Yui Kee Computing Ltd.

Newsletter

June 2014

Contents

HKMA Warns about fake HSBC emails

<web-link for this article>

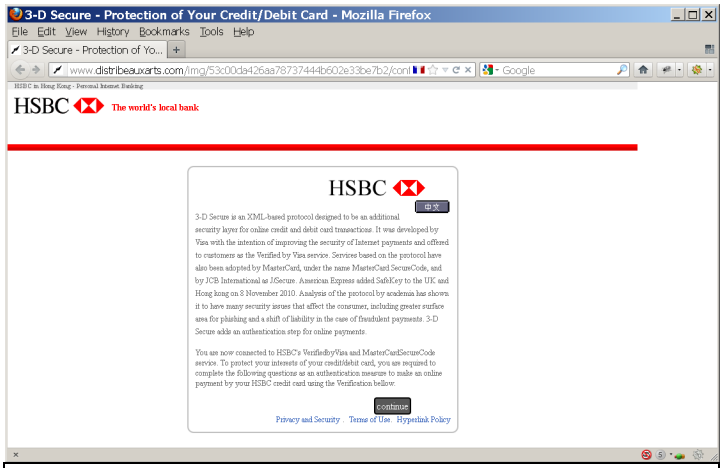


Figure 1 Fake HSBC Verified by Visa page, with Wikipedia text

The Hong Kong Monetary Authority (HKMA) has warned about e-mail purporting to be sent from The Hongkong and Shanghai Banking Corporation Limited (HSBC). The e-mail requests customers to use an embedded hyperlink to visit a webpage that mimics HSBC's Verified by Visa page.

Anyone that has followed the fraudulent instructions should contact HSBC at 2233 3000, and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

HKMA listed two example webpages linked from the fake emails: “http://www.elka.sklep.pl/tmp/” and “http://www.distribeauxarts.com/img/”. At the time of writing, the text on one of the pages included a description of the 3-D Secure protocol that was lifted almost word-for-word from Wikipedia. The links for policies went to HSBC's own policy pages. The server addresses, 213.186.33.19 and 213.186.33.48, are in the same block in France, suggesting that the criminals scanned the block for vulnerable webservers, uploaded their fake pages to each one and sent out batches of fraudulent messages with each address.

An HKMA Spokesperson advised, "Members of the public are reminded not to access their Internet banking accounts through hyperlinks embedded in e-mails, Internet search engines or suspicious pop-up windows. Instead, they should access their Internet banking accounts by typing the website addresses at the address bar of the browser, or by bookmarking the genuine website and using that for access. In addition, banks are not expected to send e-mails

asking their customers to provide their account information (e.g. Internet banking logon passwords) or verify their account information online. If in doubt, they should contact their banks".

More Information

Fraudulent email purporting to be related to The Hongkong and Shanghai Banking Corporation Limited
Alert issued on bogus email

Fake Standard Chartered Emails too, warns HKMA

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a warning about fake emails supposedly from Standard Chartered Bank (Hong Kong) Limited (SCBHK). The emails link to various fraudulent webpages that ask for personal and credit card information. The three example webpages listed by HKMA were hosted in Spain and one was still active at the time of writing (fig. 2). The details requested included the credit card number, CVV code from the back of the card, date of birth and 3D Secure password, in other words, all the information necessary to make a fraudulent online payment.

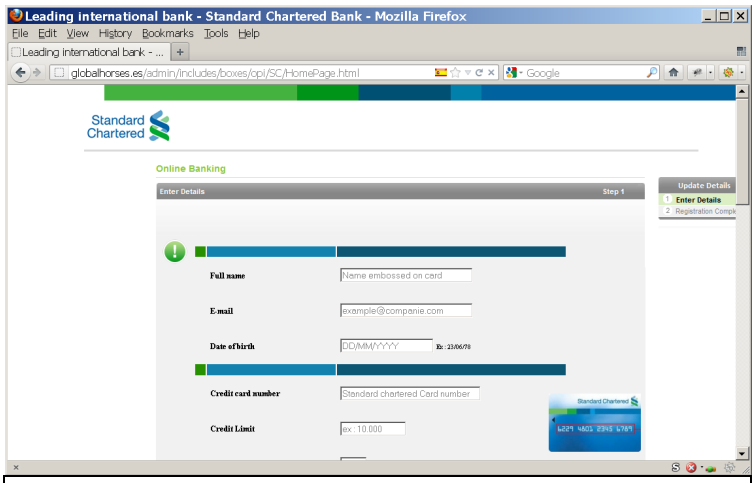


Figure 2 Fake Standard Chartered Bank webpage, asking for sensitive credit card details

