Yui Kee Computing Ltd.

Newsletter

April 2016

Contents

Internet of Things Security Seminar

<web-link for this article>

The Internet of Things (IoT) is a fast-growing trend in IT, but are the developers considering the issue of security. The Hong Kong Computer Society (HKCS) Information Security Special Interest Group (ISSIG)is holding a half-day seminar about "IoT: Security & Privacy Challenges" on 18th April 2016. With its vast application, IoT also introduces new threat landscape, including attacks, vulnerability management, access control and data privacy issues. This half day seminar aims to address different areas of IoT Security, including IoT security threats; related solutions and practices; and how to tackle IoT security & privacy problems.

The speakers from Symantec Limited, Quann HK and Macau (e-Cop), CSC® Digital Brand Services Hong Kong and Cisco Hong Kong & Macau will address the issues from cloud, technology, legal, branding and engineering perspectives.

The seminar is free for HKCS members, and HK$50 for others. Full details and registration.

More Information

- Hong Kong Computer Society
- Information Security Special Interest Group
- IoT: Security & Privacy Challenges Seminar Registration

Hang Seng Bank Warns of Phishing Email

<web-link for this article>

Hang Seng Bank has issued a warning about fraudulent e-mails supposedly from the bank, and a fraudulent website using the domain name e.bnking-secure-server-confirm.apogen.cl

linked from the emails. The fraudulent e-mails and website try to collect user's bank account details.

The Hong Kong Monetary Authority (HKMA) advised victims to contact the Bank's customer service hotline on 2822-0228, and report to the Police or contact the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860-5012.

More Information

- Alert on Fraudulent E - Mails and Website
- Phishing email related to Hang Seng Bank, Limited

MOBILedit New Version Launched

<web-link for this article>

COMPELSON Labs has launched a new version, 3.1, of its MOBILedit Forensic Express at the Forensics Europe Expo. The phone extractor improves deleted data recovery and aggregation for many applications, adds password recovery for Android, LG and HTC email apps, displays GPS location for photos in messages and improves data retrieval from Organizer for iOS.

It also seamlessly integrates with Compelson's Camera Ballistics, a tool that identifies if a photo was taken by a suspected camera device or not. Camera Ballistics uses a sensor fingerprint to analyze an unlimited amount of photos being investigated, matching it to the photos taken by that specific camera.

More Information

- Forensics Europe Expo
- Launching the new MOBILedit Forensic Express 3.1

HSBC and Bank of China Discover Dodgy e-Banking Share Trading

<web-link for this article>

Regular surveillance of e-banking platforms by Hong Kong and Shanghai Bank (HSBC) and Bank of China (Hong Kong) (BOCHK) during the last fortnight has revealed unauthorized share trading in eight accounts amounting to HK$6.86 million. The banks have informed the Police and the Hong Kong Monetary Authority (HKMA). The banks said that client compensation would be decided on the details of the individual cases.

The HKMA reassured the public in a press release saying, "In accordance with the Code of Banking Practice, a customer will not be held responsible for any direct loss suffered by him or her as a result of unauthorized e-banking transactions unless he or she acts fraudulently or with gross negligence." It also noted that no unauthorised fund transfers over these accounts were detected and that fund transfers to unregistered accounts were regarded as high-risk and required two-factor authentication.

The HKMA advised people to take precautionary measures including:

- Setting e-banking passwords that are difficult to guess and different from the ones for other internet services;
- Installing and promptly updating security software to protect their computers and mobile phones;

- Refraining from using public computers or public Wi-Fi to access e-banking accounts; and
- checking their e-banking accounts from time to time and reviewing alert messages and statements issued by banks in a timely manner.

Further advice from the HKMA is available on their website.

More Information

- Dodgy share trading via e-banking
- Consumer Corner - Consumer Education Programme
- HKMA E-banking Alert: Beware of unauthorised share trading transactions

