itsc Information Technology Services Centre

COMMON TIPS IN HANDLING PHISHING EMAILS

處理網絡釣魚電郵的常用技巧

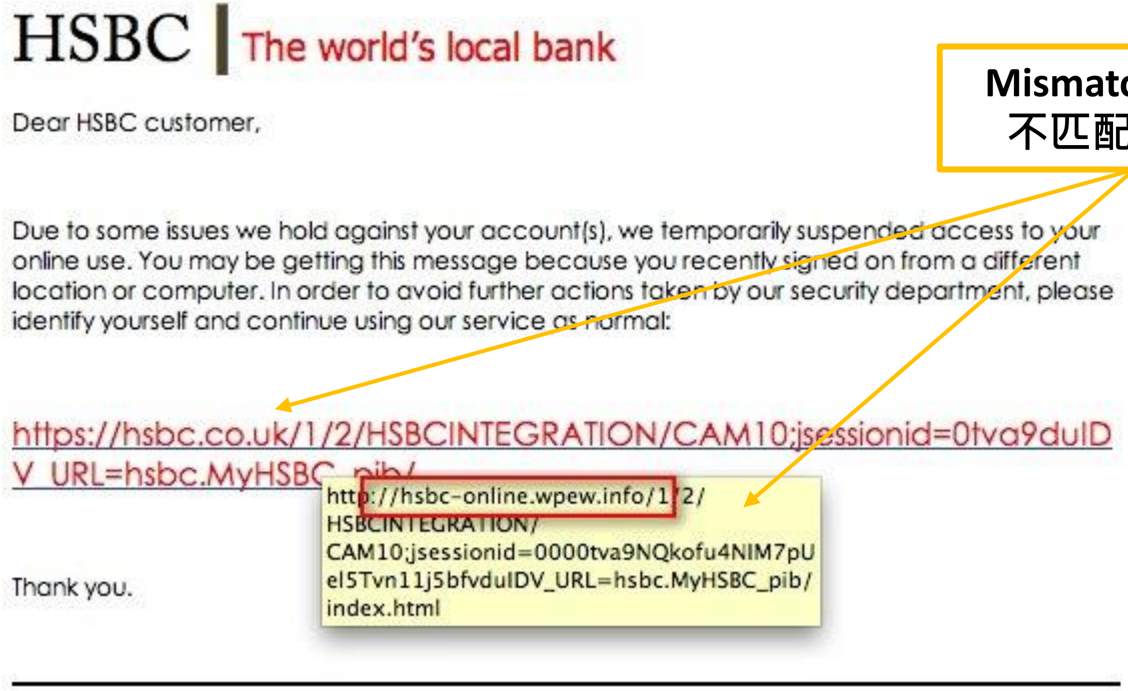
Information Technology
Services Centre

Common Tips to Identify Phishing Emails

網絡釣魚電郵的常用技巧

1. The message contains a mismatched URL
電郵內容包含不匹配的網址

This URL is very suspicious!
這條網址相當可疑！



HSBC | The world's local bank

Dear HSBC customer,

Due to some issues we hold against your account(s), we temporarily suspended access to your online use. You may be getting this message because you recently signed on from a different location or computer. In order to avoid further actions taken by our security department, please identify yourself and continue using our service as normal:

https://hsbc.co.uk/1/2/HSBCINTEGRATION/CAM10;jsessionid=0tva9duIDV_URL=hsbc.MyHSBC_pib/

http://hsbc-online.wpew.info/1/2/HSBCINTEGRATION/CAM10;jsessionid=0000tva9NQkofu4NIM7pUel5Tvn11j5bfvduIDV_URL=hsbc.MyHSBC_pib/index.html

Thank you.