Anyone who has been tricked by the emails and has used the webpages should contact SCBHK at 2886 8868 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

An HKMA spokesperson advised, "Members of the public are reminded not to access their Internet banking accounts through hyperlinks embedded in e-mails, Internet search engines or suspicious pop-up windows. Instead, they should access their Internet banking accounts by typing the website addresses at the address bar of the browser, or by bookmarking the genuine website and using that for access. In addition, banks are not expected to send e-mails asking their customers to provide their account information (e.g. Internet banking logon passwords) or verify their account information online. If in doubt, they should contact their banks".

This echoes the advice on the fraudulent webpage, "Our Bank will never ask you for your sensitive account information, e.g. username, password and other confidential account or credit card information by email".

Yui Kee Chief Consultant Allan Dyer commented, "A webpage does not become trustworthy just because it includes reasonable advice. The criminals want these pages to look genuine, so they copy the features of the original."

More Information

Fraudulent email purporting to be related to Standard Chartered Bank (Hong Kong) Limited

Beware of Purchase Order Phishing

<web-link for this article>

Online scams don't just target greedy fools, many are aimed at hard-working office staff. The Purchase Order scam has become particularly common in the last year. There are many variants, the one discussed here is just a single example, don't expect them all to be the same.

The scam starts with an email about a purchase order (fig. 3). Careful use of abbreviations like MOQ and FOB make it seem genuine. This is not aimed at the fools who believe "your email has won the lottery", but at any diligent office worker. If you are in sales, then POs are your whole existence, but everyone knows they are important. No-one wants to explain to their boss that the order was lost because they didn't act on the email.

