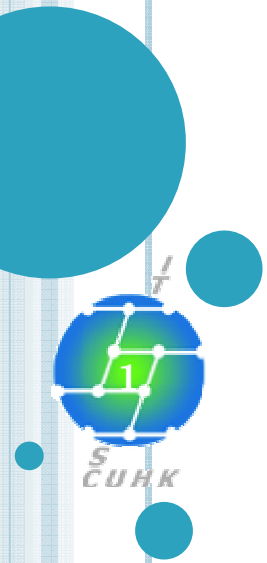
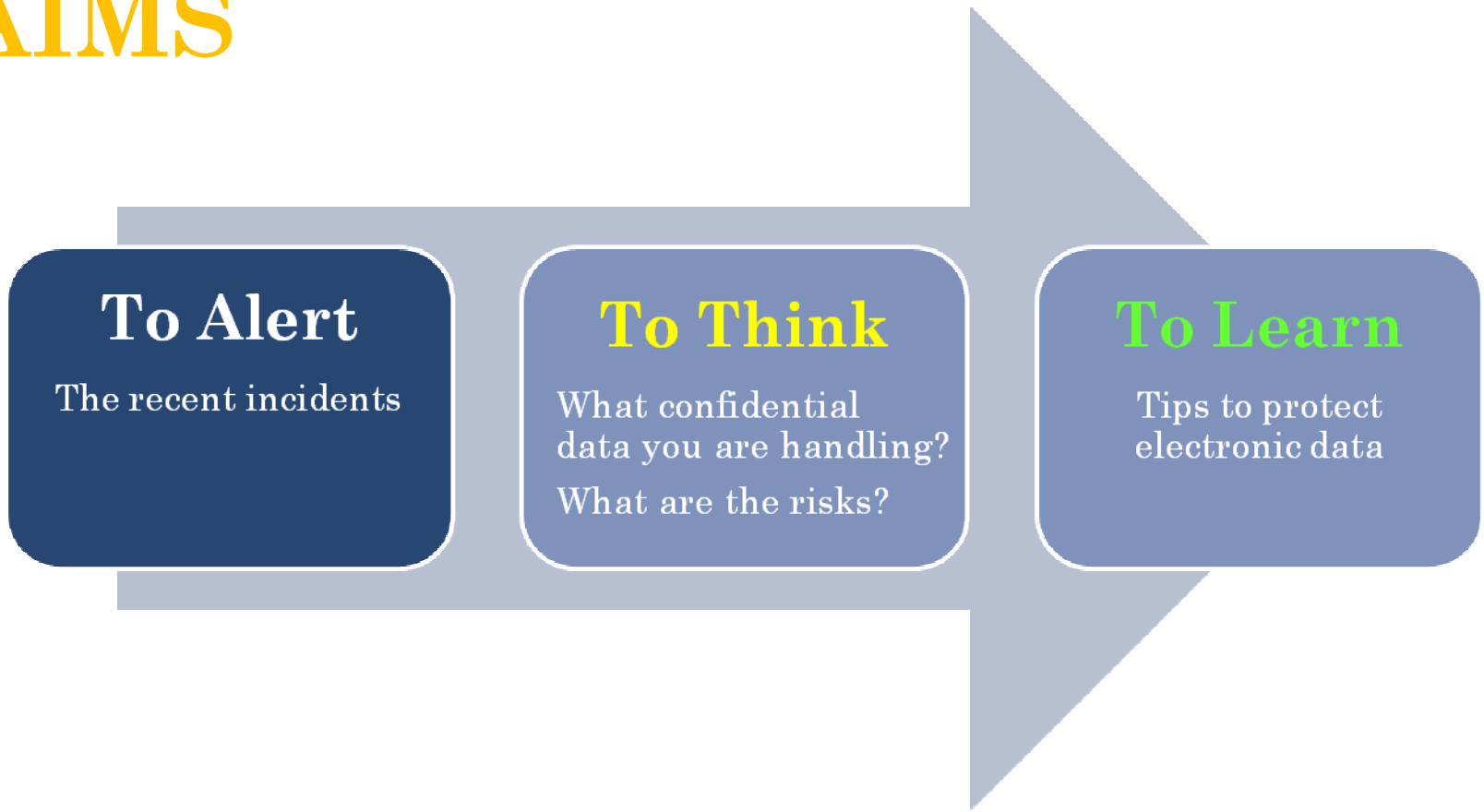
TIPS IN PREVENTING INFORMATION LEAKAGE



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

5 Sept 2008

AIMS

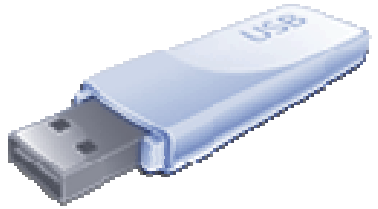

To Alert
The recent incidents
To Think
What confidential data you are handling?
What are the risks?
To Learn
Tips to protect electronic data

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&con_type=1&d_str=20080506&sear_year=2008

RECENT INCIDENTS

27 May 2008

Hong Kong Police Force
The Government of the Hong Kong Special Administrative Region

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

Source: “Fail Forum”
http://failforum.net/forum/viewthread.php?tid=563585&extra=page%3D1

WHAT INFORMATION TO PROTECT?

WHAT INFORMATION T 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.

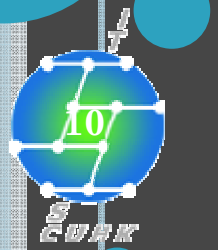
- Staff may also judge by themselves based on the regular practice and their experience.

WHAT INFORMATION TO PROTECT?

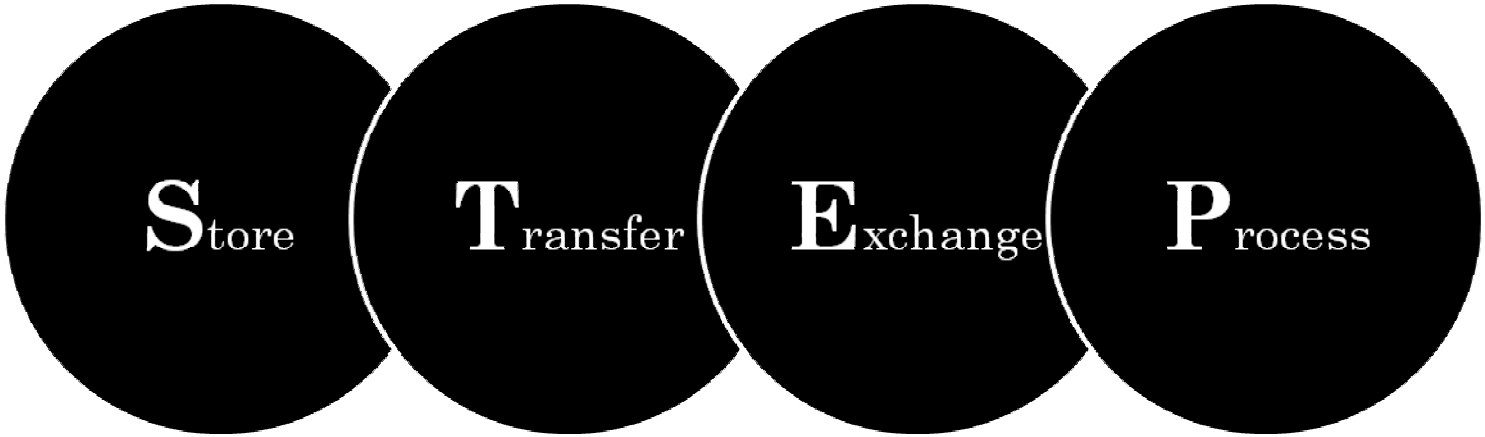
- "personal data" means any data
  - relating directly or indirectly to a living individual
  - from which it is practicable for the identity of the individual to be directly or indirectly ascertained
  - Example: name + address

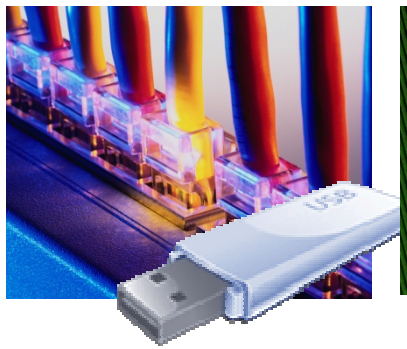
- For more information:
  - Personal Data Controlling Committee at CUHK http://www.cuhk.edu.hk/policy/pdo/
  - Personal Data (Privacy) Ordinance
  - http://www.pcpd.org.hk/english/ordinance/down.html

HOW DO WE HANDLE ELECTRONIC INFORMATION?