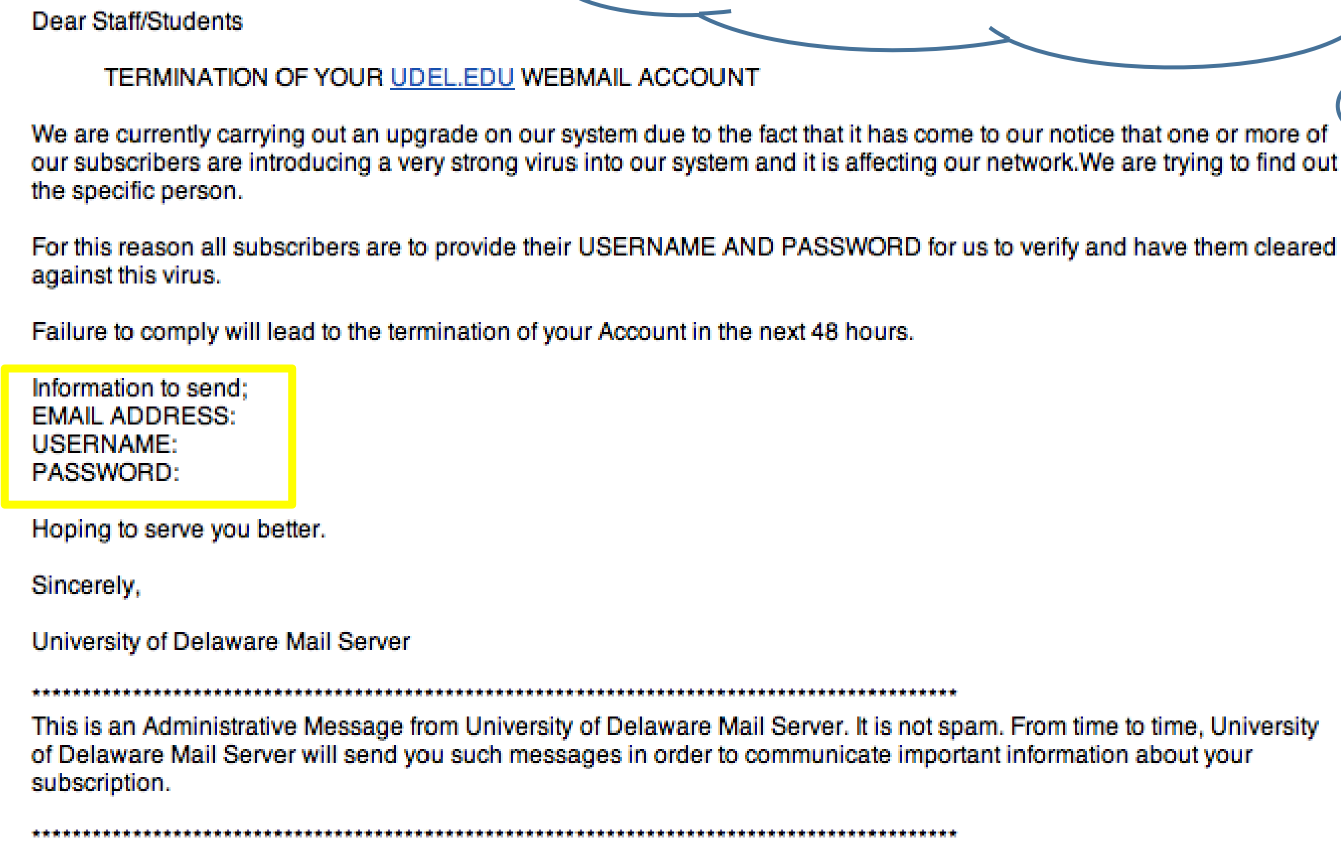
Mismatched URL
不匹配的網址

Mouseover the link,
DON't click!

將滑鼠標示移到這網址上
不要點擊！

2. They ask for personal sensitive information
對方指示交出個人敏感資料

Why do you ask for my account information?
何故要我交出我的帳戶資料？



Dear Staff/Students

TERMINATION OF YOUR UDEL.EDU WEBMAIL ACCOUNT

We are currently carrying out an upgrade on our system due to the fact that it has come to our notice that one or more of our subscribers are introducing a very strong virus into our system and it is affecting our network.We are trying to find out the specific person.

For this reason all subscribers are to provide their USERNAME AND PASSWORD for us to verify and have them cleared against this virus.

Failure to comply will lead to the termination of your Account in the next 48 hours.

Information to send;
EMAIL ADDRESS:
USERNAME:
PASSWORD:

Hoping to serve you better.

