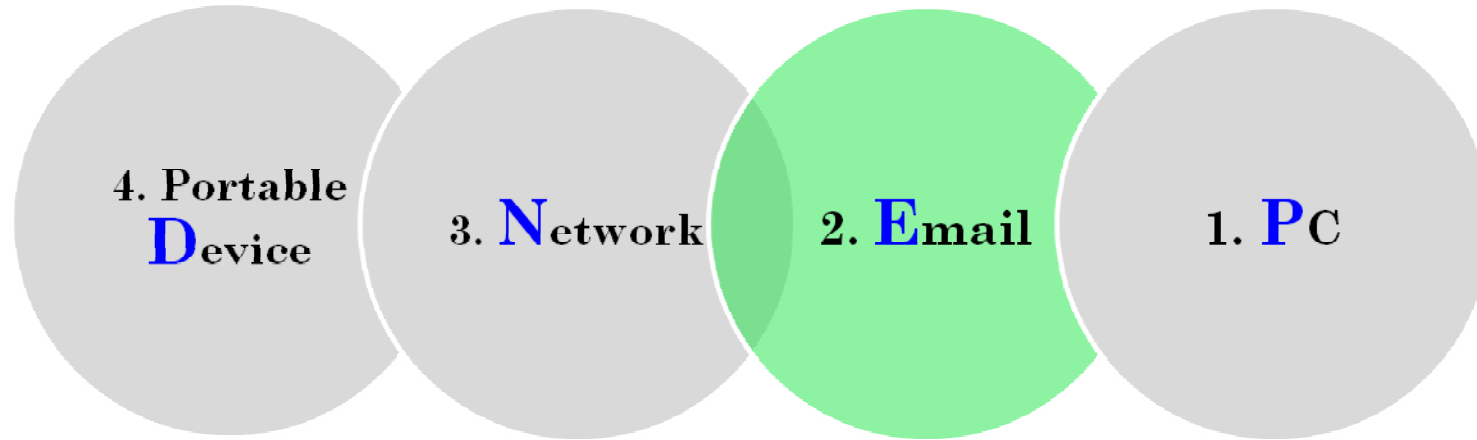
- University software standard

<http://www.cuhk.edu.hk/itsc/deptsupport/swstd/swstd.html>

- Securely configuring your computers

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

HOW WE HANDLE ELECTRONIC INFORMATION?



HOW INFORMATION LEAKS FROM

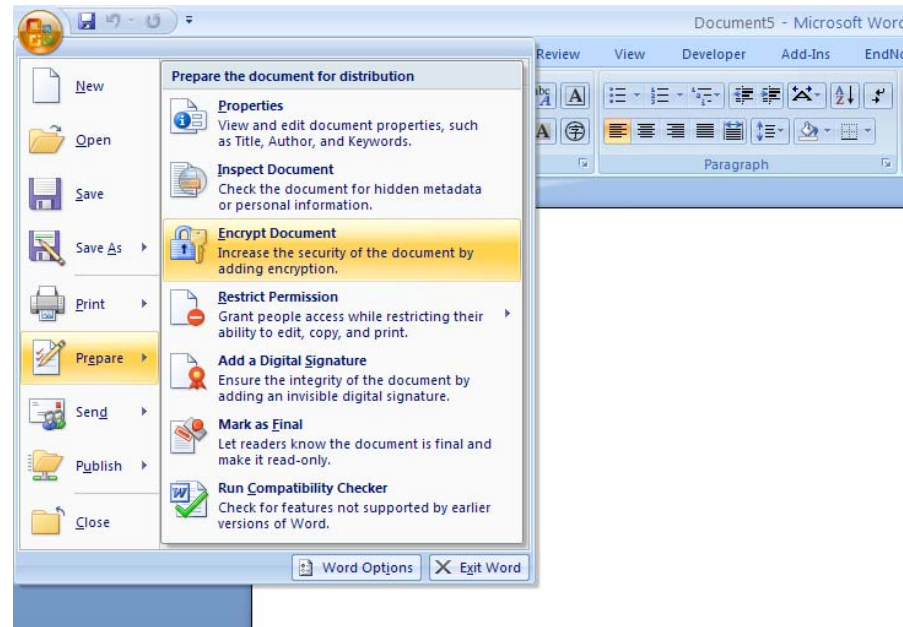
2. EMAIL



- a. Careless mistake (wrongly sent to another person)
- b. Wrongly trust the email sender (email spoofing)
- c. Phishing email

a. CARELESS MISTAKE (SENT TO A WRONG PERSON)

