Yui Kee Computing Ltd.

Newsletter

May 2016

Contents

Contents....1
Corporate Finance (D.T.C.) Warns of Fraudulent Website....1
AVAR Conference Call for Papers and Early Bird Registration....2
Hong Kong Privacy Commissioner Shows Teeth, Marketing Company Fined....3
Public Bank (Hong Kong) Limited Warns of Unauthorised App Distribution....4
HKMA Launches Cybersecurity Fortification Initiative....4
Fraudulent Standard Chartered Website Wacked....5

Corporate Finance (D.T.C.) Warns of Fraudulent Website

<web-link for this article>

In a PDF dated 29 April 2016, Corporate Finance (D.T.C.) Limited has issued a warning about a fraudulent website, www.cfdtcltd.hk, using their name, saying they had reported the incident to the Hong Kong Monetary Authority (HKMA) and the Police. The HKMA issued a press release about the incident on 3rd May 2016. The fraudulent website remained active at the time of writing.

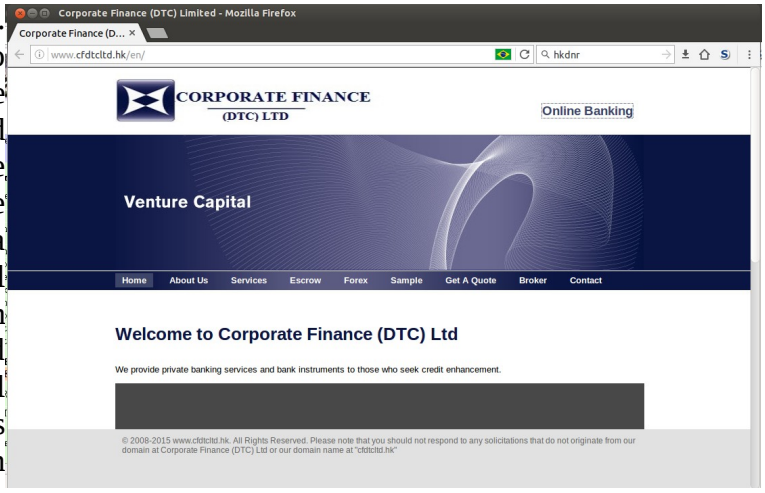
Victims should contact Corporate Finance (D.T.C.) Limited at (852) 2832 0180 Gloria Yu and the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860 5012.

Real Corporate Finance Website

Two features stand out in this incident: the inconsistent attention to detail in the fraud and the delay in effective action by the authorities.

The objective of the fraudulent site appears to be capturing customer login credentials, there is a prominent link to an "Online Banking Portal" that collects the account number and password. Comparing the real and fake websites, it is difficult to believe that any customer would be fooled. The real site is in Chinese, with no English, and the fake site is in English with no Chinese, and the corporate branding is entirely different. However, the contact details of the fake site use the real Company Registration number of Corporate Finance (D.T.C.) Limited

and a likely Hong Kong address. Why did the fraudster bother to get details that most people wouldn't check correct, and neglect to copy the corporate branding? This suggests that the fraudster was doing the same for a large number of financial companies, perhaps working from a list that provided the names and registration numbers. The email address provided in the whois record for the cfdtcltd.hk domain is jp-morgan0110@outlook.com, which suggests the domain owner was also involved with a scam targeting JP Morgan customers. If this is the case, there may be many more fraudulent .hk domains registered by the same person, and HKIRC should investigate the holding account, HK5017218T and consider suspending any domains found to be suspicious.



Fake Corporate Finance Website

Assuming Corporate Finance (D.T.C.) Limited issued their warning on 29 April, and the GIF of the warning on their website has the modification timestamp, "Friday, April 29, 2016 PM05:41:17 HKT", so the claim appears to be true, then why did it take HKMA four days to issue their warning, and why is the domain still accessible, when it is a .hk domain that HKIRC has the capability of suspending? Also, the whois record for the domain reveals it was registered on 12-10-2015, so it is likely that the fraudulent site has been operating for half a year. There is clearly a lot of room for improvement in responding to online fraud.

More Information

- Corporate Finance (D.T.C.) Limited ' s Statement on Fraudulent Website
- HKMA Press Release concerning Fraudulent website related to Corporate Finance (D.T.C.) Limited

AVAR Conference Call for Papers and Early Bird Registration

<web-link for this article>

The 19th annual conference of the Association of Anti-Virus Asia Researchers will be held in Kuala Lumpur from 30 November to 2 December 2016. The call for papers is open until 15 August 2016.

The conference theme is "Is AV dead?", and the organisers are looking to hear from proponents on both sides of the argument.

Early Bird registration for the conference is available before 20 September 2016. A range of sponsorship packages are available.