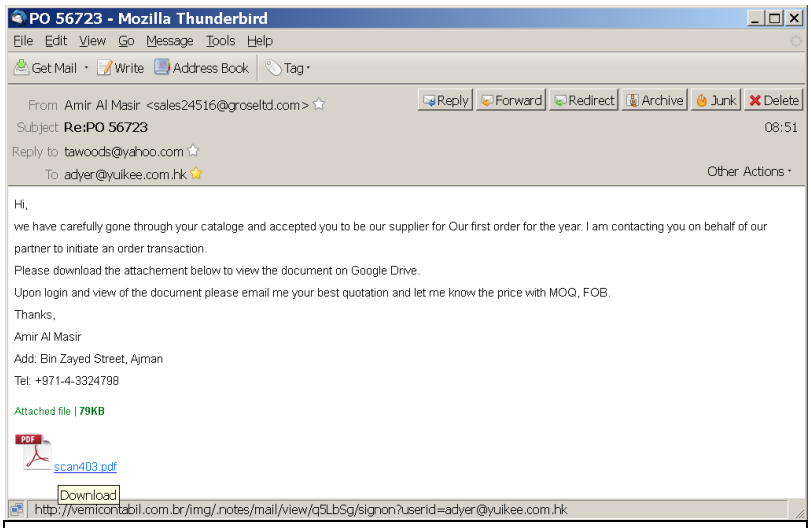


Figure 3 Phishing email

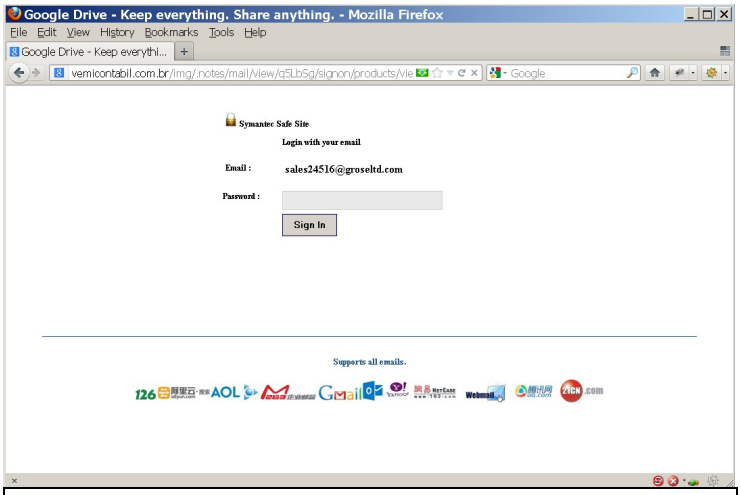


Figure 4 Fake Google Drive login, note the address bar

This breaks down their defences for the next stage. How do you access the coveted PO? There is a link at the bottom to "Google Drive" (or "Dropbox, or any online filestore). Follow the link and there is (apparently) a Google Drive login page (fig. 4) for the victim to enter their password on. Of course, the eager office worker who enters their password does not get a PO, but the scammers get access to their account, to misuse as they wish.

So how can you recognise and avoid these scams? This is not an exhaustive list:

- ☐ Familiarise yourself with your software's security features and normal operation. Anything that is out of the ordinary is suspicious. The examples below refer to the email client (Thunderbird) and browser (Firefox) that I use, the one you use may be different.
- ☐ Think about why you are receiving this PO. Even if you are in Sales, is this one of your customers? If not, whose is it? If it seems odd, then be a bit more cautious.
- ☐ The example does not mention what the product is. If there is nothing specific in the message, then it is more likely to be a generic scam.
- ☐ Watch out for other mis-matches. In the example, the message says there is an attachment, it says, "Attached file" at the bottom, but the file is not with the message. In Firefox, hovering over the link shows the address in the status bar (at the bottom), this is

a very useful feature because it is easy to see that the link goes to 'vemicontabil.com.br' and not Google Drive, which is a major warning. If your email client doesn't show links like this, check whether you can change that setting, or change your email client.

- ☐ If you follow the link, does it end up where you expect? The example doesn't go to Google Drive, check the address bar.
- ☐ Check the site identity. Firefox uses a blue or green bar next to the address to indicate a verified connection, check what is normal for your browser.
- ☐ Know what is normal for the site you think you are visiting. The real Google Drive login looks like fig. 5. Note Firefox is showing a blue bar next to the address, the site has been verified.
- ☐ Only enter your password to the matching service. When you are asked for your Google password, make sure it is Google asking you.
- ☐ Don't use the same password on multiple services.

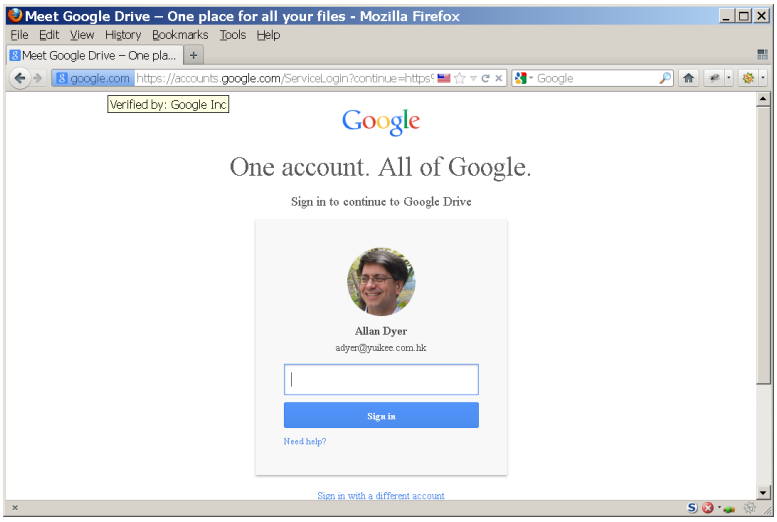


Figure 5 Real Google login

- ☐ Don't think you are not a target. Often, these are mass attacks against thousands of email addresses. If they can't get something valuable from your account, they can still misuse it, sending more scams indiscriminately, or targeting your contact lists (who are more likely to fall for the scam because they trust messages from you).

Scammers are constantly adjusting their tactics to catch the unwary. Beware.

More Information

How do I tell if my connection to a website is secure?