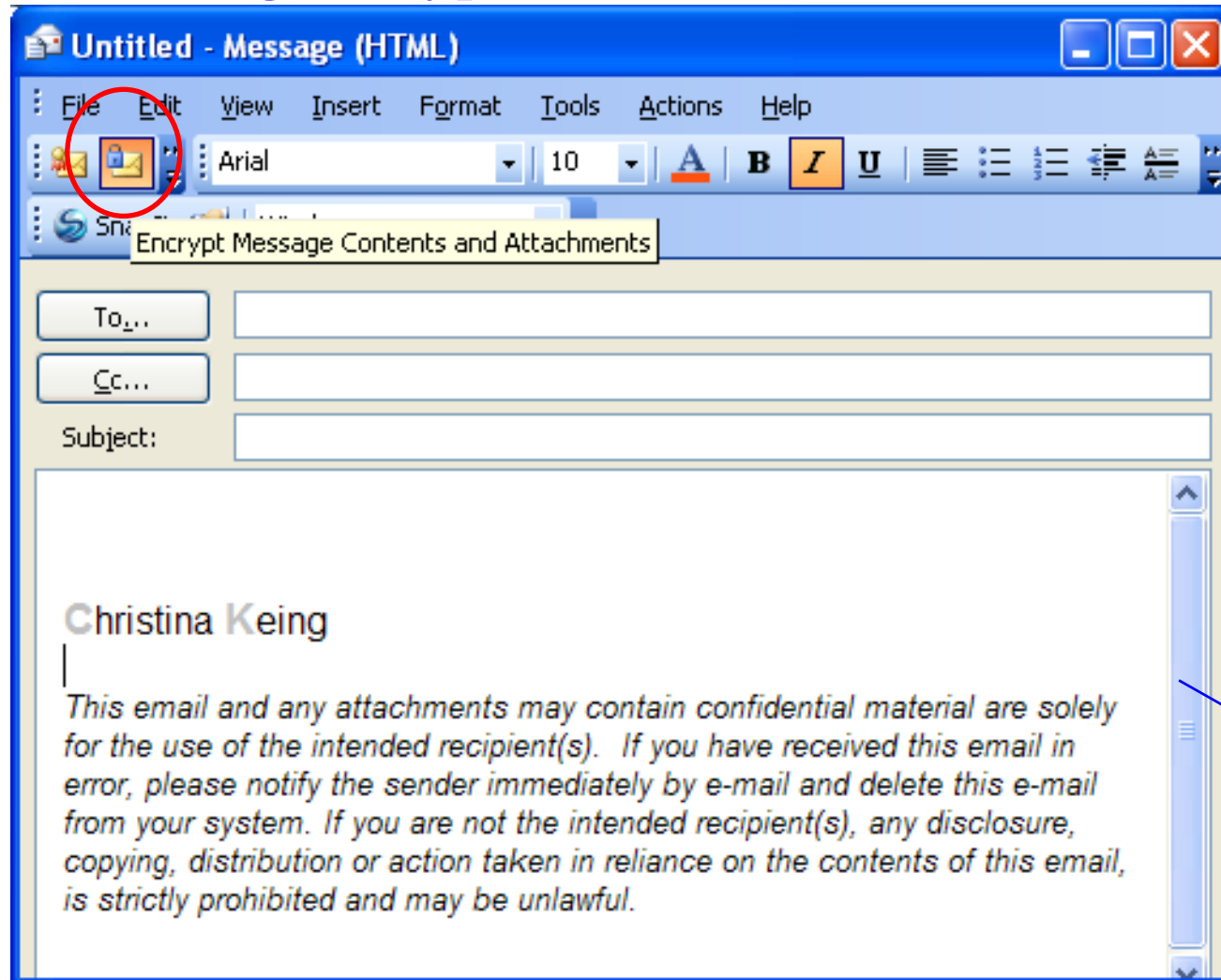
o Data encryption – MS Office



- Encrypt the file before sending through email.
- Share the password in another secure channel.
 - Common secret
 - Share in other media (phone or postal mail)

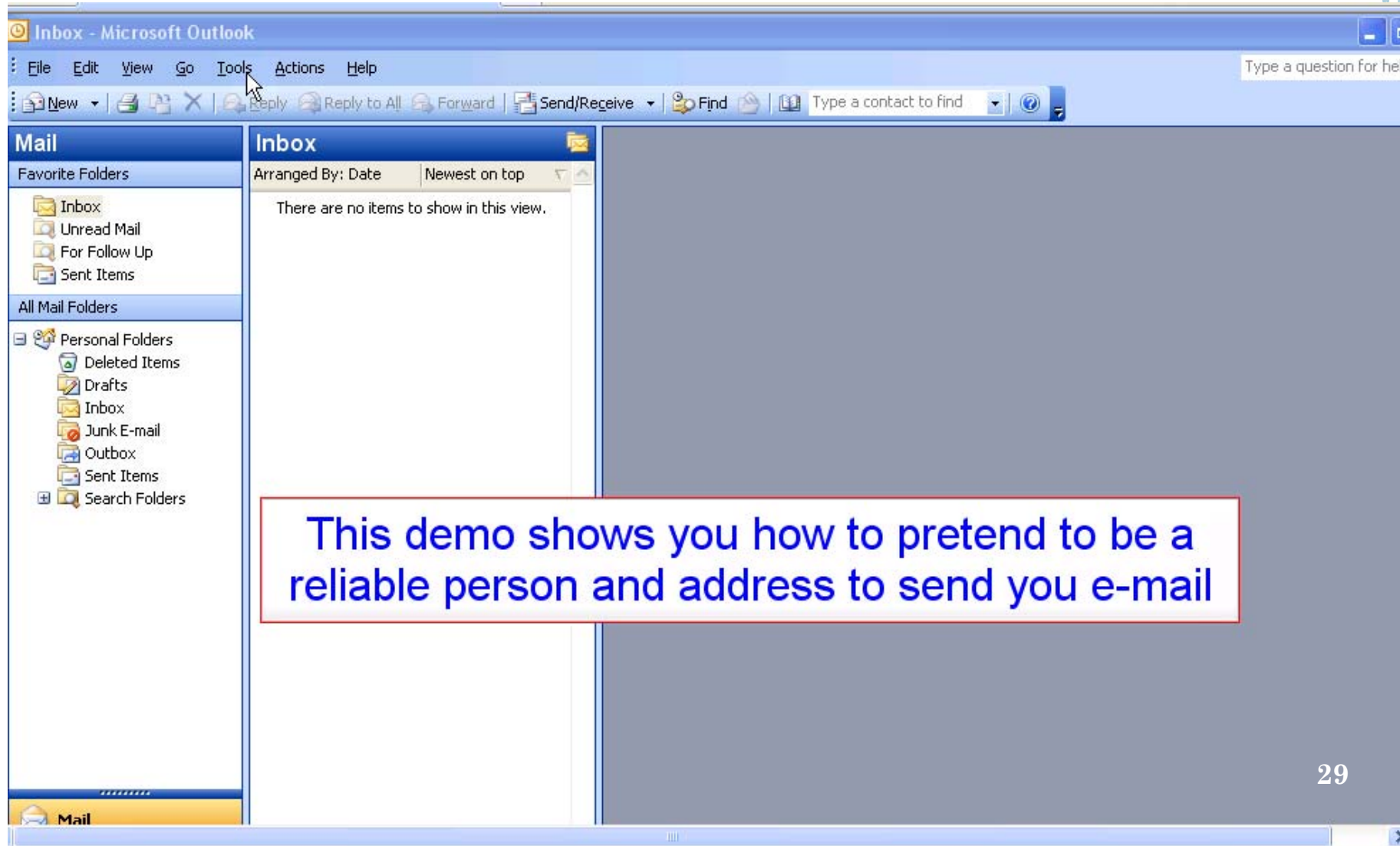
a. CARELESS MISTAKE (SENT TO A WRONG PERSON)