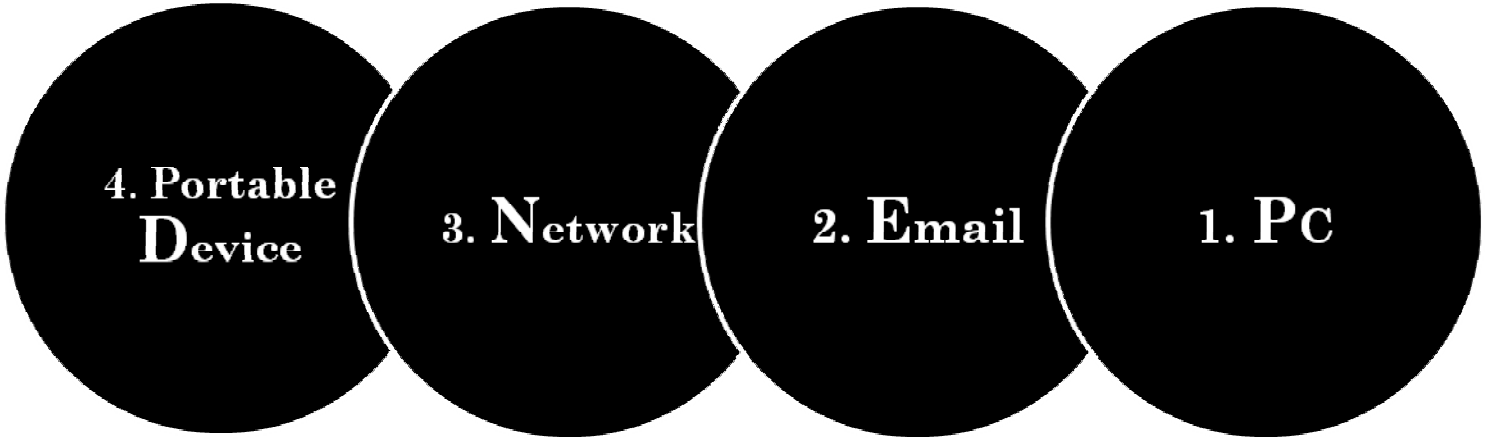


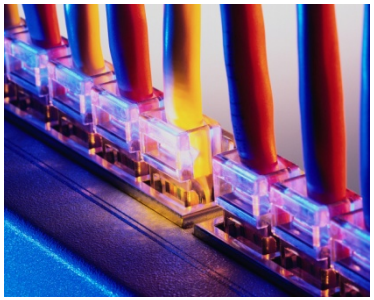
HOW WE HANDLE ELECTRONIC INFORMATION?





HOW WE HANDLE ELECTRONIC INFORMATION?





HOW INFORMATION LEAKS?

TIPS OF PREVENTION?

HOW INFORMATION LEAKS FROM

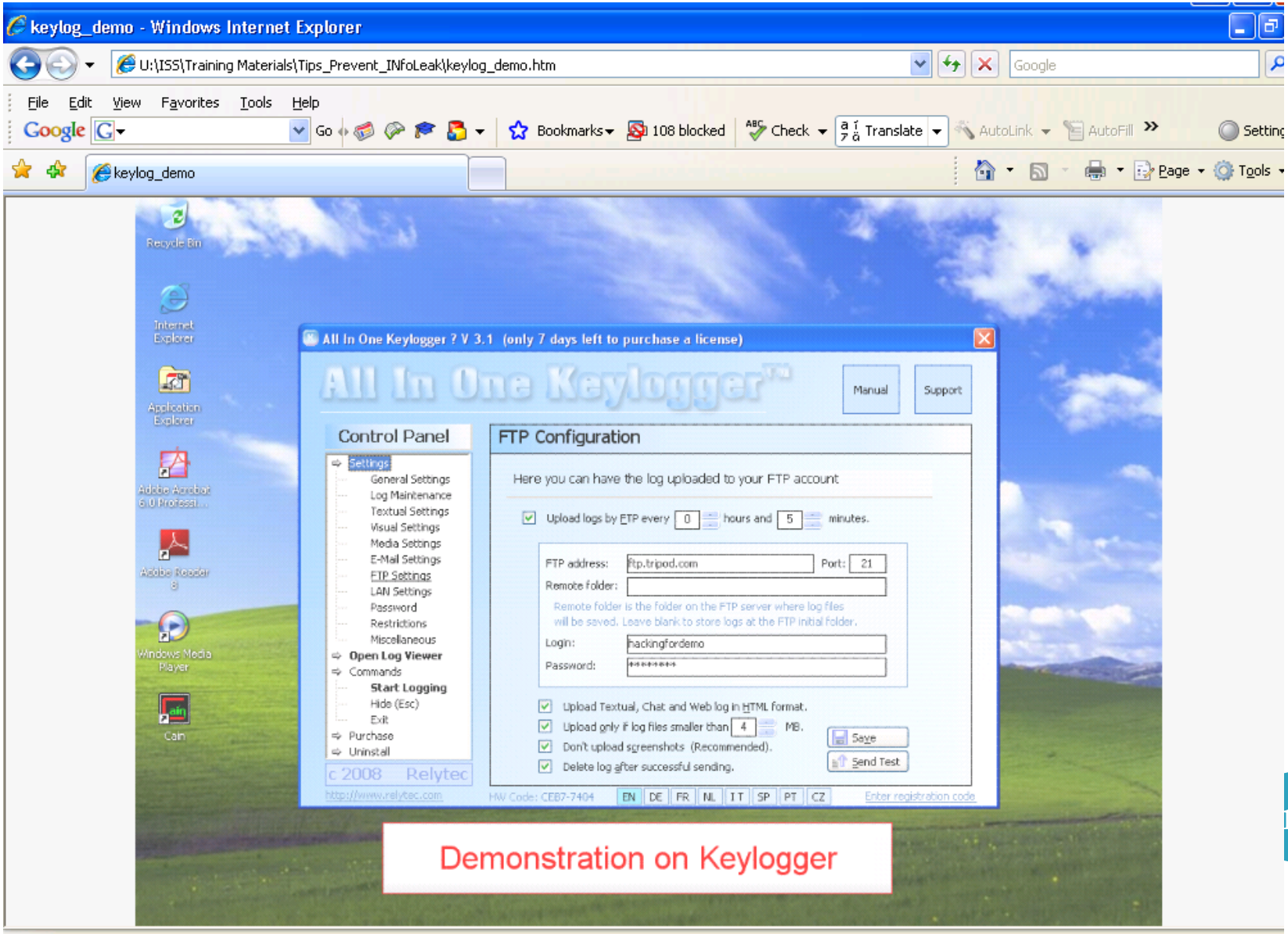
1. PC

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)



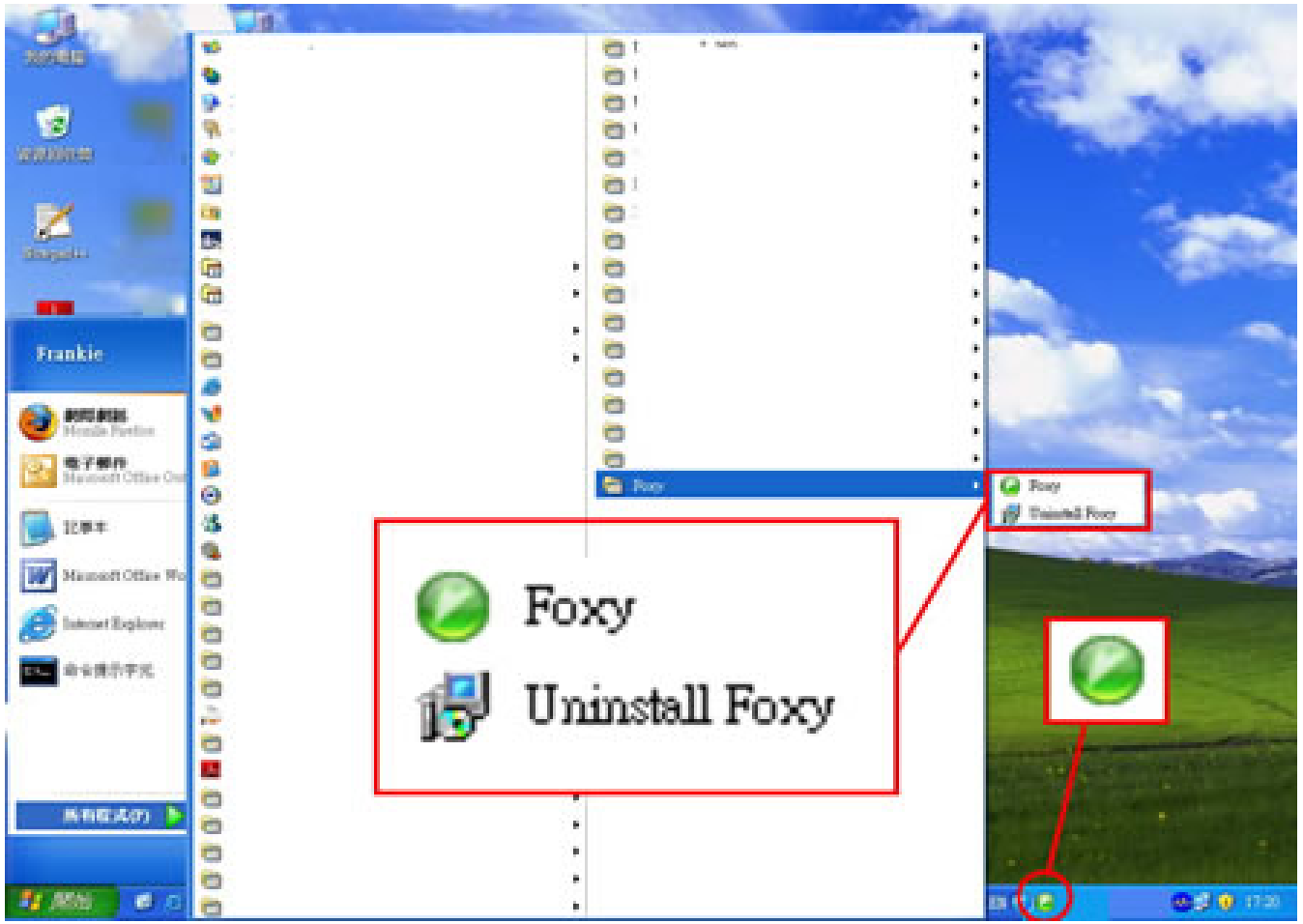
- The Best Protection is:
  - Don’t process and save confidential information in unfamiliar computers (e.g. computer in cyber café or public area)