Sincerely,

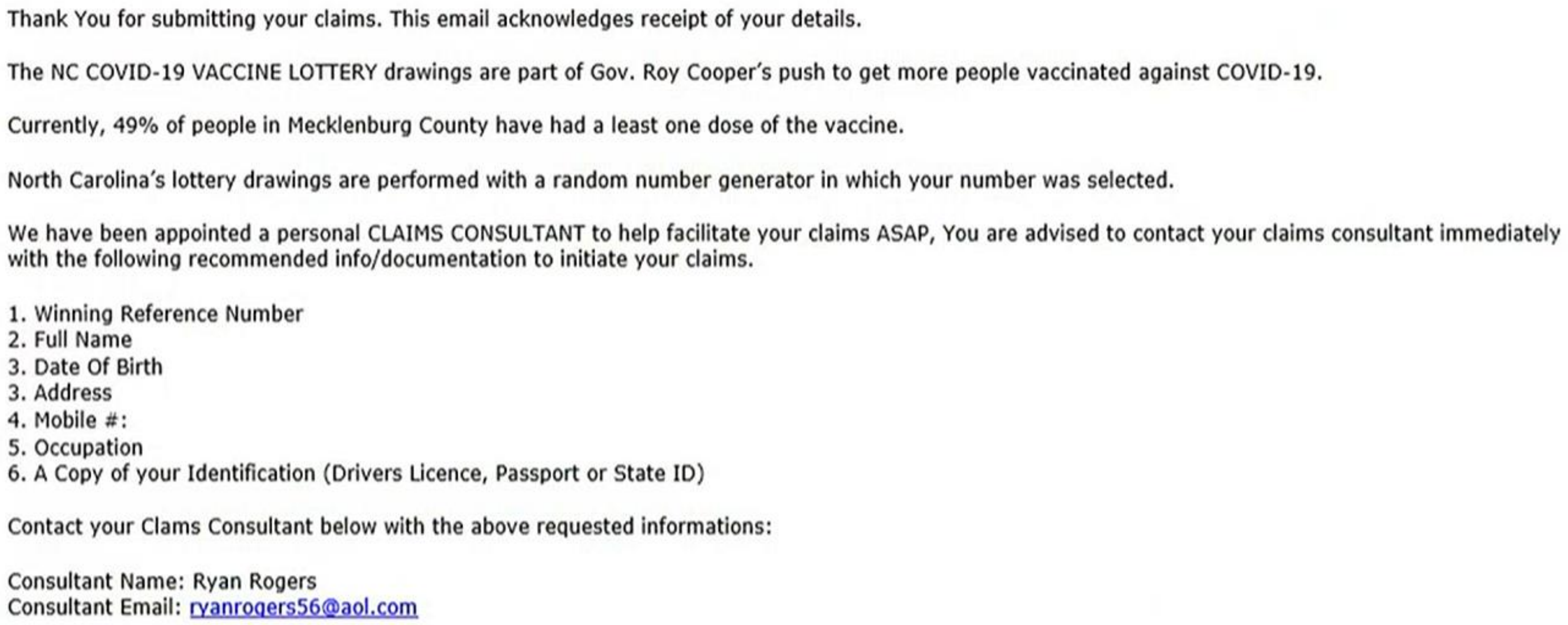
University of Delaware Mail Server

****

This is an Administrative Message from University of Delaware Mail Server. It is not spam. From time to time, University of Delaware Mail Server will send you such messages in order to communicate important information about your subscription.

****

3. The offer seems too good to be true
內容好得令人難以置信



Thank You for submitting your claims. This email acknowledges receipt of your details.

The NC COVID-19 VACCINE LOTTERY drawings are part of Gov. Roy Cooper's push to get more people vaccinated against COVID-19.

Currently, 49% of people in Mecklenburg County have had a least one dose of the vaccine.

North Carolina's lottery drawings are performed with a random number generator in which your number was selected.

We have been appointed a personal CLAIMS CONSULTANT to help facilitate your claims ASAP, You are advised to contact your claims consultant immediately with the following recommended info/documentation to initiate your claims.

1. Winning Reference Number
2. Full Name
3. Date Of Birth
3. Address
4. Mobile #:
5. Occupation
6. A Copy of your Identification (Drivers Licence, Passport or State ID)