o Sending encrypted email with disclaimer



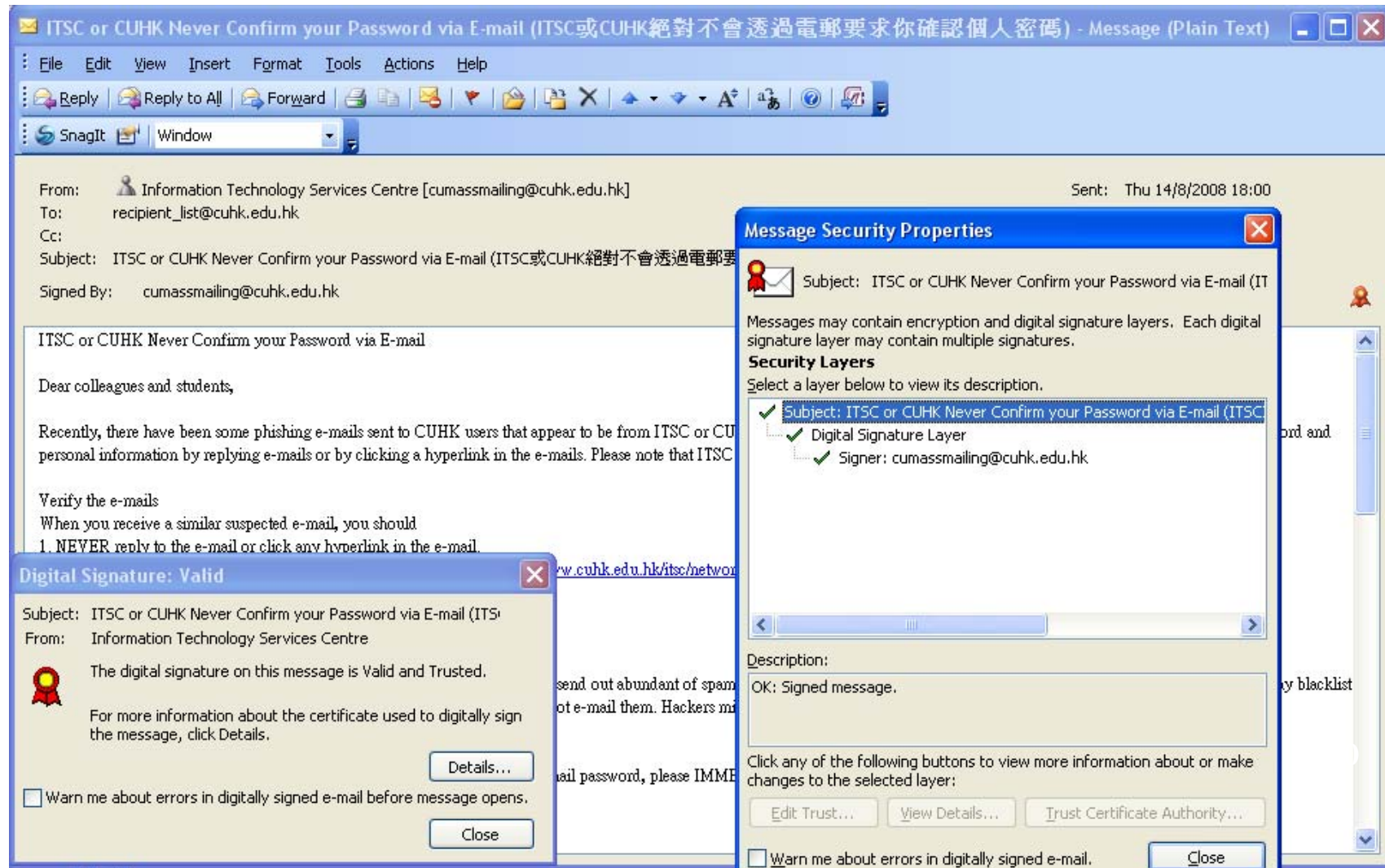
Email Disclaimer
for your reference

b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)

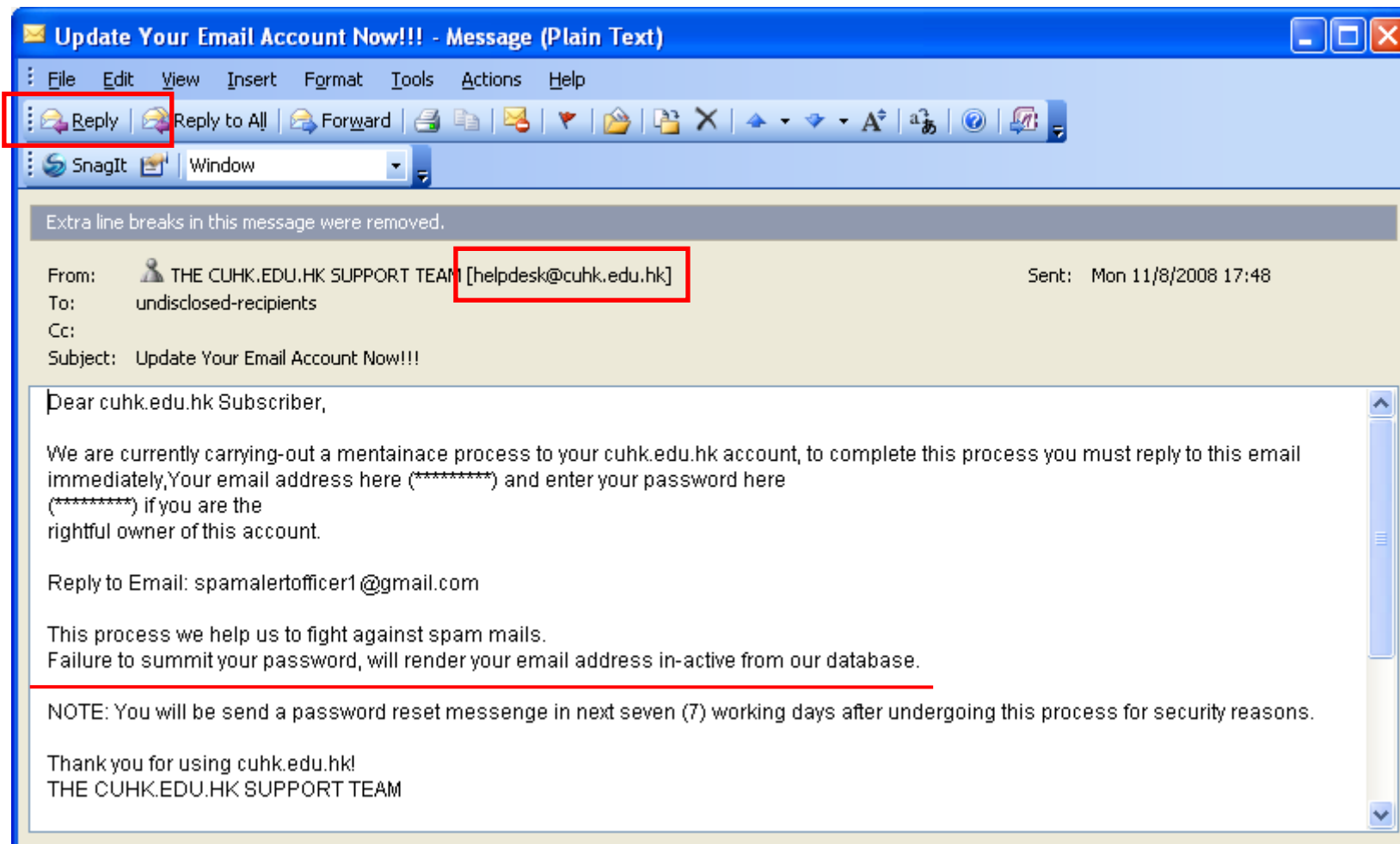


b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)