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%

Quoted from Dr. K P Chow, Associate Director,
Centre for Information Security and Cryptograph, University of Hong Kong

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

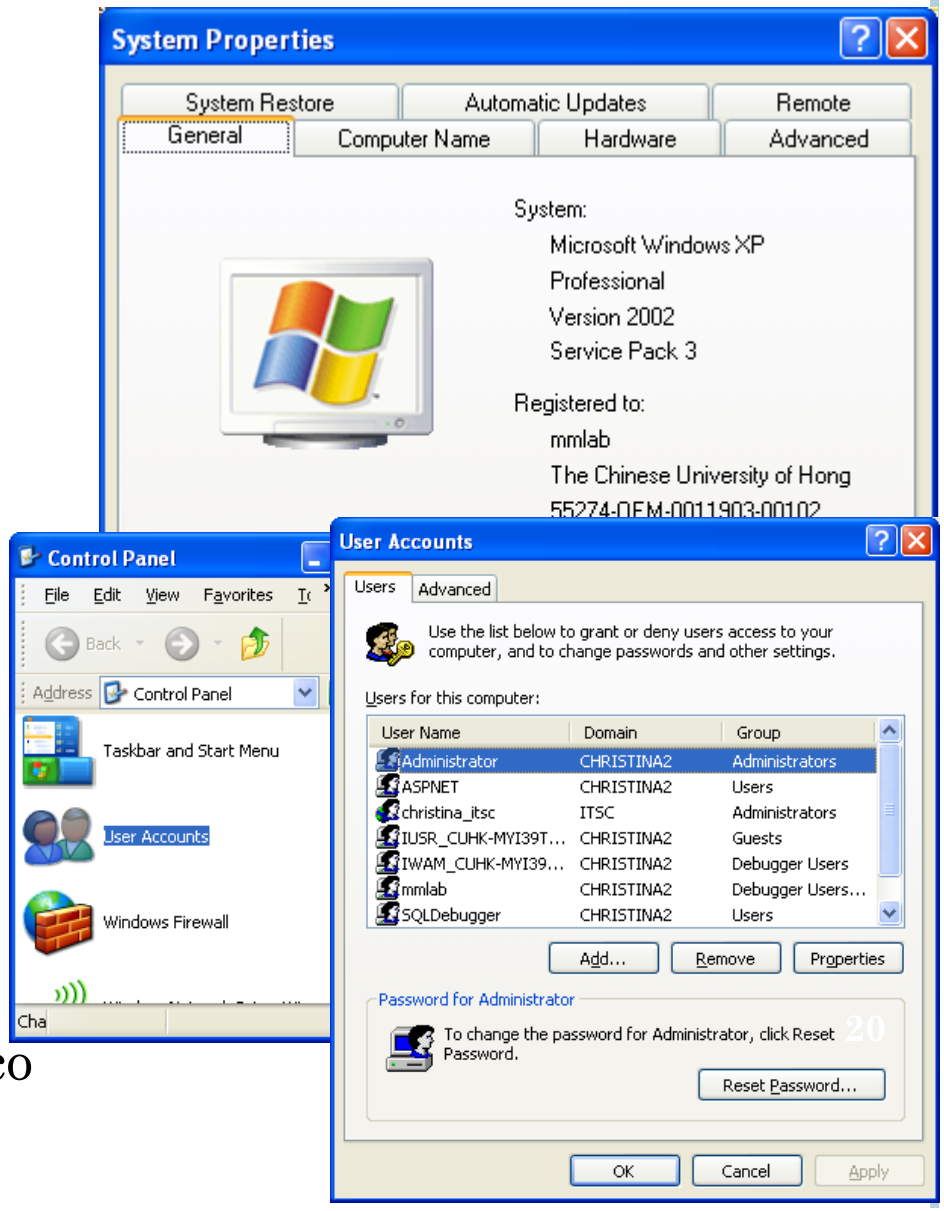


b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY)

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

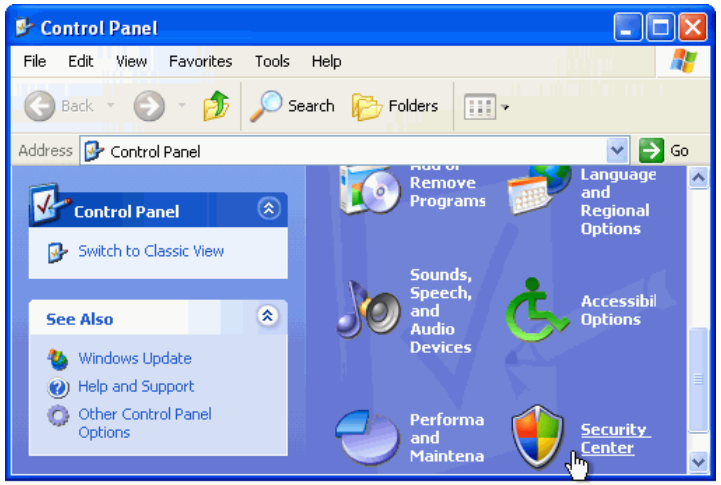
Use separate user accounts with no administrator right under a shared environment.

- 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
  - 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

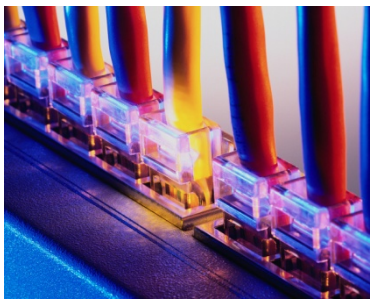
HOW WE HANDLE ELECTRONIC INFORMATION?

4. Portable Device

3. Network

2. Email

1. PC



HOW INFORMATION LEAKS FROM
2. EMAIL

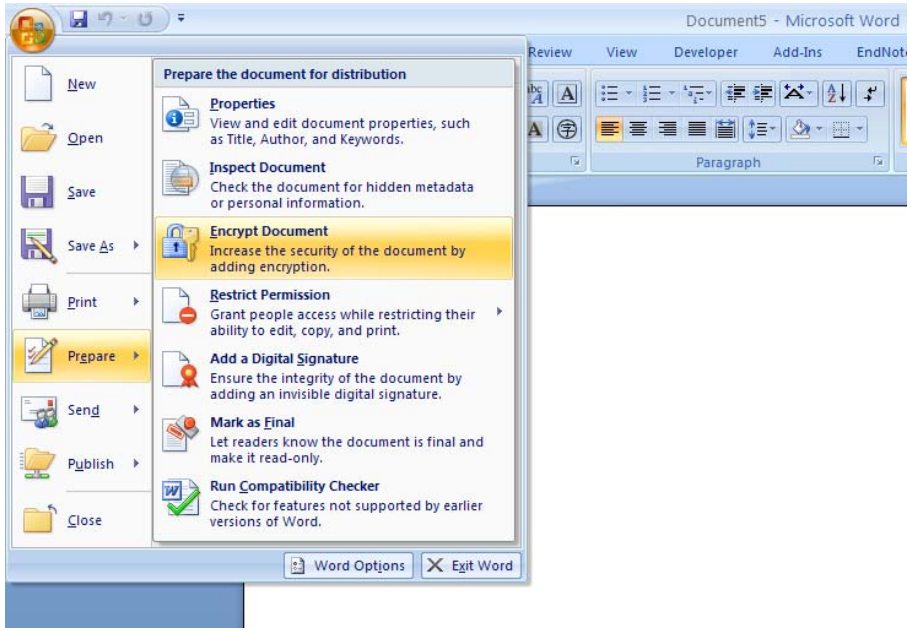
a. Careless mistake (wrongly sent to another person)

b. Wrongly trust the email sender (email spoofing)

c. Phishing email

a. CARELESS MISTAKE (SENT TO A WRONG PERSON)