More Information

- AVAR 2016 Call for Papers
- AVAR 2016 Delegate Registration
- AVAR 2016 Sponsorship Packages

Hong Kong Privacy Commissioner Shows Teeth, Marketing Company Fined

<web-link for this article>

Marketing company, GMS (Asia Pacific) Limited ("GMS"), was fined HK$16,000 at the Kwun Tong Magistrates' Court on 16th May 2016 after pleading guilty to two offences under the Personal Data (Privacy) Ordinance (PDPO). The charges were using personal data without consent, contrary to section 35C of the PDPO and not complying with an opt-out request, contrary to section 35G of the PDPO.

In ay 2014, a complaint was made to the Privacy Commissioner from a person who had once made a hotel restaurant reservation, providing their surname and phone number. They stated that they had never given written or verbal consent for use of their personal data for direct marketing. Since then, they had received calls promoting the membership and services of the hotel. In April 2014, they received a call from GMS promoting the hotel and they requested opt-out. GMS agreed, but called again in May 2014.

GMS admitted receiving the opt-out request and claimed to have notified its IT department to place the number on their opt-out list, but suggested blame lay with part-time promoters who had not received or had overlooked the updated opt-out list.

The Privacy Commissioner for Personal Data Mr Stephen Kai-yi WONG said, "In order to comply with the marketing target's (data subject's) opt-out request effectively, marketing companies (data users) have to maintain a list of all customers who have indicated that they do not wish to receive further marketing approaches (i.e., the "Opt-Out List") and distribute the Opt-Out List to the staff members of the relevant department in a timely manner and thereafter communicate with the department from time to time. If the list is distributed other than by a computer network, it is recommended that marketing staff members are notified of the updates at a frequency of no less than once per week. A marketing company should have standing procedures for its staff members to follow and provide appropriate training with regard to accessing and updating the Opt-Out List for compliance with opt-out requests by marketing targets."

Yui Kee's Chief Consultant, Allan Dyer, commented, "Marketing companies are stupid and irresponsible if they rely on call centre staff to manually check their opt-out list. They provide the list of numbers to call to the staff, so they should automatically filter that list, removing matches with the opt-out list before they are provided to the staff."

More Information

- A Marketing Company Fined for Using Personal Data in Direct Marketing without Customer's Consent and Failing to Comply with an Opt-out Request
- PCPD fines GMS over opt-out regulation breach
- Guidance on Direct Marketing
- Exercising Your Right of Consent to and Opt-out from Direct Marketing Activities under the Personal Data (Privacy) Ordinance
- It is Your Choice to Accept or Refuse Direct Marketing

Public Bank (Hong Kong) Limited Warns of Unauthorised App Distribution

<web-link for this article>

Public Bank (Hong Kong) Limited (PBHK) has issued a warning about unauthorised distribution of PBHK mobile banking Apps. The apps appeared to be still available at these links at the time of writing:

- http://www.appdownloader.net/Android/App/1822599/com.publicbank.mobile/Download
- http://www.appdownloader.net/Android/App/1821512/ttl.android.winvest.pub
- http://www.appdownloader.net/iOS/App/991725973/com.pbhk.mst
- http://www.appdownloader.net/iOS/App/844658336/com.pbhk.app

The bank denies any connection with the website concerned and advises those who have used the apps from the unauthorised links to call their Customer Service Hotline at (852) 81070818 and to report the incident to the Hong Kong Police.

The domain name for the APPDownloader website was registered in 2015, and the site appears to host a large number of Android and iOS apps.

Yui Kee Chief Consultant Allan Dyer commented, "This may be a case of the website owner using the popularity of app downloads to serve advertisements but the risk is clear. Without a verified source, there is no-one to hold responsible if the download is malicious. PBHK could improve the information they give to customers by providing, on their website, a direct link to the authorised distribution point at the Google Play and Apple AppStore."

More Information

- Public Bank (Hong Kong) Limited Announcement Un-authorized Distribution of PBHK Mobile Apps
- Suspicious Internet banking mobile application (Apps) related to Public Bank (Hong Kong)

HKMA Launches Cybersecurity Fortification Initiative

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) announced today the launch of a “Cybersecurity Fortification Initiative” (CFI) at the Cyber Security Summit 2016. The initiative aims to raise the level of cybersecurity of the banks in Hong Kong using a three-pronged approach:

1. The Cyber Resilience Assessment Framework seeks to establish a common risk-based framework for banks to assess their own risk profiles and determine the level of defence and resilience required;
2. A new Professional Development Programme in Hong Kong including training and certification which aims to increase the supply of qualified professionals in cybersecurity;
3. The Cyber Intelligence Sharing Platform will be developed to allow sharing of cyber threat intelligence among banks in order to enhance collaboration and uplift cyber resilience.

Mr Norman T.L. Chan, Chief Executive of the HKMA, said “If we wish to raise the cybersecurity of our banking system to a level commensurate with Hong Kong's position as

the leading international financial centre in Asia, we cannot afford to go slow or lose any time. In a spirit of cooperation to achieve this common goal, the HKMA, the banking industry and our partners will work closely together to implement this ambitious but necessary CFI according to plan."