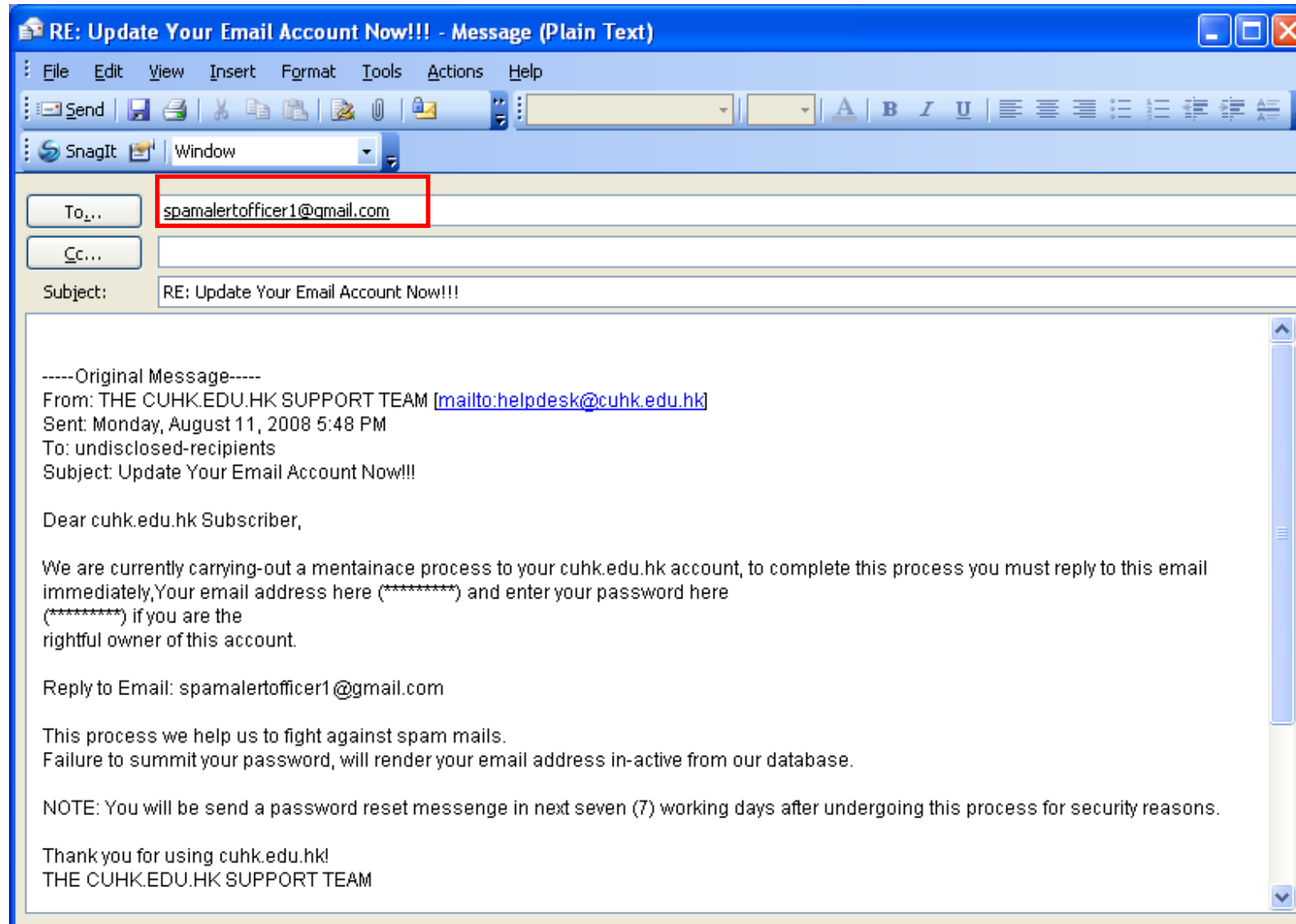
- Beware of the reply address
- Send email with digital signature



b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)



c. PHISHING EMAIL



c. PHISHING EMAIL

Phishing IQ Test by SonicWALL - Mozilla Firefox

File Edit View History Bookmarks Yahoo! Tools Help

http://www.sonicwall.com/phishing/index.html

SONICWALL Comprehensive Internet Security™

SonicWALL Phishing IQ Quiz

SonicWALL Phishing IQ Test (Formerly the MailFrontier Phishing IQ Test)

Chances are that in the past week you've received an e-mail in your inbox that pretends to be from your bank, e-commerce vendor, or other on-line site. Hopefully you've realized that many times this e-mail is fake - a phishing e-mail. The sender (phisher) of these fake e-mails wants you to click on the link in the e-mail and go to a phishing Web site - which will look just like the Web site of the company being phished. Once on the phishers Web site they hope to obtain your account, financial, credit and even identity information. Of course not every e-mail you receive is a phish. In fact you should expect your bank or e-commerce vendor to send you legitimate e-mail. But how can you tell the difference? Well that's what the Phishing IQ test is all about - give it a try.

Instructions

To begin click the "Start the Test" button below. Each question will be displayed one at a time in a browser window and you decide if the e-mail is a "Phish" or "Legitimate." When you have completed the test you'll get a score along with a chance to see "why" a question was a phish or legitimate. Good Luck!

[Start the Test](#)

Phishing Facts

- 886** – The average dollar loss per Phishing Victim (Gartner, Dec 17, 2007)
- 3.6 Billion** – The total dollar loss of all phishing victims over a 1 year period (Gartner, Dec 17, 2007)
- 3.2 Million** – The number of people who fell victims to phishing scams over that same 1 year period (Gartner, Dec 17, 2007)
- 8.5 Billion** – The estimated number of phishing e-mails sent world-wide each month (SonicWALL, 2008)
- 32,414** – The number of phishing web sites that were operational in

Done McAfee SiteAdvisor

TIPS TO PREVENT INFORMATION LEAKAGE FROM

2. EMAIL

a. Careless mistake (wrongly sent to another person)

b. Wrongly trust the email sender (email spoofing)

c. Phishing emails

TIPS TO PREVENT INFORMATION LEAKAGE FROM

2. EMAIL

a. Encrypt confidential file; Share the password in other media; Add email disclaimer

b. Beware of the reply email address; Use and read digital email signature

c. Don't click any link and reply to suspicious email; Never tell your password to anyone

TIPS TO PREVENT INFORMATION LEAKAGE FROM

2. EMAIL

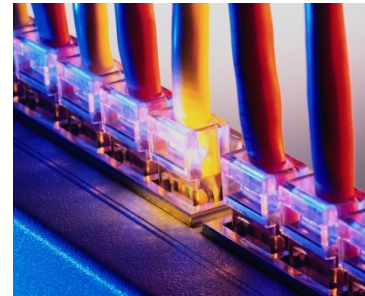


- Take a few minutes to apply your CUHK digital certificate NOW!
- <https://ca.itsc.cuhk.edu.hk/ca/request/>