Hong Kong's Biggest DDoS Targets Political Poll

<web-link for this article>

PopVote.HK and Apple Daily were both hit by large Distributed Denial of Service (DDoS) attacks on 18th June 2014. The attack on PopVote.HK, which uses web services provided by Amazon Web Services (AWS), CloudFlare and UDomain, reached 85Gbps, making it the largest DDoS attack seen in Hong Kong. However, Cloudfront is a large international content delivery network and DNS provider, and it recorded the biggest ever DDoS seen on the internet, reaching 400Gbs, in February 2014 against an unnamed customer.

PopVote.HK is the website of the Public Opinion Programme (POP) of The University of Hong Kong (HKU). It is a sensitive time for PopVote.HK because it is preparing for a so-called referendum this weekend commissioned by the Secretariat of the "Occupy Central with Love and Peace" on the question of constitutional reform in Hong Kong, particularly on the matter of public nominations for the Chief Executive. AWS and UDomain have withdrawn from providing services to the site, leaving CloudFlare as their only service provider.

The DDoS on Apple Daily, a Chinese-language newspaper with an often controversial pro-democracy stance, at the same time seems more than mere coincidence.

Almost all the attack traffic to PopVote.HK was from local ISPs. The Police are investigating.

A founder of Occupy Central, Professor Benny Tai Yiu-ting, said there was "reason to suspect" that government bodies were behind the hacking activities and that the attacks must have come from "a political power which doesn't want to see universal suffrage being implemented in Hong Kong" but he did not elaborate on the evidence.

In and email Legislative Councillor for the IT Function Constituency Charles Mok has urged his constituents to condemn the attacks, writing, "it is shameful that technology is now used to thwart our civil society". He has set up a Facebook page to gather cases of cyber-attacks and condemn those behind them. He urged the Police to investigate.

Acting Secretary for Security John Lee issued a press release that did not reference the attacks directly. He urged the public to report cyber attacks to the Police so that they could take action. He mentioned a previous conviction for a DDoS attack. The release was confused on technical details, saying, "that to stop such attacks, Police must have access to the targeted system, which requires consent." Particularly for DoS attacks, the contents of the targeted system are irrelevant, all that is required are system logs showing the details of the traffic, which might come from an intermediate system, not the final target. The target might contain confidential information that the victim is obliged to protect, so the Police should have access to sufficient information for the investigation and no more. When a mob is throwing mud at your windows, do the Police need to search your safe?

More Information

PopVote hit with HK's largest DDoS attack, says HKU
'Referendum' organisers to extend poll after cyberattacks on electronic voting system
Cyberattackers brought down Apple Daily website with 40 million hits every second
Public urged to report cyber attacks
6.22 Civil Referendum
'Biggest ever'? Massive DDoS-attack hits EU, US
Biggest DDoS ever aimed at Cloudflare's content delivery network
Reforms vote extended one week due to hacker attacks
譴責網絡暴力 要求警方主動調查網絡攻擊
全民投票：實體票站詳情

HKMA Warns about general purpose web proxy domain p.uberthepyro.com

<web-link for this article>

The Hong Kong Management Authority (HKMA) has issued a warning about the domain p.uberthepyro.com that can be used as a proxy to any website. HKMA specifically warn that three banks (Chong Hing Bank Limited, Fubon Bank (Hong Kong) Limited and Public Bank (Hong Kong) Limited) have reported that their websites can be accessed via the proxy domain. The case has been referred to the Police for investigation.

The report did not mention any attempts to use the proxy domain fraudulently, for example, by distributing links to proxied bank websites by email.

Yui Kee Chief Consultant Allan Dyer commented, "This domain can be used to access many websites, for example the HK Government portal: http://www.gov.hk.p.uberthepyro.com/en/residents/. While it is possible it was set up for

fraudulent purposes, it seems more likely that it was intended as a private web-proxy, and the public access was unintended."

The HKMA advised, "bank customers are reminded to always connect to a bank website by typing the authentic website address in the browser or by bookmarking the genuine website for subsequent access, rather than through this suspicious website".