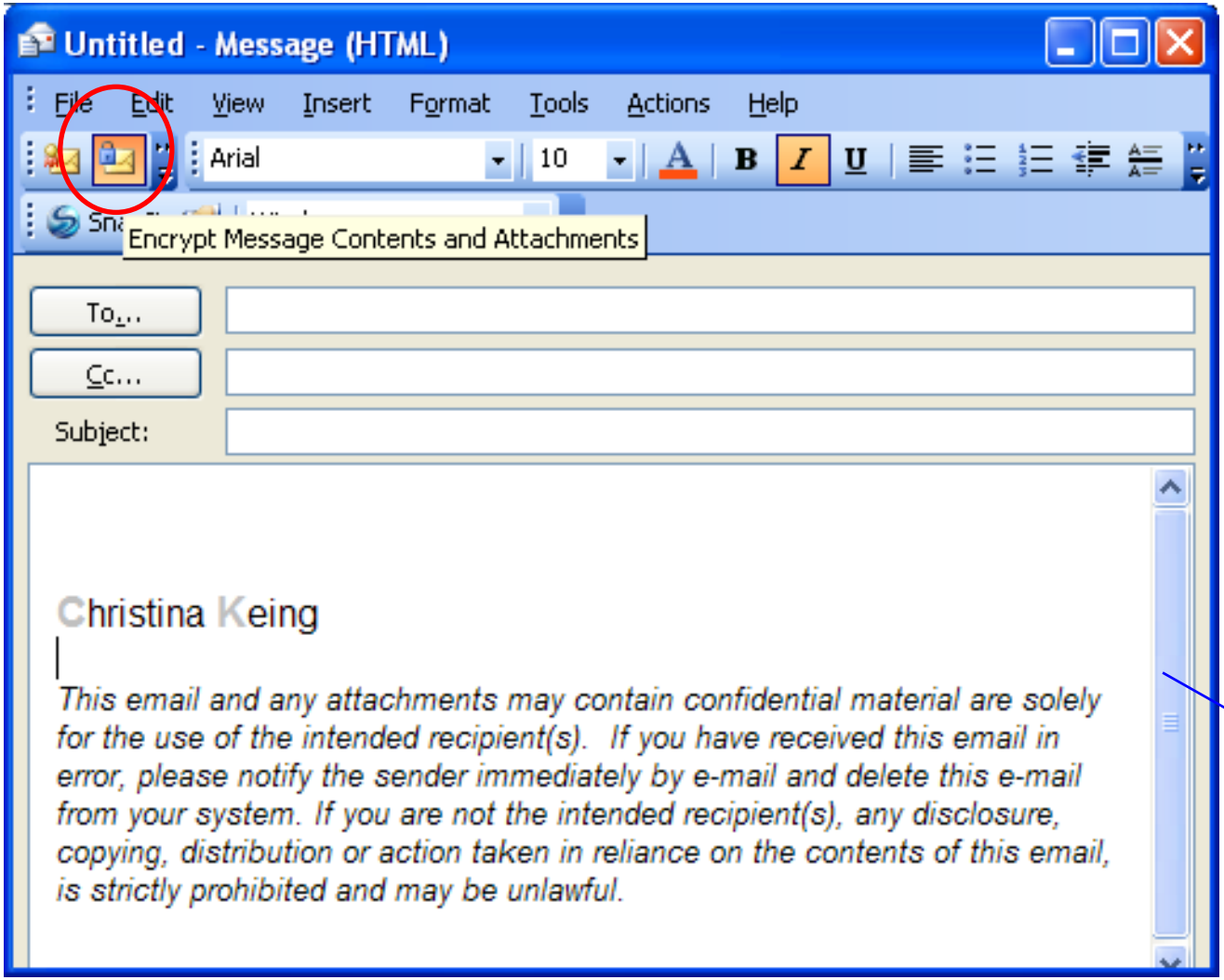
- Data encryption – MS Office



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

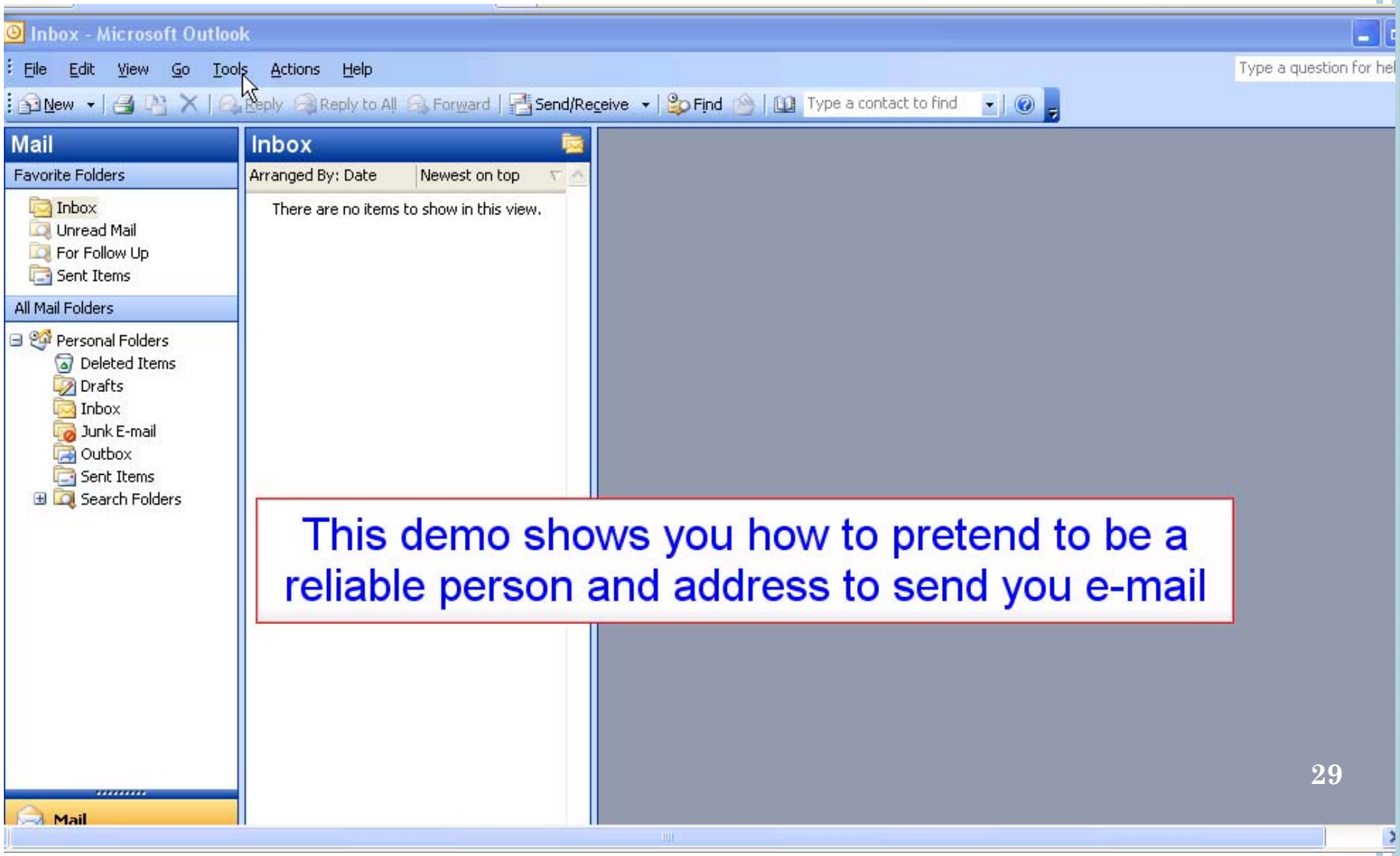
a. CARELESS MISTAKE (SENT TO A WRONG PERSON)

- Sending encrypted email with disclaimer



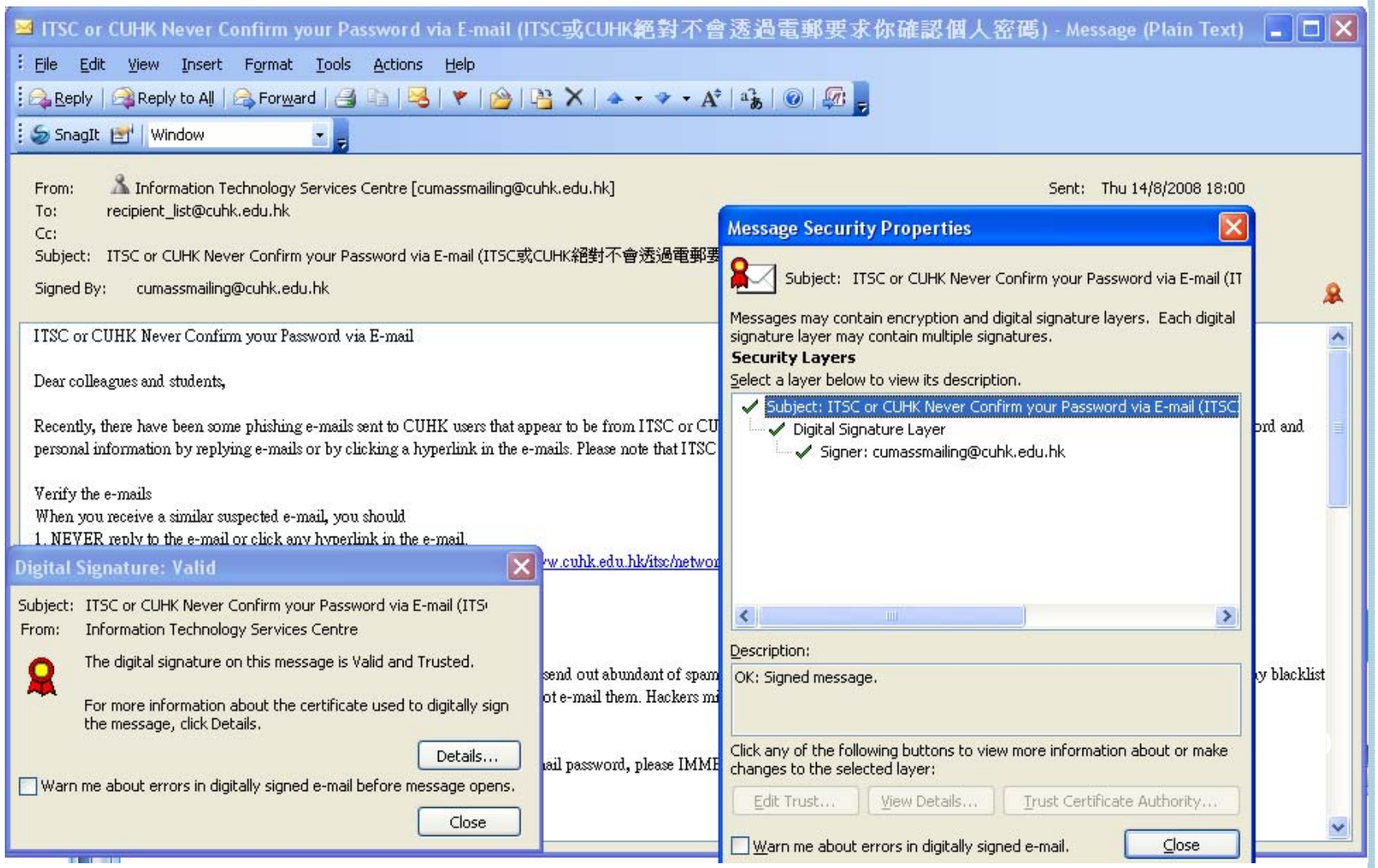
Email Disclaimer for your reference

b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)