HOW INFORMATION LEAKS FROM

3. NETWORK

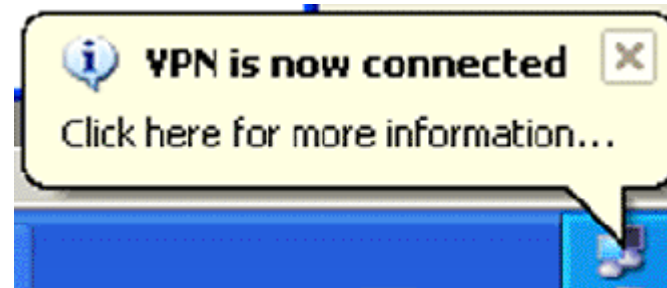
a. Sniff especially for wireless network



TIPS TO PREVENT INFORMATION LEAKAGE FROM

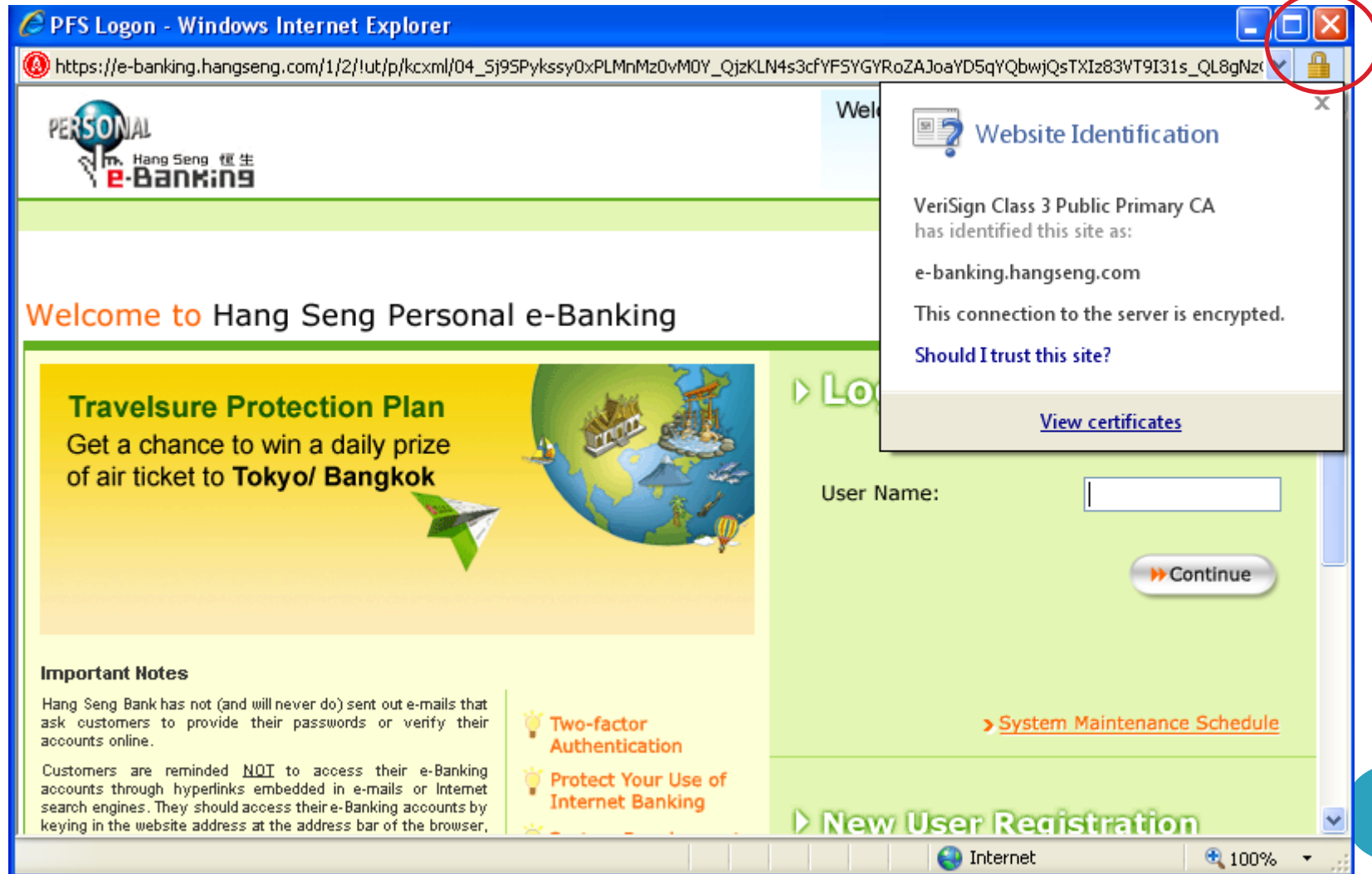
3. NETWORK

- Use of VPN especially for wireless network
- If you use the Wi-Fi service at CUHK, remember to connect Virtual Private Network as well which supports encryption.



TIPS TO PREVENT INFORMATION LEAKAGE FROM

3. NETWORK



TIPS TO PREVENT INFORMATION LEAKAGE FROM

3. NETWORK

- Good practice
 - Do not connect wireless connections of unknown source.
 - Turn off unnecessary wireless connections.
 - Do not enable both wireless and wired network interface at the same time.
 - For sending critical information, it is more safe to send through wired network over encrypted site(https) and check the certificate.
 - More information
<http://www.cuhk.edu.hk/itsc/about/bestpractices-wlan.html>

HOW INFORMATION LEAKS FROM

4. PORTABLE DEVICES

- a. Left or stolen
- b. Broken



a. LEFT OR STOLEN

- Data encryption – Hardware



- USB drive

- e.g. Stealth MXI about \$2000 for 4GB

- Notebook

- e.g. Dell Latitude D630 Notebook about \$7500

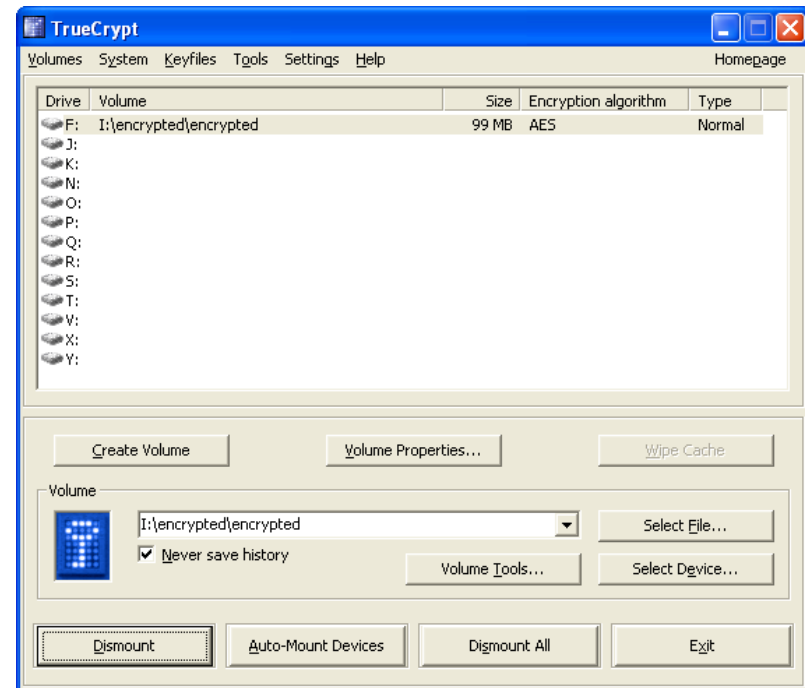
- This solution is more expensive but most convenient and fast