Dyer advised, "It is important to understand the security features of your browser. Modern browsers try to inform you which site you are using by highlighting the domain name. If the normal domain name of your bank is not highlighted, then you should be warned, and not enter sensitive information." For example, compare the browser address bar of the Fubon Bank via this proxy:

and direct: 

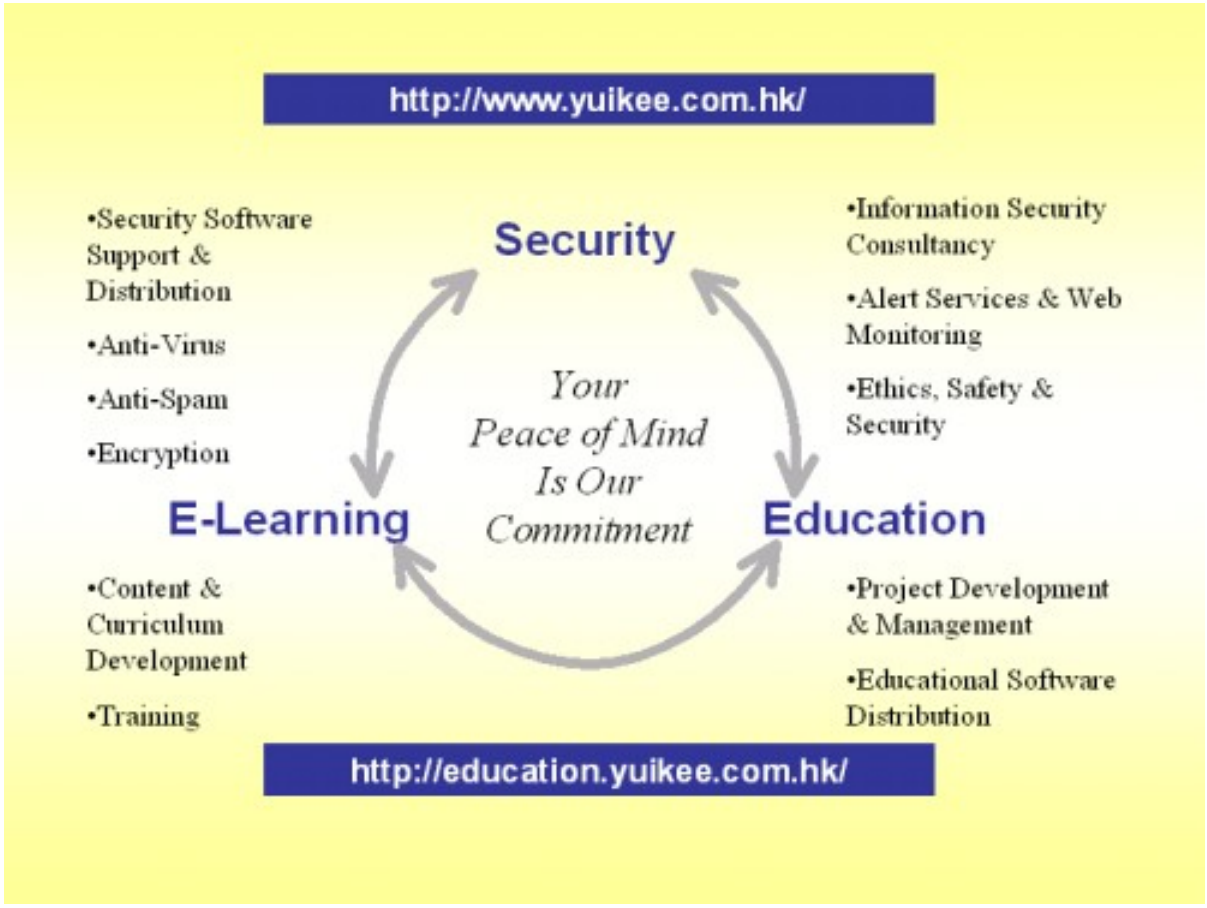
.

Dyer continued, "For bank transactions, or any other sensitive information, you should be using an encrypted connection, which can also verify the identity of the site. Firefox uses a blue or green bar next to the address to indicate a verified connection, as illustrated in our article on Purchase Order Phishing this month".

Anyone who has provided his or her personal information to the website or has conducted any financial transactions through the website should contact the bank concerned and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

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/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/