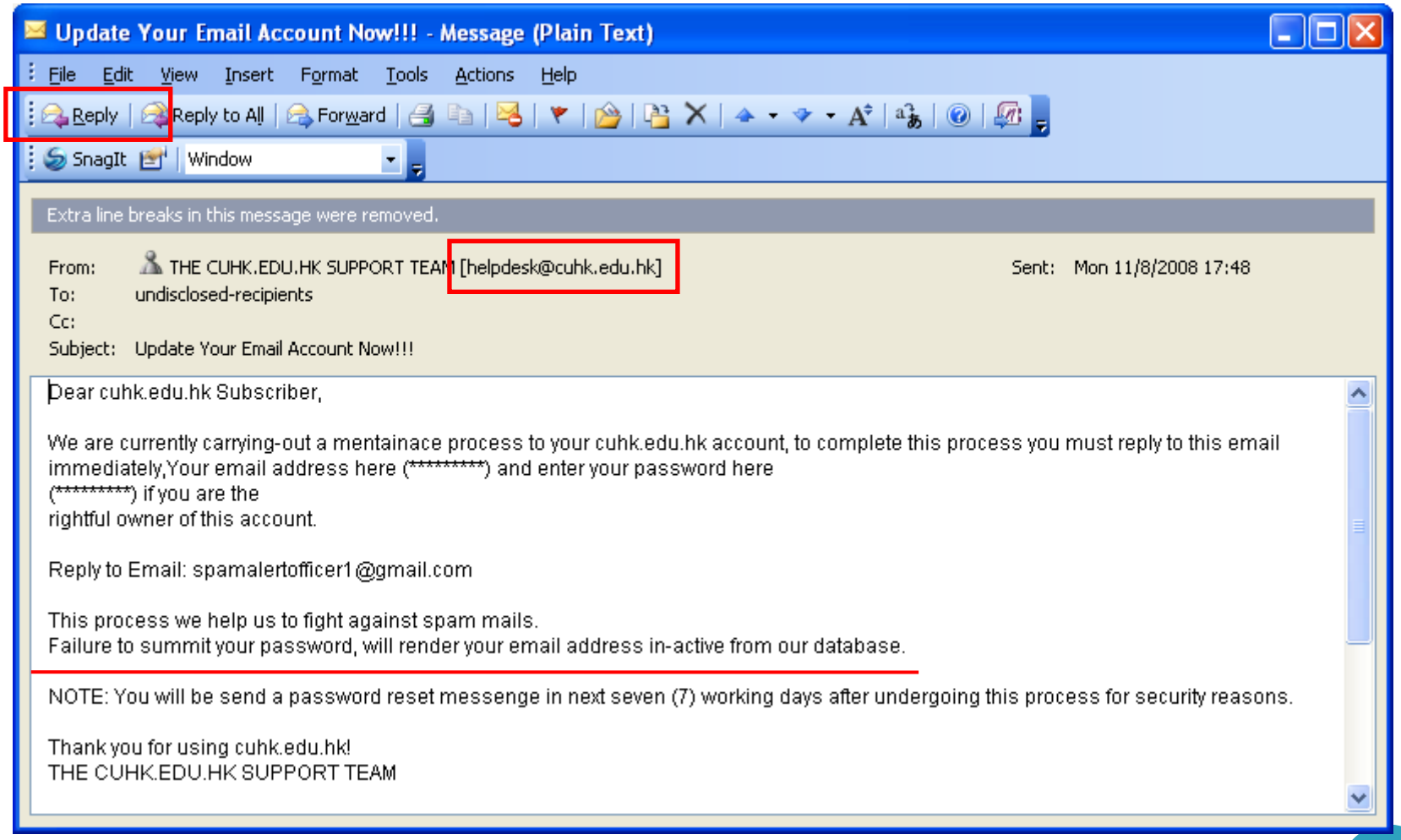


b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)

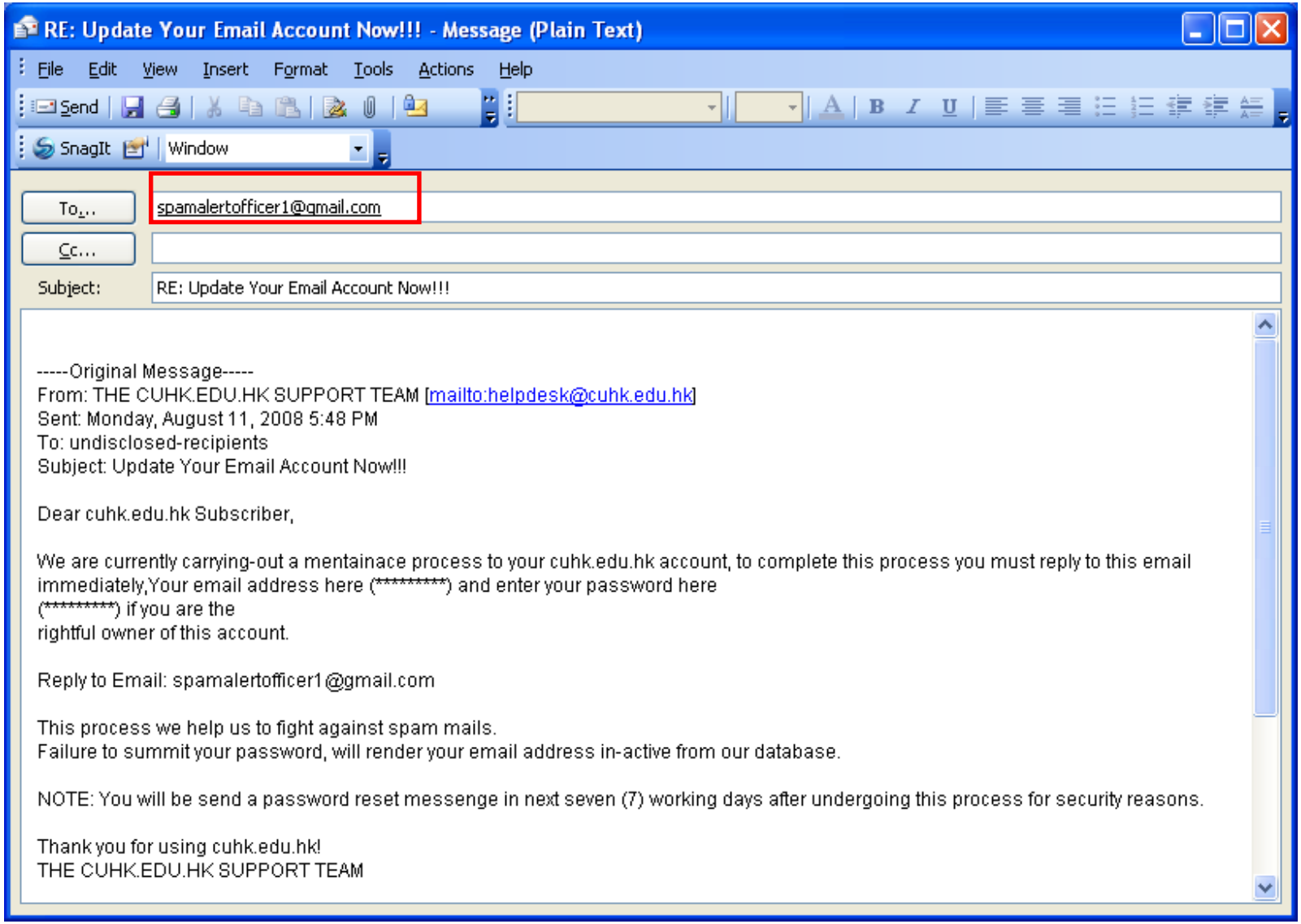
- Beware of the reply address
- Send email with digital signature



b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)



c. PHISHING EMAIL



c. PHISHING EMAIL

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

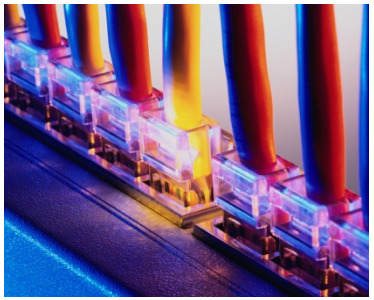
TIPS TO PREVENT INFORMATION LEAKAGE FROM