a. LEFT OR STOLEN

- Data encryption – Software
e.g. TrueCrypt

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



- This is a cheaper but slower solution.
- It can be used for PC, notebook and storage device.
- It supports to encrypt entire partition, entire drive or storage device

b. BROKEN

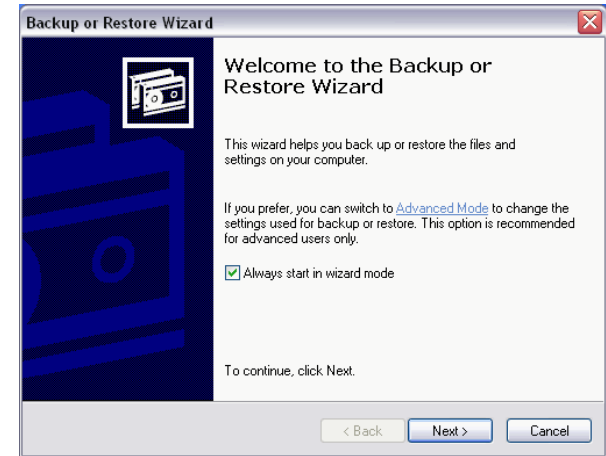
- Safely remove your USB drives

- Do regular backup and testing

- e.g. Microsoft built-in “Backup or Restore Wizard”

- e.g. SynToy from Microsoft

- <http://www.microsoft.com/downloads/details.aspx?FamilyId=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en>



b. BROKEN

Demonstration of SynToy

[HTTP://WWW.MICROSOFT.COM/DOWNLOADS/DETAILS.ASPX?FAMILYID=E0FC1154-C975-4814-9649-CCE41AF06EB7&DISPLAYLANG=EN](http://www.microsoft.com/downloads/details.aspx?familyid=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en)

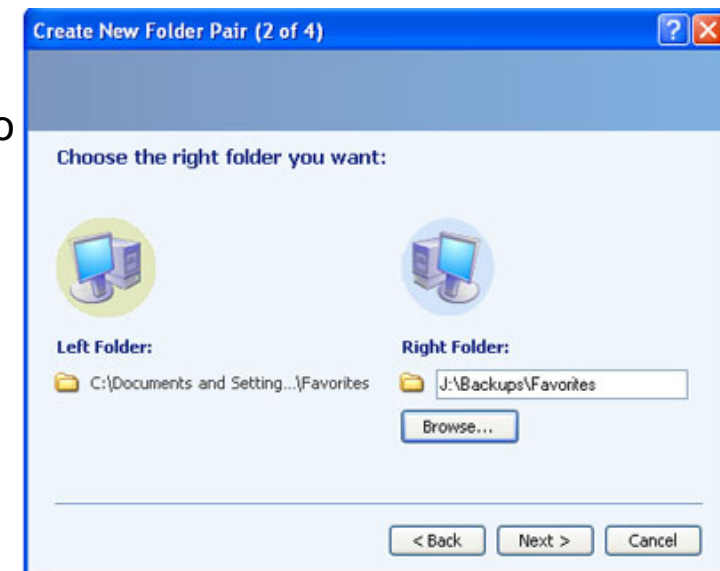
Synchronize: New and updated files are copied both ways. Renames and deletes in one folder is repeated on the other.

Echo: New and updated files are copied left to right. Renames and deletes on the left are repeated on the right.

Subscribe: Updated files on the right are copied to the left if the file name already exists on the left.

Contribute: New and updated files are copied left to right. Renames on the left are repeated on the right. Similar to Echo, except there are no deletions.

Combine: New and updated files are copied both ways. Renamed and deleted files are ignored



TIPS TO PREVENT INFORMATION LEAKAGE FROM

4. PORTABLE DEVICES

a. Left or stolen

b. Broken

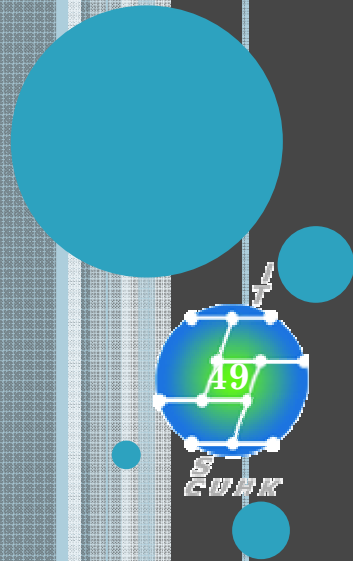
TIPS TO PREVENT INFORMATION LEAKAGE FROM