More Information

- Launch of the Cybersecurity Fortification Initiative by the HKMA at Cyber Security Summit 2016

Fraudulent Standard Chartered Website Wacked

<web-link for this article>

Standard Chartered Bank (HK) Limited has issued a warning about a phishing email and linked fraudulent website. The email advised customers to click on a "VERIFY MY ACCOUNT" link, which led to a page, cachoeiradoouro.com.br/cgi-sys/suspendedpage.cgi?id=hk, asking for e-banking account, password, transaction password, ATM card number and ATM PIN. Obviously, this is highly sensitive information that could be used for fraudulent transactions. The website had been removed at the time of writing.

Standard Chartered advised customers that it does not request customers' personal information (including user names and passwords) by email. It also does not request passwords, such as One-Time passwords, over the phone. Customers should log in to Standard Charter's Online Banking through its website, https://www.sc.com/hk/, and not through hyperlinks embedded in emails or third-party websites. Customers should verify they are connected to the real Standard Chartered website (e.g., by checking the SSL certificate) before entering sensitive information.

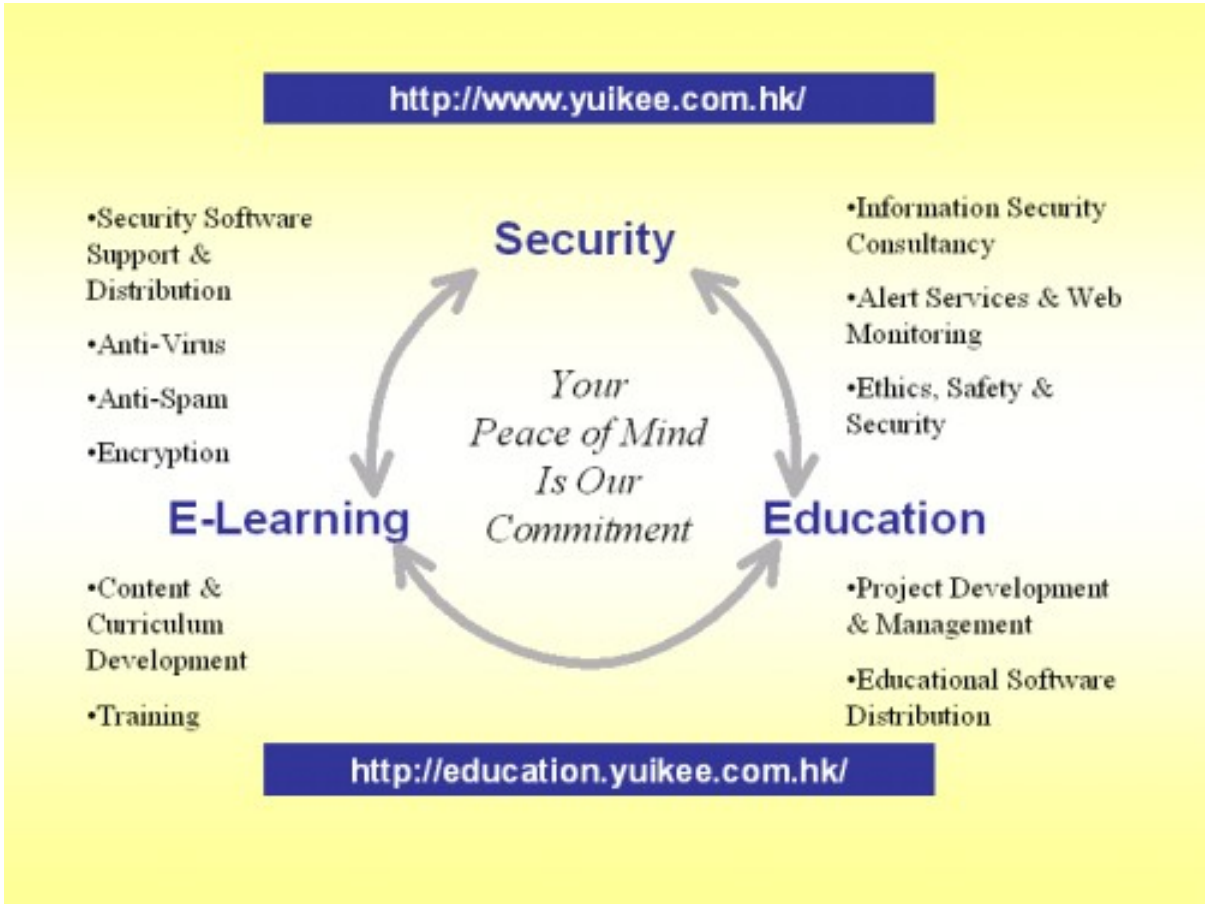
Victims should report the incident to the Police.

More Information

- Standard Chartered Alerts Customers to Fraudulent Website
- Phishing email related to Standard Chartered Bank (Hong Kong) Limited

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/