2. EMAIL

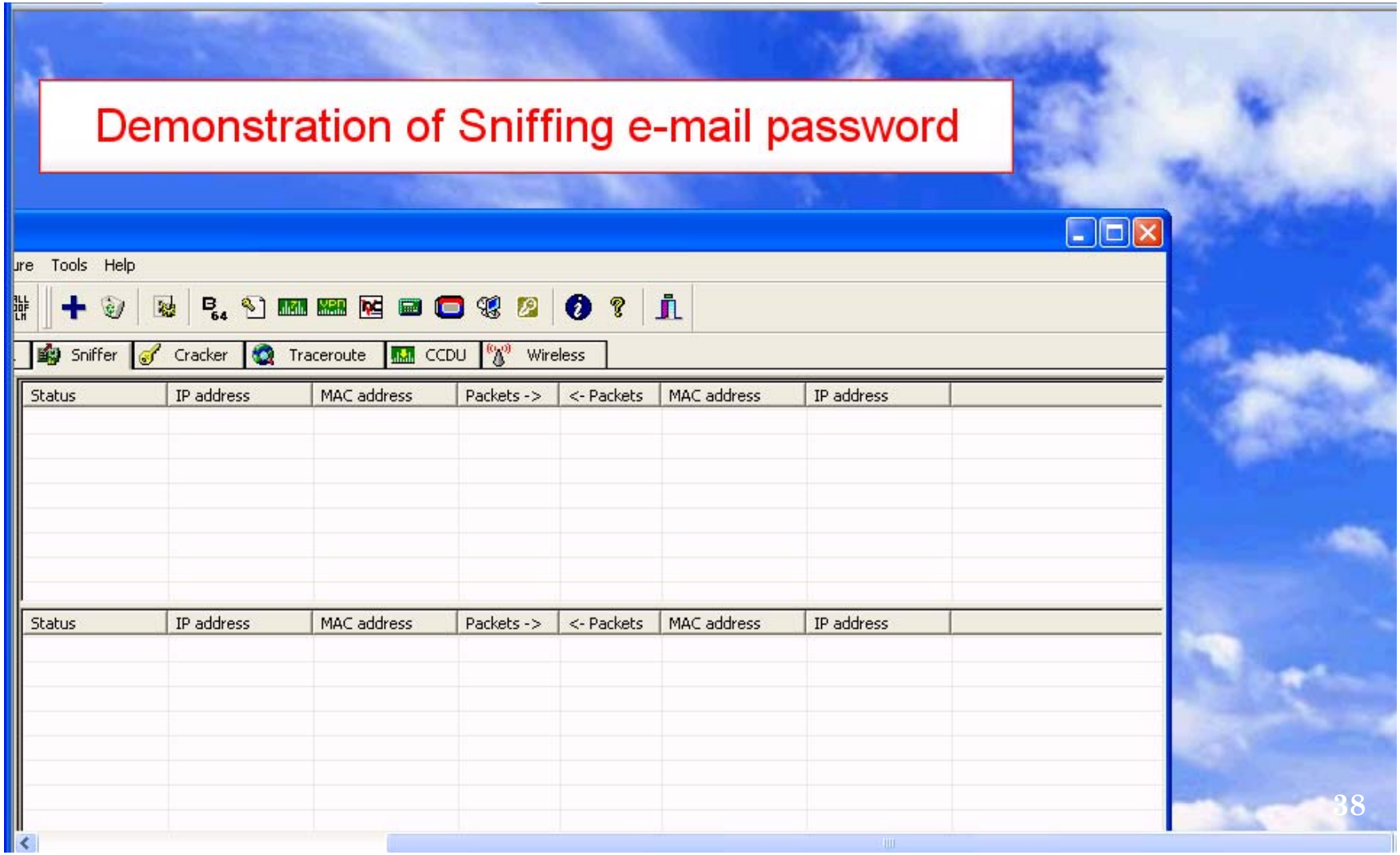
- Take a few minutes to apply your CUHK digital certificate NOW!
- https://ca.itsc.cuhk.edu.hk/ca/request/

HOW INFORMATION LEAKS FROM
3. NETWORK

a.Sniff especially for wireless network



a. SNIFF ESPECIALLY FOR WIRELESS NETWORK

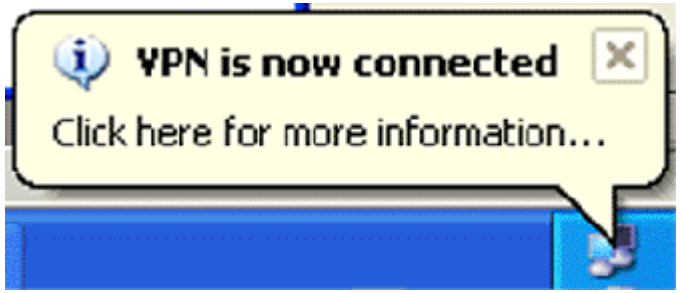


TIPS TO PREVENT INFORMATION LEAKAGE FROM

3. NETWORK

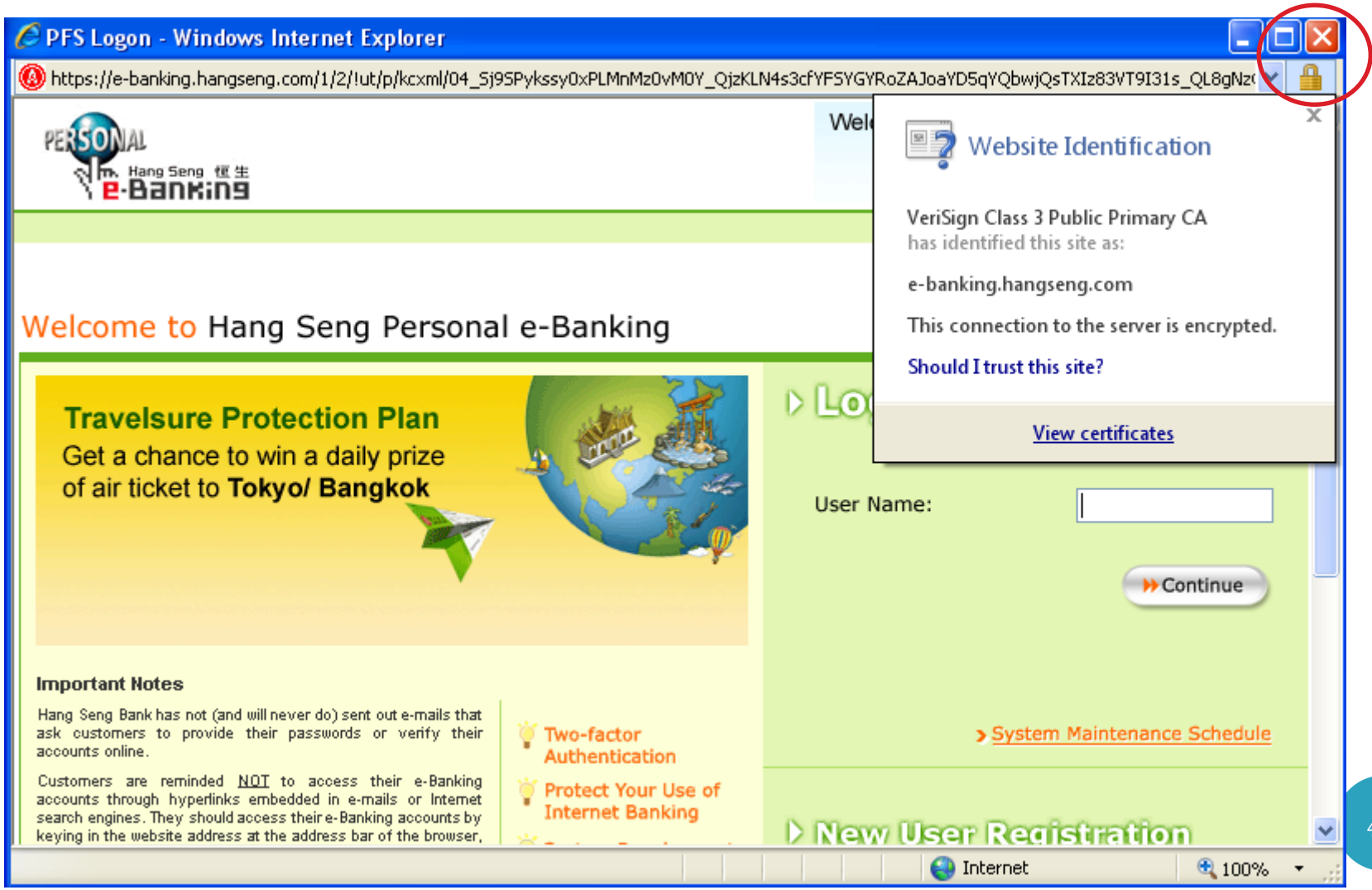
- Use of VPN especially for wireless network