4. PORTABLE DEVICES

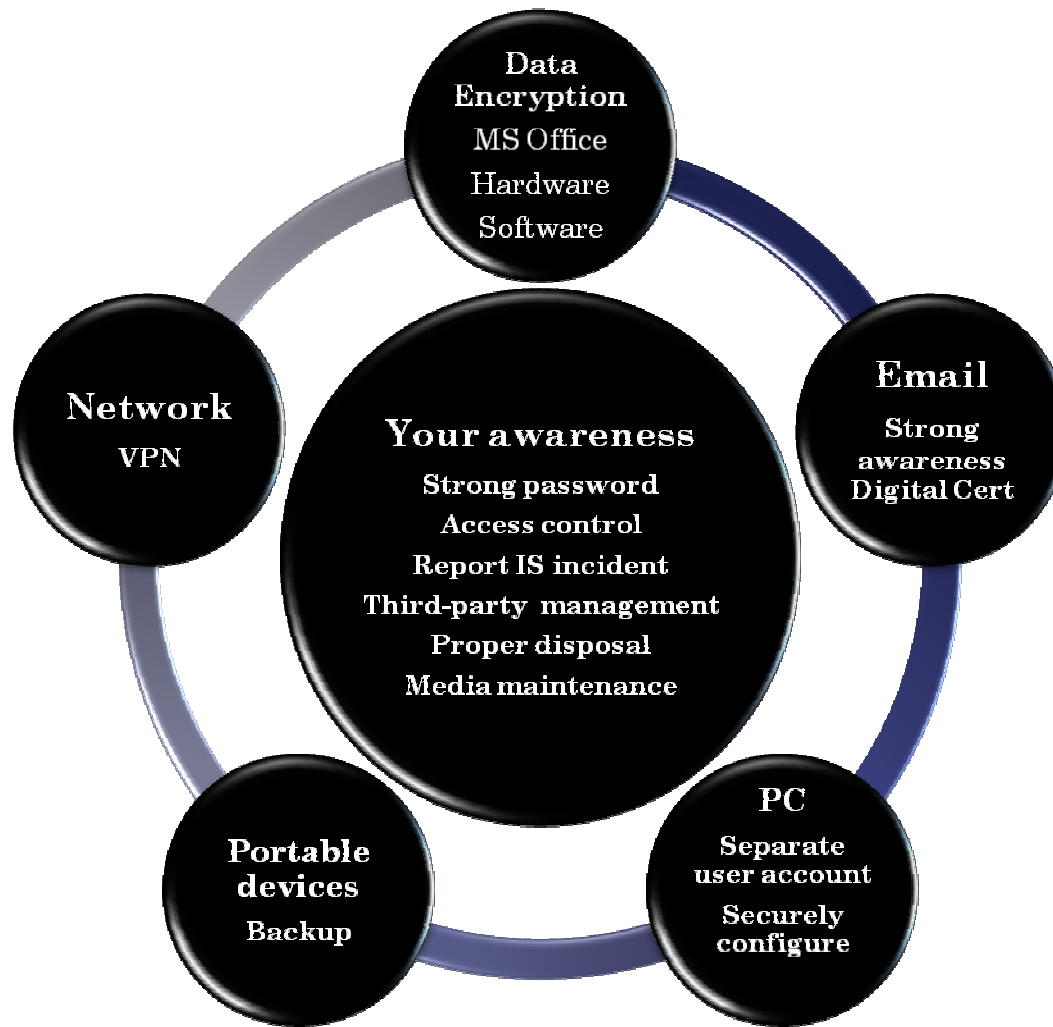
a. Use of encryption.

b. Safely remove your device; regular backup and test the restore.