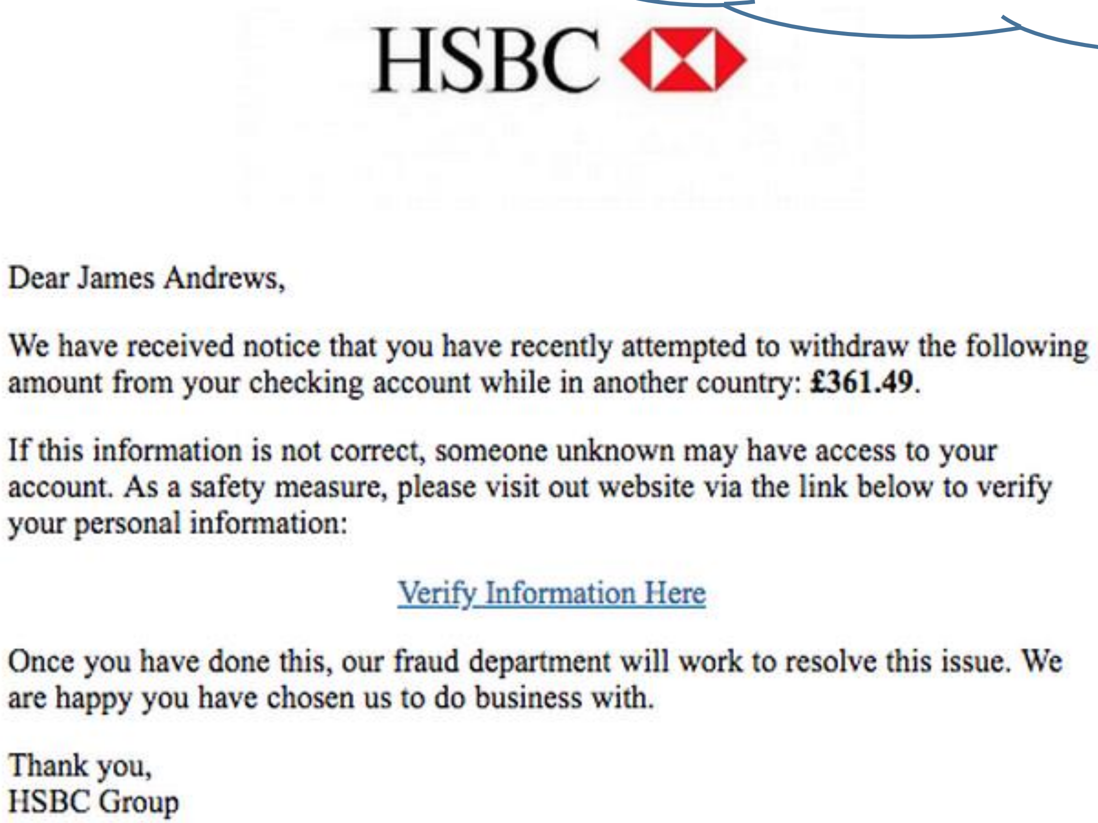
Contact your Clams Consultant below with the above requested informations:

Consultant Name: Ryan Rogers
Consultant Email: ryanrogers56@aol.com

I won the prize for no reason!?
無緣無故中獎！？

4. You didn‘t initiate the action
你之前沒有做過相關的行動

I haven’t recently withdrew the money from HSBC!
我最近沒有從匯豐取錢！！



HSBC

Dear James Andrews,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: **£361.49**.

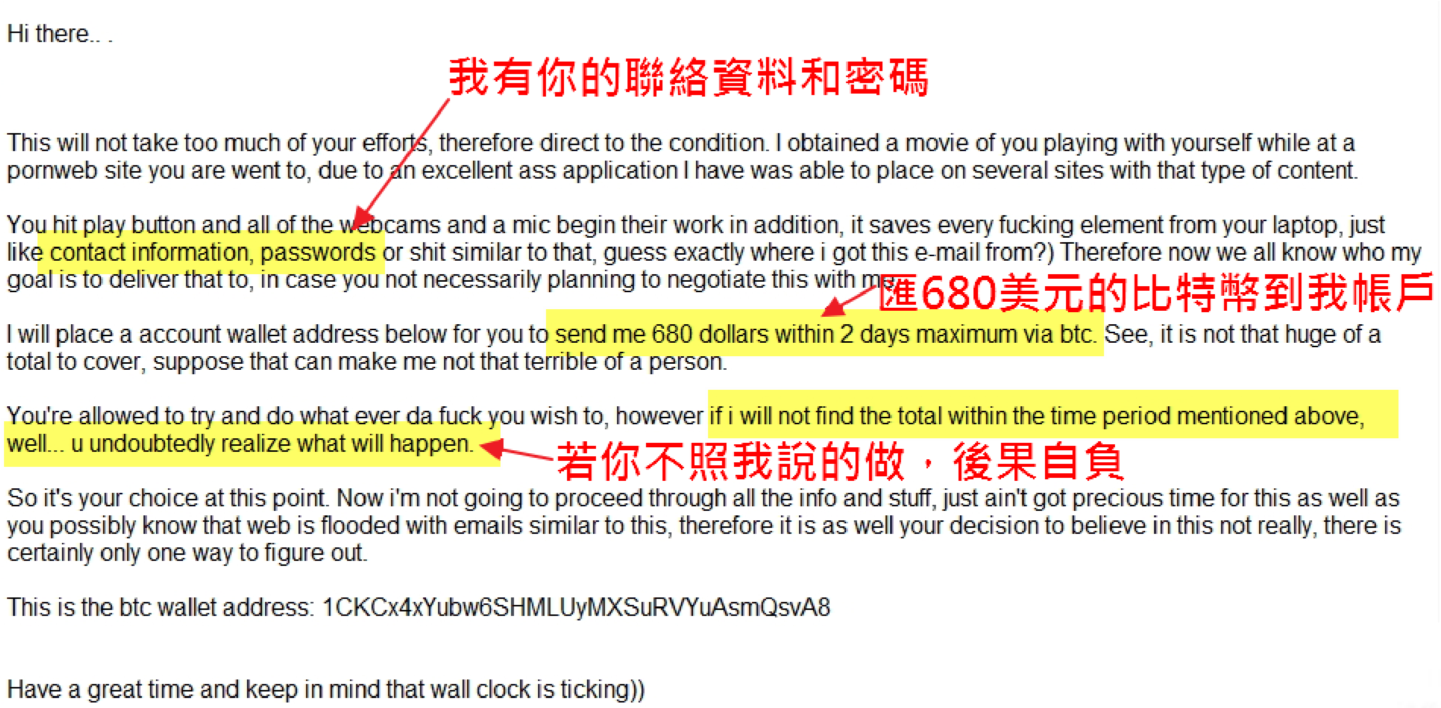
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit out website via the link below to verify your personal information:

Verify Information Here

Once you have done this, our fraud department will work to resolve this issue. We are happy you have chosen us to do business with.

Thank you,
HSBC Group

5. You are asked for money
被要求匯款



Hi there.. .

我有你的聯絡資料和密碼

This will not take too much of your efforts, therefore direct to the condition. I obtained a movie of you playing with yourself while at a pornweb site you are went to, due to an excellent ass application I have was able to place on several sites with that type of content.

You hit play button and all of the webcams and a mic begin their work in addition, it saves every fucking element from your laptop, just like contact information, passwords or shit similar to that, guess exactly where i got this e-mail from?) Therefore now we all know who my goal is to deliver that to, in case you not necessarily planning to negotiate this with me.

匯680美元的比特幣到我帳戶

I will place a account wallet address below for you to send me 680 dollars within 2 days maximum via btc. See, it is not that huge of a total to cover, suppose that can make me not that terrible of a person.

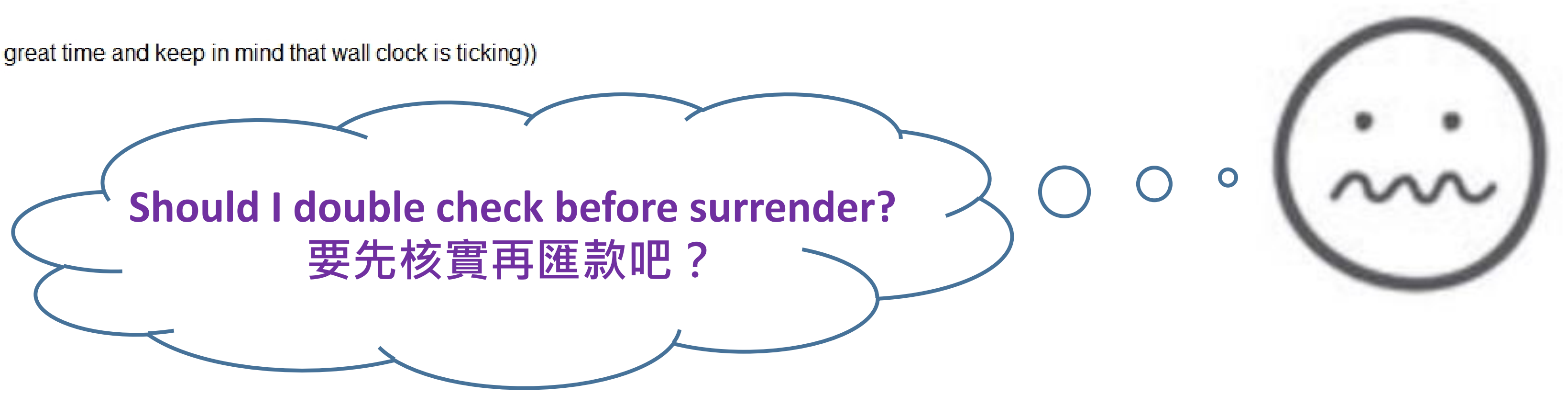
You're allowed to try and do what ever da fuck you wish to, however if i will not find the total within the time period mentioned above, well... u undoubtedly realize what will happen.