- 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

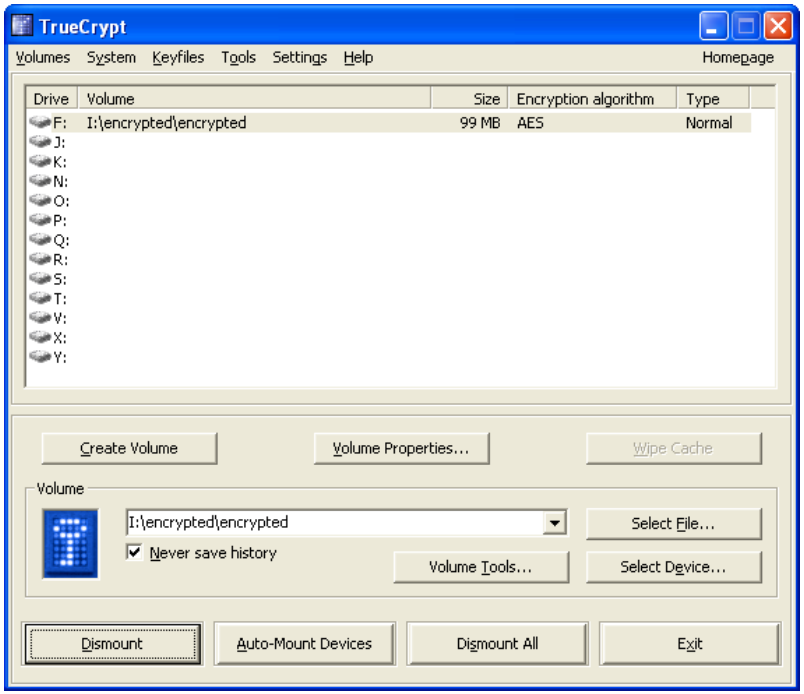
- USB drive
  - e.g. Stealth MXI about $2000 for 4GB
- Notebook
  - e.g. Dell Latitude D630 Notebook about $7500
- This solution is more expensive but most convenient and fast

a. LEFT OR STOLEN

- Data encryption – Software

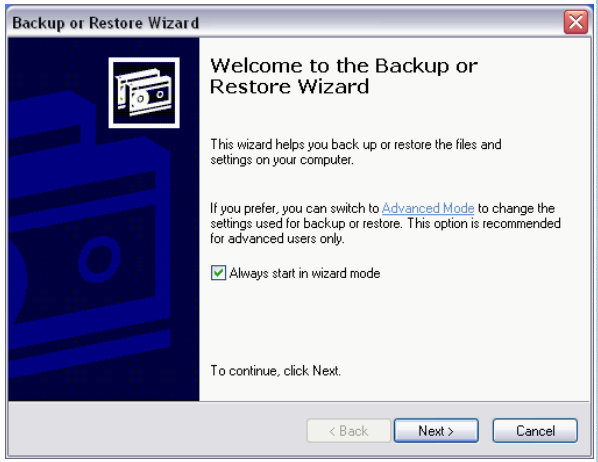
  e.g. TrueCrypt

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

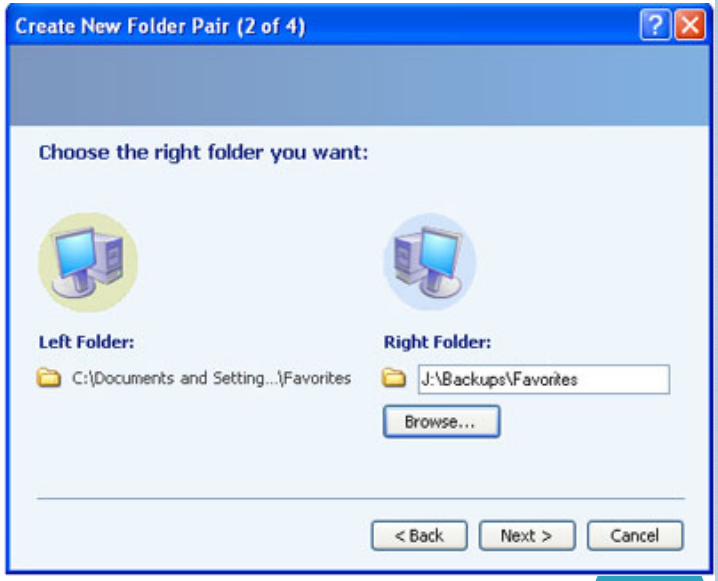
Synchronize: New and updated files are copied both ways. Renames and deletes in one folder is repeated on the other.

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 is 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