TIPS IN PREVENTING INFORMATION LEAKAGE

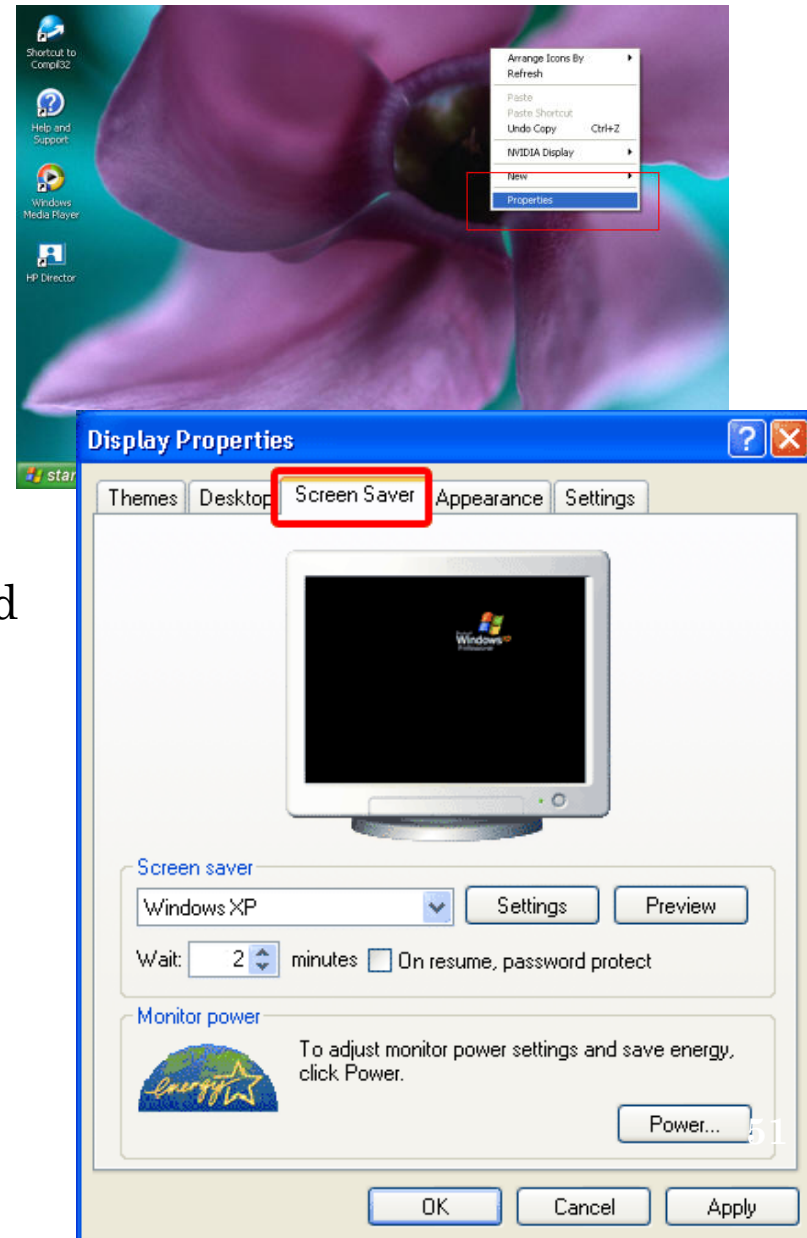


TIPS IN PROTECTING ELECTRONIC INFORMATION

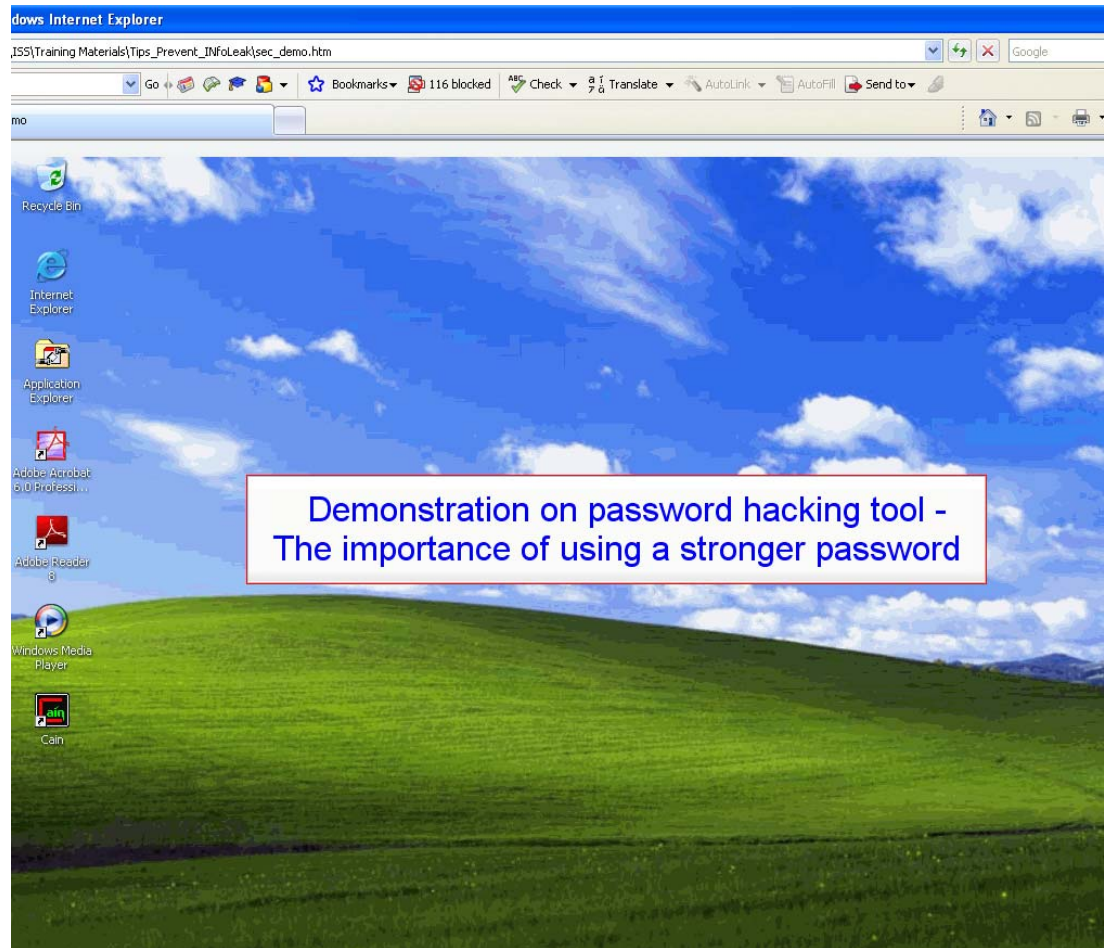


TIPS IN PROTECTING ELECTRONIC INFORMATION

- Your awareness
- Access control
 - e.g. Screen Saver
- Strong password
 - At least eight characters composed of random letters, digits and symbols;
 - Use different sets of password in different systems, and;
 - Never use dictionary words and personal related information such as name, date, telephone number, HKID and user ID, etc.



DEMONSTRATION OF BRUTE-FORCE ATTACK



Password checker

<http://www.microsoft.com/protect/yourself/password/checker.msp>

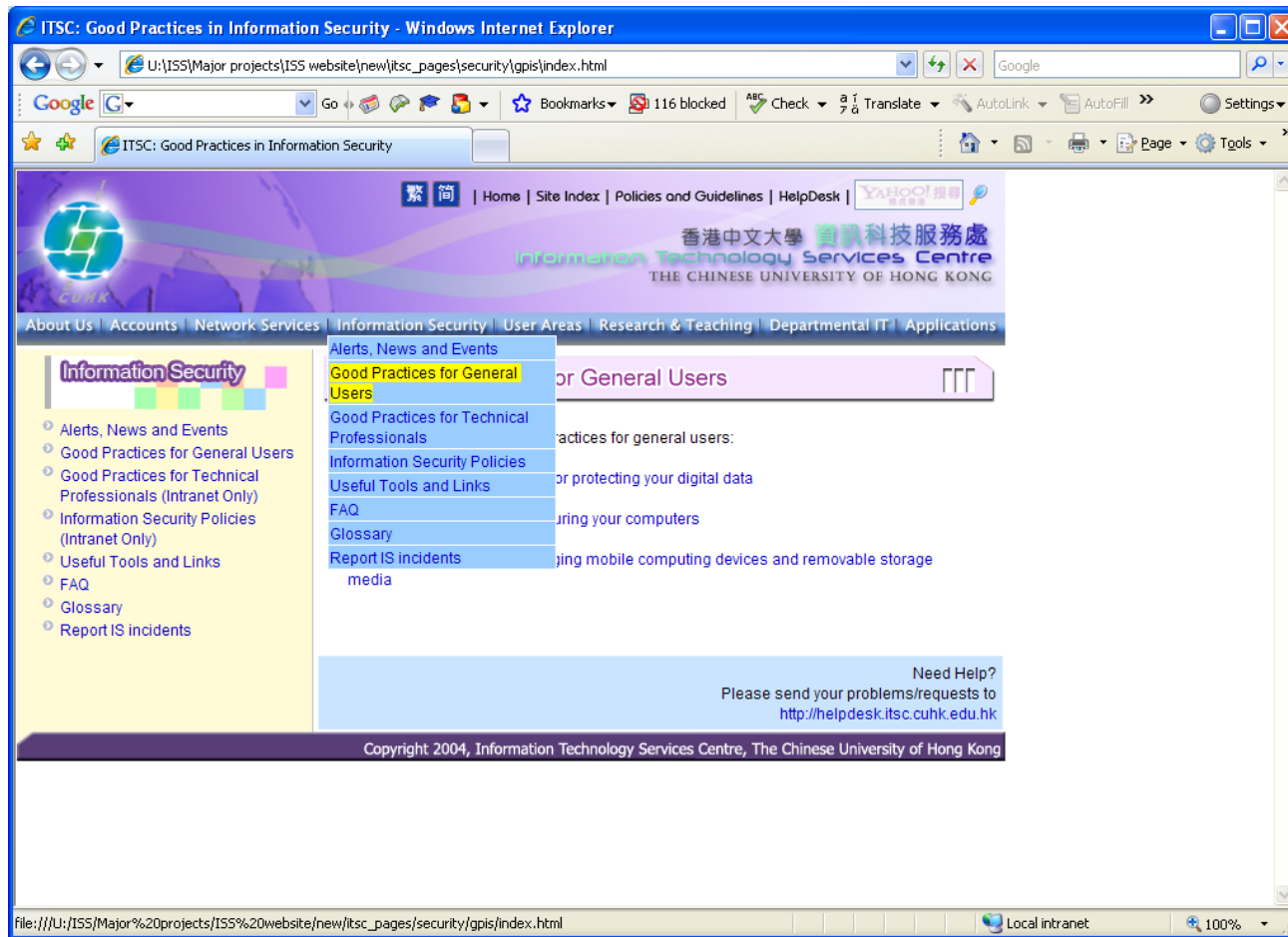
TIPS IN PROTECTING ELECTRONIC INFORMATION

- 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>
- Third-party management
 - Sign confidentiality agreement

TIPS IN PROTECTING ELECTRONIC INFORMATION

- Your awareness
- Proper disposal
 - Degaussing the devices
 - Physically destroying them, or by using a data cleaner to erase data inside
 - e.g. Blancco Data Cleaner
<http://www.cuhk.edu.hk/itsc/compenv/license/blancco.html>
- Media maintenance
 - Buy device which supports hardware data encryption
 - Remove hard disk before repairing
 - Clean up hard disk
 - Sign confidentiality agreement

FOR MORE INFORMATION:



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