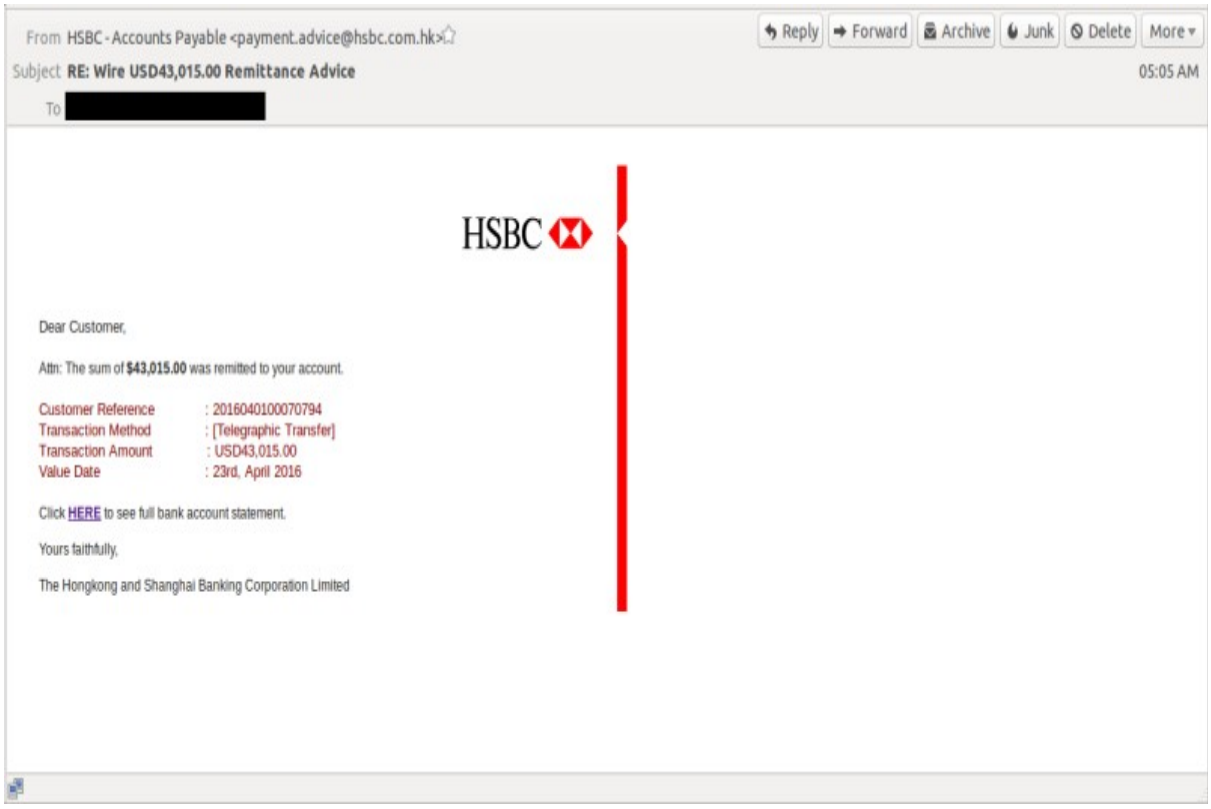
HSBC Phishing Detection Challenge

<web-link for this article>

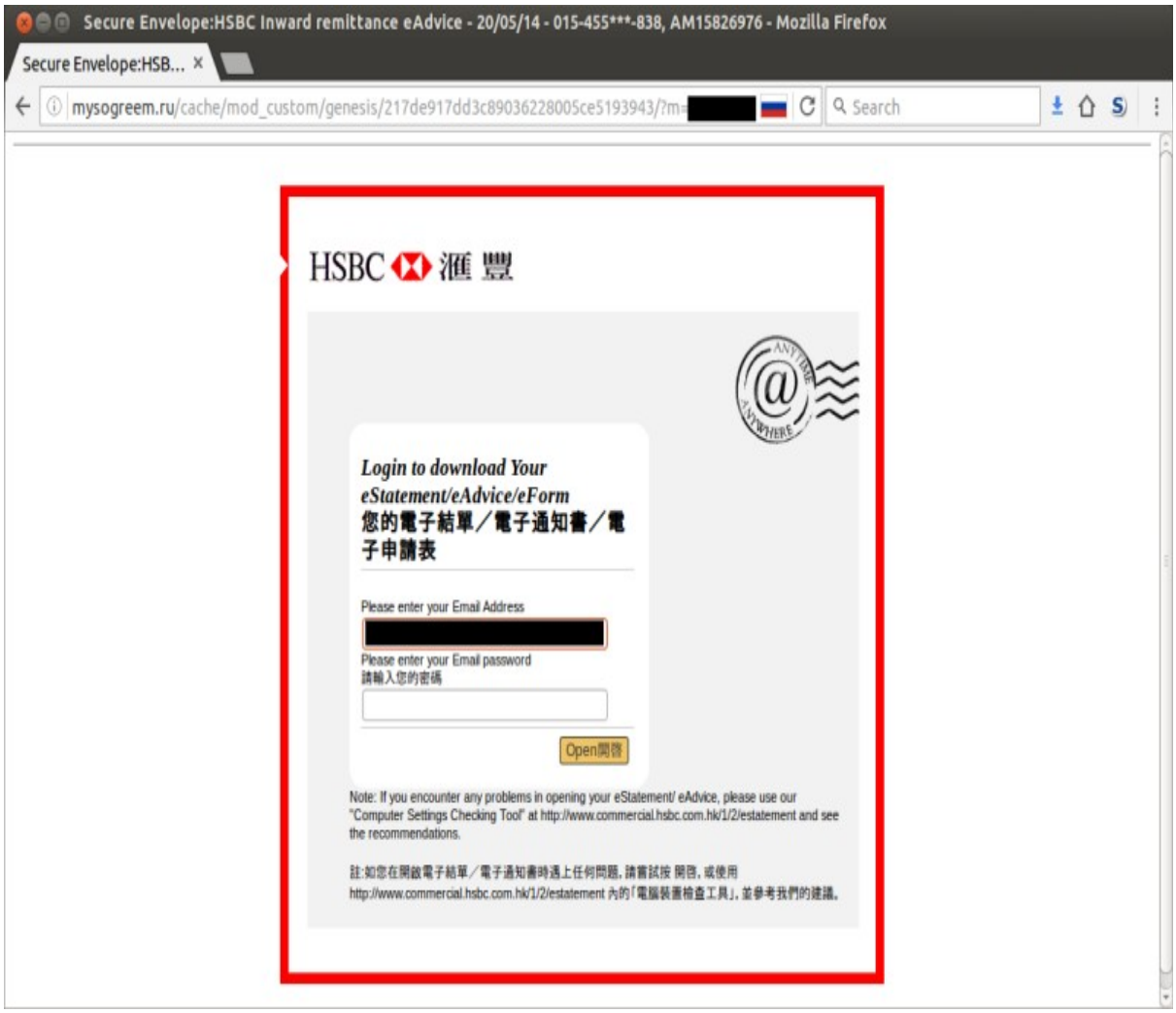
We are often told to watch out for suspicious emails, but what is suspicious? Could you tell the difference between a real and fake notification from your bank? This challenge uses a real and a fake notification "from" HSBC bank to a 'Business Direct' account holder, see if you can tell which is which. Black rectangles have been used to obscure customer information in the screenshots.

Notification A

This email:

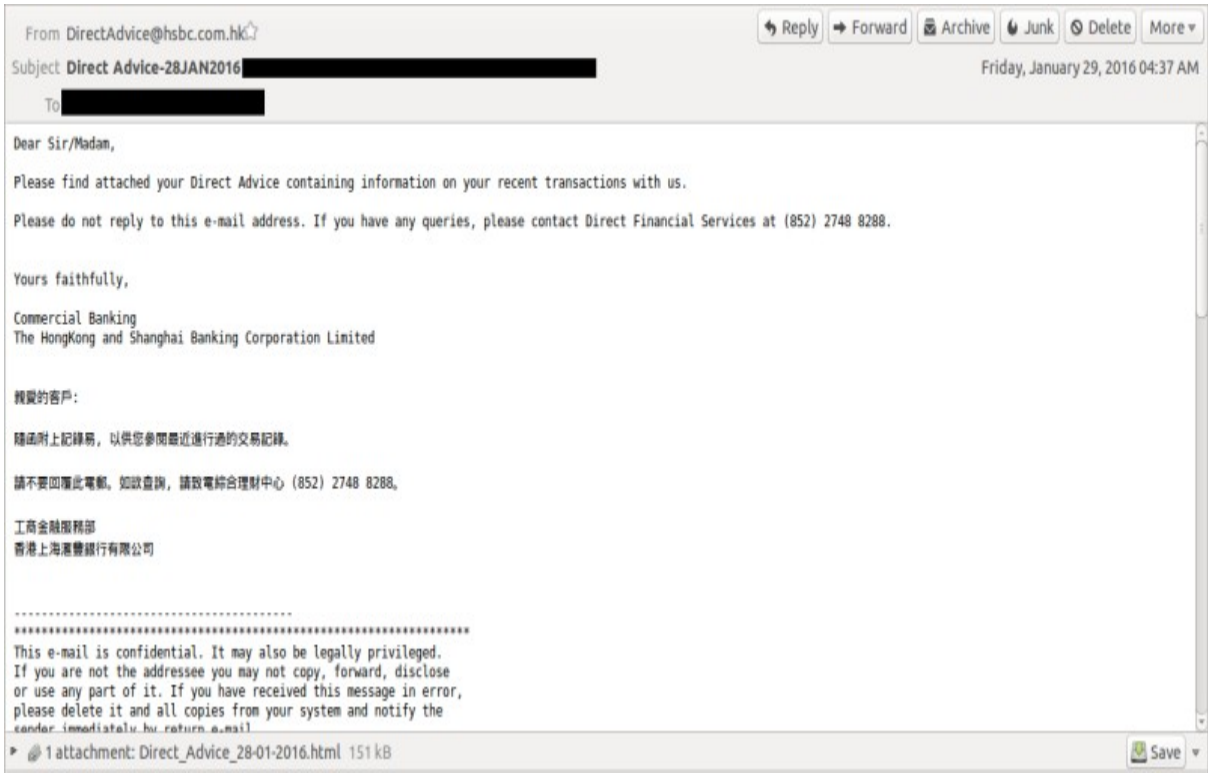


Has a link to this webpage:

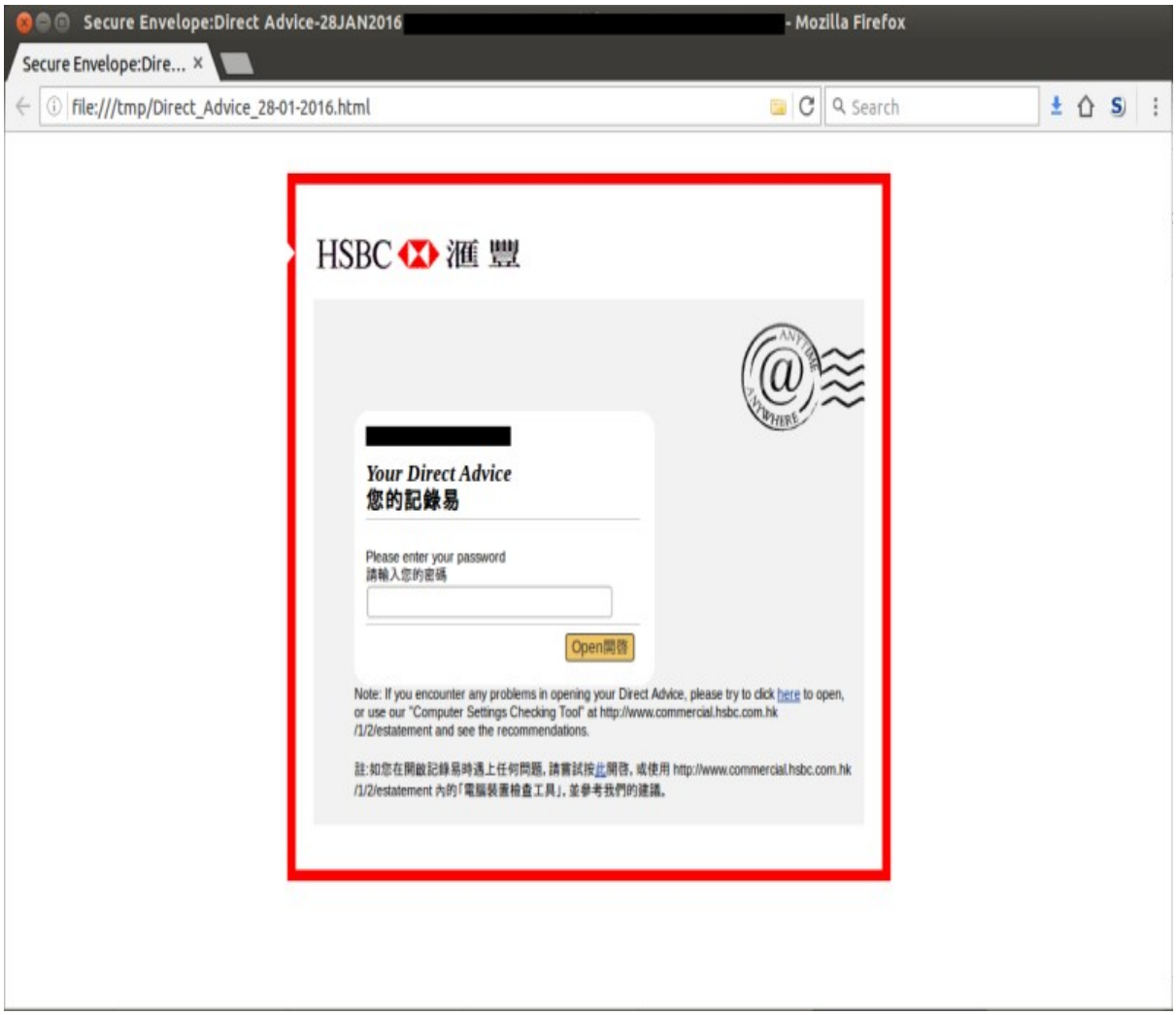


Notification B

This email:



Has this webpage attached:



What is the Risk?

HSBC Business Direct accounts use a security device that generates six-digit codes that must be used in conjunction with the user's password to log into the HSBC website. Neither of these notifications asks for the security device code, so not enough information is collected to enable unauthorised transactions. However, this does not mean the money in the account is safe, this may be the first step of a multi-stage attack. Alternatively, the target might not be the HSBC account at all, but the victim's email account.

The Answer and Comments

Notification A is the fake. What doesn't help us distinguish between them?

- The title of both webpages starts, "Secure Envelope:". For the genuine page, this has some meaning: the attachment is encoded so that the correct "Direct Advice" password must be entered for the transaction details to be seen, but there is no way to verify that it is a "Secure Envelope", any webpage can start their title with that text.
- The fake webpage title includes, "015-455***-838" - this looks like a partially-obscured account number, and all HSBC Business Direct account numbers end in -838. Think carefully before assuming, "it knows my account number, therefore it's genuine".
- Corporate Branding: The webpages are very similar, using the HSBC logo, the "Anytime, Anywhere" postmark image and even the notch in the red border next to

the logo. The fake uses the same branding in the email, so it might appear more genuine than the real thing.

What might help:

- Familiarity with the genuine article. This fake asks for the user's email password instead of the 'Direct Advice' password, the email message is HSBC branded, not plain text, other text details are different. These changes from the familiar might help the user become suspicious of the fake. Unfortunately, HSBC has not published detailed examples and made clear statements like, "this is how we do these messages, we will not change without notifying you first", so users can be easily misled by "improvements".
- Checking the email headers. The real message includes the header line:

  ```
  Received: from hsbc.com.hk (psmtp6.hsbc.com.hk [203.112.90.16])
  ```

  The equivalent line in the fake is:

  ```
  Received: from srv-01.hostcloud.vn (unknown [210.86.239.114])
  ```

  Why would HSBC be using a cloud server in Vietnam instead of their own server? Unfortunately, this method requires some technical knowledge (which header line to look at and why?, how to interpret the line) and might still be unreliable.

- Understanding the URL. The fake webpage URL starts:

  ```
  http://mysogreem.ru/cache/mod_custom/genesis/217de917dd3c89036228005ce5193943/
  ```

  Why would HSBC use 'mysogreem.ru' as their web server? The real webpage URL is:

  ```
  file:///tmp/Direct_Advice_28-01-2016.html
  ```

  This doesn't reassure us, the page is just a temporary file created from the email attachment, any email could create a similar file. This test might reveal a fake, but doesn't tell us what is genuine, and it may be too technical for an ordinary user.

- Checking where the webpage is served from. A neat Firefox extension, called Flagfox, helps with this. Flagfox adds the national flag of the location of the web server. This can be seen in the screenshot of the fake webpage, where it shows the Russian Federation flag. For the genuine webpage, it shows that it is a local file. Like the preceding test, this might reveal a fake, but doesn't prove the genuine. It is easier for an ordinary user to understand.

In this case, if the fake notification successfully tricks the end user, the attacker will have access to their email account. HSBC is not responsible for keeping your email account secure. However, Banks might benefit from taking a wider view of helping their customer's overall security. Very often, when looking at suspicious messages, we are not certain about the attacker's ultimate objective. In this case, if the attack is successful, the attacker will be able to access the victim's email account, **and** will know they have an HSBC Business Direct account. How will they seek to monetise that information?

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/