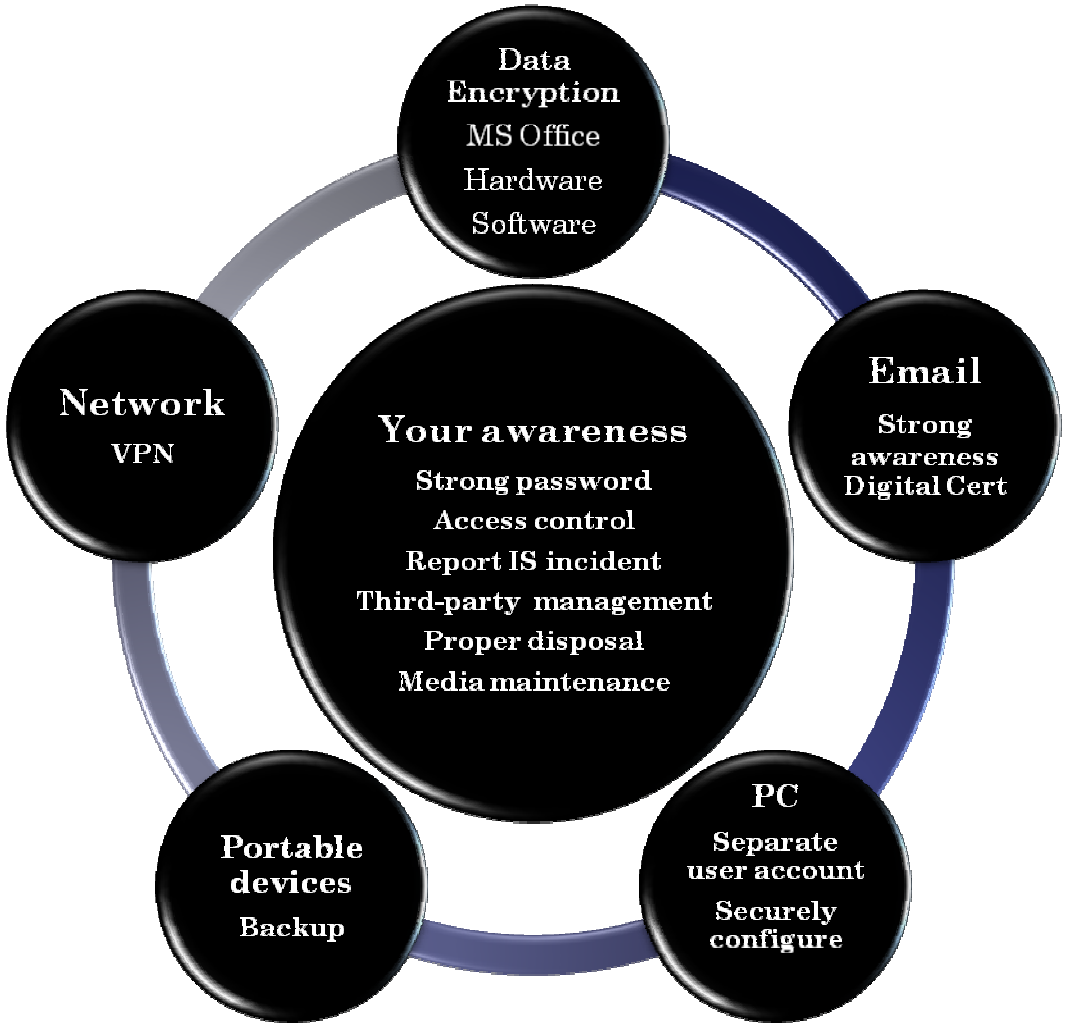
TIPS TO PREVENT INFORMATION LEAKAGE FROM
4. PORTABLE DEVICES

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

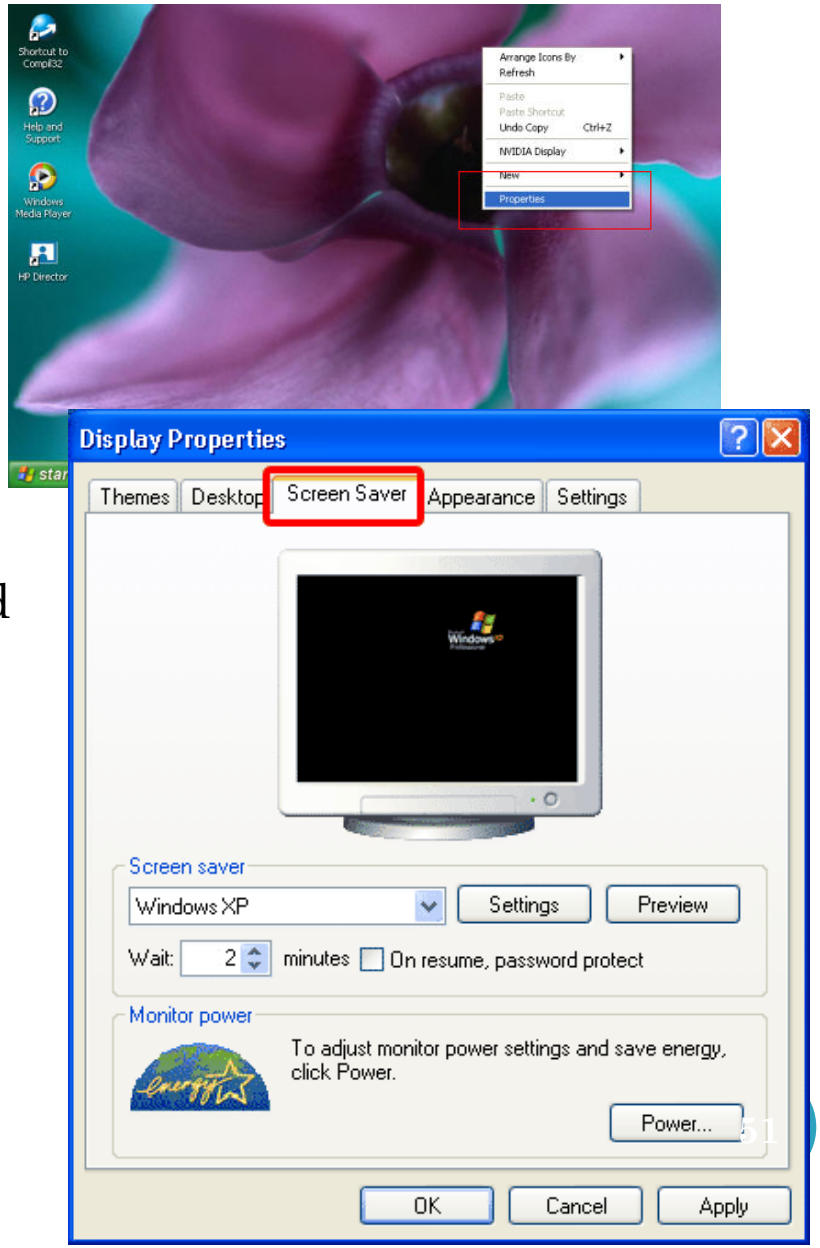


TIPS IN PROTECTING ELECTRONIC INFORMATION

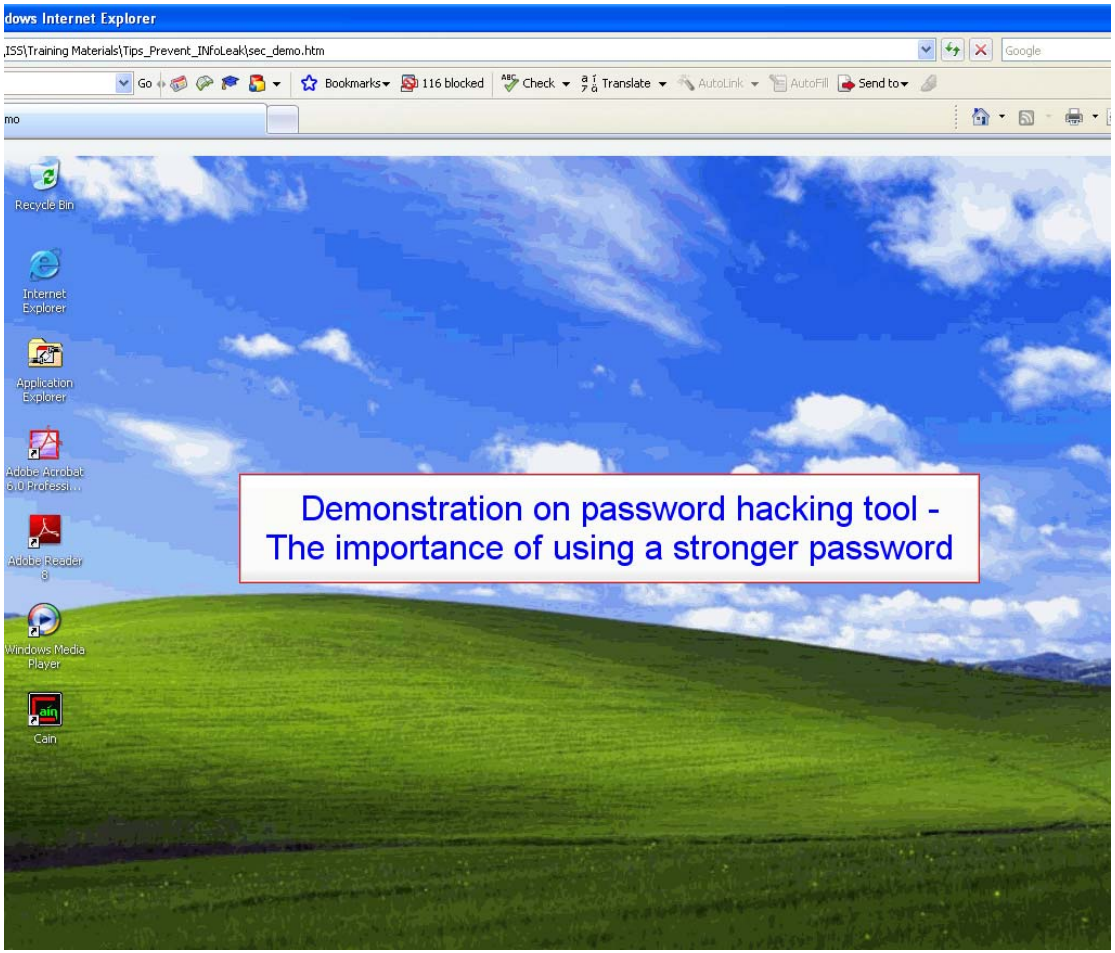
- Your awareness

- 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.mspx

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**

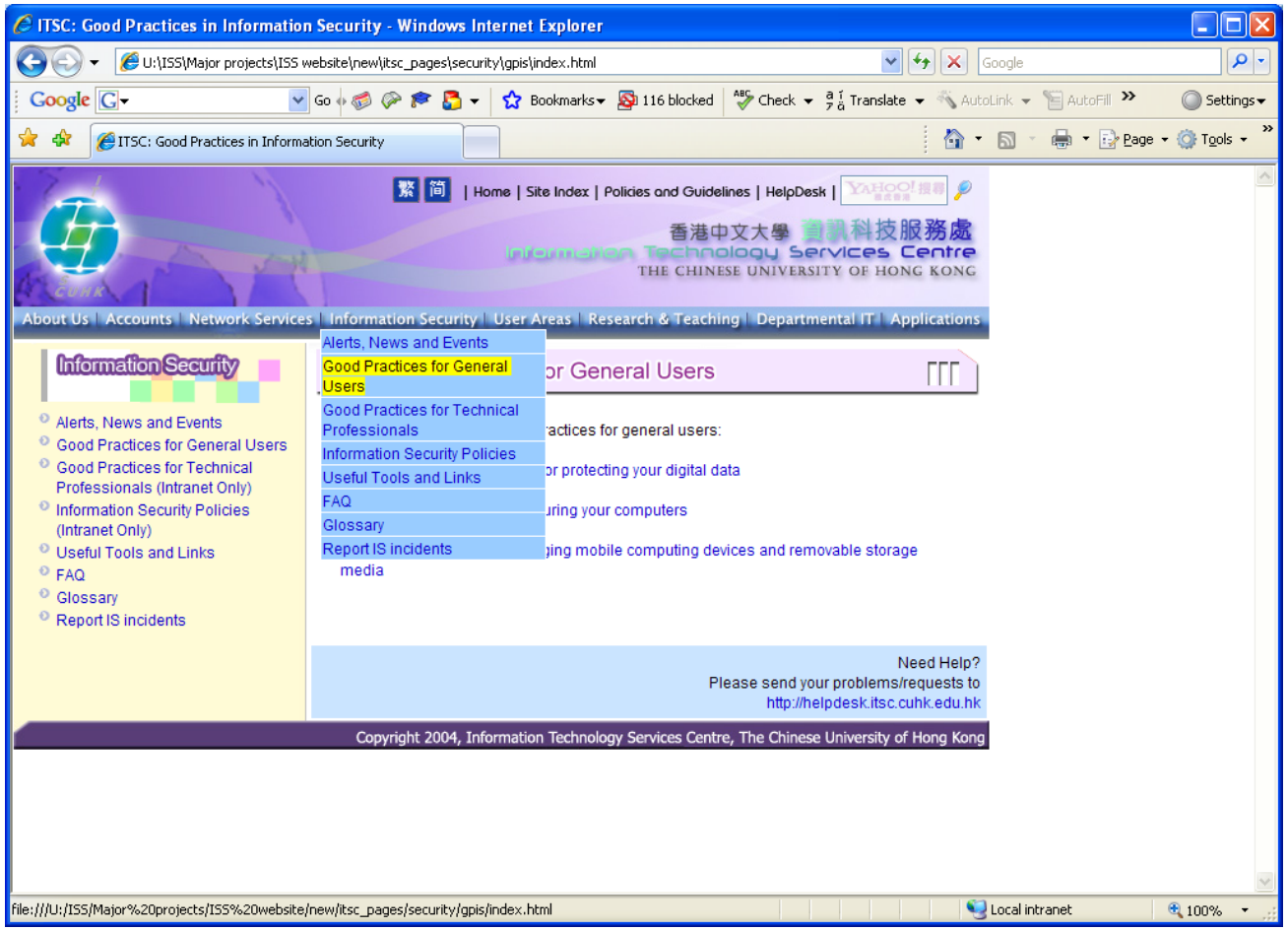
TIPS IN PROTECTING ELECTRONIC INFORMATION

- Your awareness

- **Proper disposal**
  - **Degaussing the devices**
  - **Physically destroying them, or by using a data cleaner to erase data inside**
  - **e.g. Blancoo 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