若你不照我說的做，後果自負

So it's your choice at this point. Now i'm not going to proceed through all the info and stuff, just ain't got precious time for this as well as you possibly know that web is flooded with emails similar to this, therefore it is as well your decision to believe in this not really, there is certainly only one way to figure out.

This is the btc wallet address: 1CKCx4xYubw6SHMLUyMXSuRVYuAsmQsvA8

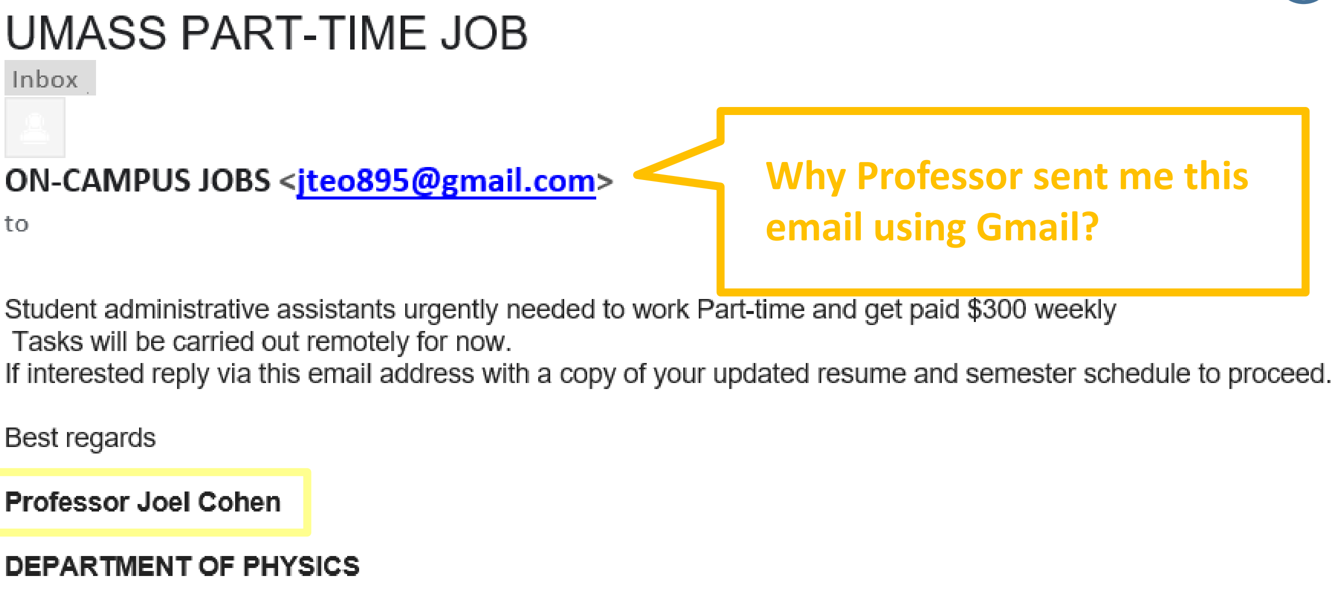
Have a great time and keep in mind that wall clock is ticking))



Should I double check before surrender?
要先核實再匯款吧？

6. Sending address not exactly right
發送電郵者有可疑

Who is Professor Joel?
誰是Professor Joel？



UMASS PART-TIME JOB

Inbox

ON-CAMPUS JOBS <jteo895@gmail.com>

to

Student administrative assistants urgently needed to work Part-time and get paid $300 weekly
Tasks will be carried out remotely for now.
If interested reply via this email address with a copy of your updated resume and semester schedule to proceed.

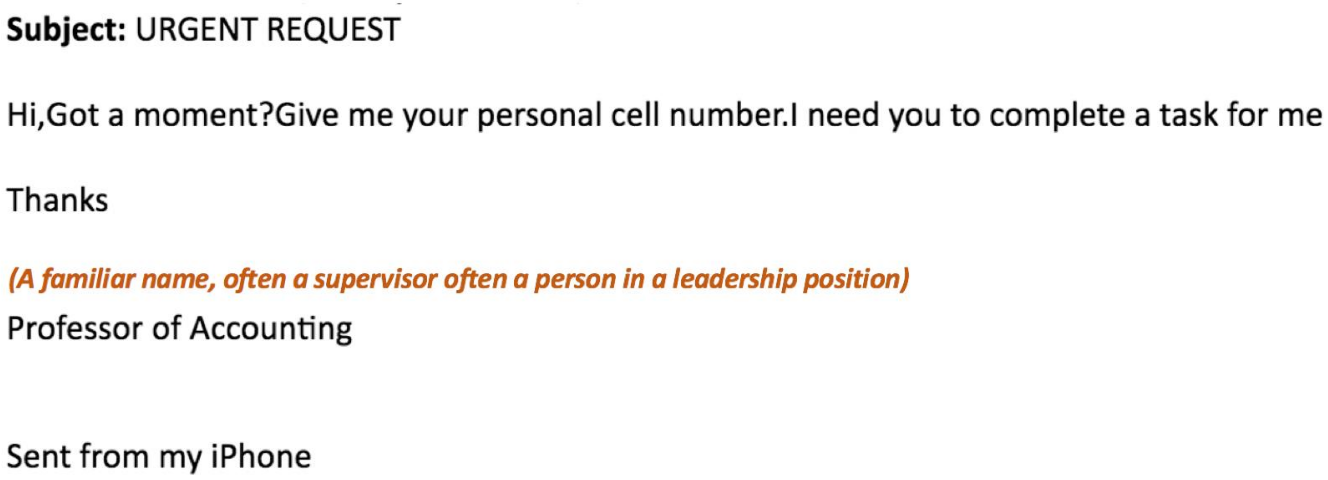
Best regards

Professor Joel Cohen

DEPARTMENT OF PHYSICS

Why Professor sent me this email using Gmail?

7. Urgent or threatening language
讓人焦慮或威脅性的字句



Subject: URGENT REQUEST

Hi,Got a moment?Give me your personal cell number.I need you to complete a task for me

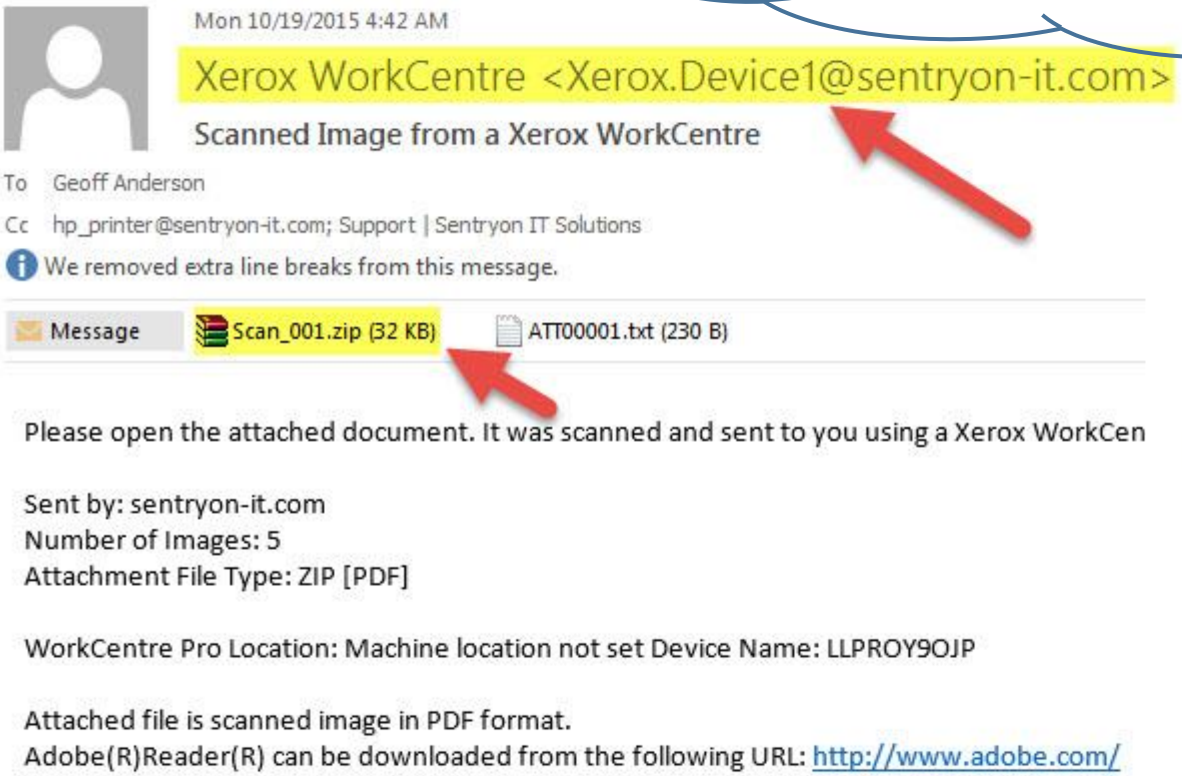
Thanks

(A familiar name, often a supervisor often a person in a leadership position)
Professor of Accounting

Sent from my iPhone

8. Beware of suspicious / unexpected attachments
提防可疑 / 意外收到的附件

What did I just scan from the printer?
我剛剛從打印機掃描了什麼？



Mon 10/19/2015 4:42 AM

Xerox WorkCentre <Xerox.Device1@sentryon-it.com>

Scanned Image from a Xerox WorkCentre

To Geoff Anderson

Cc hp_printer@sentryon-it.com; Support | Sentryon IT Solutions

We removed extra line breaks from this message.

Message | Scan_001.zip (32 KB) | ATT00001.txt (230 B)

Please open the attached document. It was scanned and sent to you using a Xerox WorkCen

Sent by: sentryon-it.com
Number of Images: 5
Attachment File Type: ZIP [PDF]

WorkCentre Pro Location: Machine location not set Device Name: LLPROY9OJP

Attached file is scanned image in PDF format.
Adobe(R)Reader(R) can be downloaded from the following URL: http://www.adobe.com/

Beware of the above situations, don’t click on any links or open any email attachments.

若遇有以上清況，切勿隨便點擊電郵內的連結或打開附件

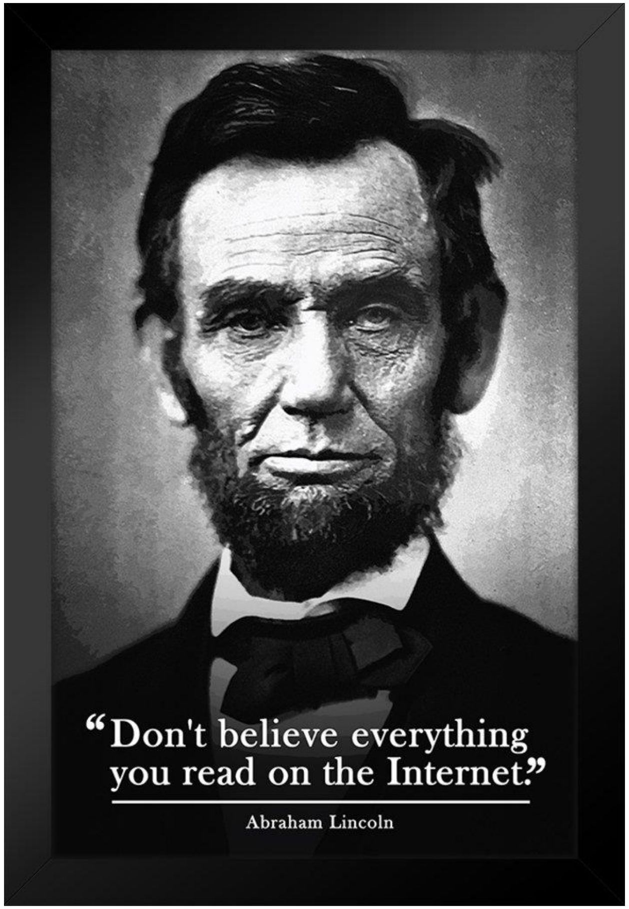
Conclusion

結語

Think before your action
眼看手勿動

I won’t do anything before confirmation.
弄清楚前，絕不行動。

Don’t believe everything you see
不要只相信表面信息



100% EXPERT

Let’s validate...
核實一下吧...

Report phishing activities to relevant department
向相關部門報告網絡釣魚活動

- Report to your LAN administrator or ITSC through infosec@cuhk.edu.hk or ITSC Service Desk with the original suspicious email attached.
  請報告給你部門的電腦支援同事，或聯絡ITSC服務台或電郵到infosec@cuhk.edu.hk，並附上原本的可疑電郵。

  *How to attach an original email, please refer:
  如何附加原始電子郵件，請參考：
  https://www.itsc.cuhk.edu.hk/all-it/information-security/phishing-email-web-fraud-alert/

In general, can we stop all phishing emails?
一般來說, 我們可以阻截所有釣魚電郵嗎？

No, we cannot, even with latest technologies.

不，就算用上最新科技，也是不可能 。

What can we do finally?
最後我們可以做些甚麼？

We can Mitigate, Prevent, Avoid phishing attacks with Knowledge & Good Practices (#THINKB4UCLICK).

通過知識與良好習慣 (#THINKB4UCLICK)，減輕、預防及避免遭受釣魚攻擊。

Thanks for your time!

謝謝你的時間！