Yui Kee Computing Ltd.

Newsletter

October 2010

Contents

Contents 1
Beware of the Domain Name Registration Scam 1
    Recommendations 2
Dogbert on Privacy 3
Toothless Privacy Commissioner Fails to Gum Octopus 3
Privacy Laws to be Tightened 4
Privacy Commissioner Issues New Guidelines 4

Beware of the Domain Name Registration Scam

<web-link for this article>

The Domain Name Registration scam is not new, variants have been around for at least five years, but it is still happening. Presumably, some victims are falling for it, or the scammers wouldn't bother.

The scam starts with an email from a "domain name registration center" to a domain owner, the victim-to-be, warning them that another company is applying to register variants of their domain name under another top level domain. However, the scammers claim, they can keep the domain names safe, if the victim contacts them urgently. This is a recent typical example, received by Yui Kee:

From: "Angela" <info@ygnetworks.org>
Subject: Notice of Intellectual Property-Trademark Name
Date: Thu, 9 Sep 2010 16:31:54 +0800

Dear Manager:

We are a Network Service Company which is the domain name registration center in Shanghai, China. On September,8th,2010, We received HUATAI Company's application that they are registering the name "yuikee" as their Internet Trademark and "yuikee.cn","yuikee.com.cn" ,"yuikee.asia"domain names etc.,It is China and ASIA domain names.But after auditing we found the brand name been used by your company. As the domain name registrar in China, it is our duty to notice you, so I am sending you this Email to check.According to the principle in China,your company is the owner of the trademark,In our auditing time we can keep the domain names safe for you firstly, but our audit period is limited, if you object the third party application these domain names and need to protect the brand in china and Asia by yourself, please let the responsible officer contact us as soon as possible. Thank you!

Kind regards

Angela Zhang

Angela Zhang

Registration Department Manager
3002, Nanhai Building 854.Nandan Road
Xuhui District, Shanghai
Office: +86 216296 2950
Fax: +86 216296 1557
web: http://yg-networks.com
web: http://www.yg-networks.com

Other variants say that the Chinese character version of the domain name or the "Internet Keyword" is being registered, or that the registration is in the .hk top level domain. If you are a company worried about your brand-name you might panic and ask to register all of these, at considerable cost. What you would get for your money is uncertain, but it certainly won't include an "Internet Trademark", there is no such thing, the status of an "Internet Keyword" is more confused, but there is no recognised registration, so you won't get that, either. You might get a real registration of your name in some top level domains, at a greatly inflated price, or maybe nothing.

There are plenty of reports of this scam, mostly on various blogs and forums, but it is difficult to find any warnings on official sites - Police, Government, Registries or CERTs. In fact, some official sites act as a primer for the scam, for example this Hong Kong Government webpage about protecting against phishing says, "*Consider to register domain names that are similar to the one that is currently used by the organisation e.g. in addition to the original domain name "www.abcbank.com.hk", domain names "www.abcbank.com", "www.abc.com", "www.abcbank.hk" can also be registered.*". Anyone who has read that and later receives a scam email will think, "I was warned about this, and now it's happening", making it more likely they will succumb to the trick.

The top level domain usually targeted is .cn, along with .asia, .hk and .tw, and the sender usually claims to be the registration centre in China, to the extent that this is usually referred to as the "China Domain Name Scam". Maybe the scammers are preying on companies' eagerness to be prepared to enter important emerging markets?

Is this scam raking in big money for the scammers? We do not know, there seem to be no studies on it, and victims may not even realise they've been tricked. It is not even clear where reports should be made, your local police, the police in the scammers supposed location, a legitimate registry, a CERT, or a regulatory body?

Recommendations

- Domain owners should be aware of these scams, and remember that legitimate registrars do not send such notices.
- Warnings about domain hijacking and phishing should be amended to mention these scams.
- ICANN should provide clear, easy to find information on how to identify legitimate registrars for all top level domains.
- Law enforcement and regulatory agencies should decide on the most appropriate channel for receiving and processing reports of this scam, and publicise it.

More Information

Chinese Domain Name Fraud
Asia Domain Name Registration scam
The Chinese Domain Name Scam
Domain Name Registration Scam
Hong Kong Police Force - Provide Crime Information
Protect Against Phishing Attacks
Hong Kong Internet Registration Corporation Ltd.
Internet Keyword Scam
Briefing Paper on Internet Keyword Issues
Internet Keywords
Internet Trademark email - spam or scam?
What Is An Internet Trademark?
Office of the Telecommunications Authority, Hong Kong

Dogbert on Privacy

<web-link for this article>

One for the Privacy Commissioner.

More Information

Dogbert consults on Customer Data
Office of the Privacy Commissioner for Personal Data, Hong Kong

Toothless Privacy Commissioner Fails to Gum Octopus

<web-link for this article>

Hong Kong's Privacy Commissioner for Personal Data has released the results of his three-month investigation into the sale of personal data by Octopus Cards Limited. The current limit of the Privacy Commissioner's powers is to issue an "enforcement notice", but Commissioner Allan Chiang Yam-wang said that Octopus is unlikely to contravene the Personal Data Privacy Ordinance again, so no notice will be issued.

The investigation revealed that Octopus had broken three Data Protection Principles, but the company stopped after the investigation started and Brenda Kwok, the Office of the Privacy Commissioner's chief legal counsel, explained that an enforcement notice could be issued only if it was likely that a contravention would continue.

Yui Kee's Chief Consultant, Allan Dyer, commented, "Ms. Kwok's interpretation of 'likely' is very interesting. From a business standpoint, Octopus Cards made tens of millions of dollars from the sale of the data. If the Privacy Commissioner had issued an enforcement notice, Octopus would face fines or jail for another violation. However, in the current situation, Octopus could sell the data again, and the worst possibly penalty would be an enforcement notice. The rational business decision in this situation is to repeat the violation until an enforcement notice is issued, naturally apologising abjectly on each repeat."

More Information

Privacy Commissioner completed investigation on Octopus Holdings Ltd
Investigation Report – Octopus Rewards Program
Predator Cooperation
Octopus escapes penalty for selling data
Octopus slips off the hook after data privacy breach

Related Articles

Privacy Commissioner Issues New Guidelines

Privacy Laws to be Tightened

<web-link for this article>

The Hong Kong Government has published its Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance (PDPO) and launched further public discussions on the legislative proposals to strengthen personal data privacy protection under the PDPO.

The Government claims that most of the proposals are generally supported by the public and plans to draft legislation on 37 proposals in a number of areas, including direct marketing, data security, powers and functions of the Privacy Commissioner for Personal Data (PCPD) and offences and sanctions. The publications include the full report, highlights of the report and the public's written submissions. Some of the changes would certainly make data users think twice, such as a proposed maximum fine of HK$1 million and five years' jail for the unauthorised sale of private information, but others are decidedly weak, for example, the introduction of a voluntary personal data security breach notification system. Why would the worst offenders reveal their negligence?

The Privacy Commissioner has expressed disappointment that the Government is pursuing other proposals.

More Information

Views on the Review of the Personal Data (Privacy) Ordinance
Highlights of the Report on the Public Consultation on the Review of the Personal Data Privacy Ordinance
Report on the Public Consultation on the Review of the Personal Data Privacy Ordinance
Written Submissions to the Consultation on the Review of the Personal Data Privacy Ordinance
Press release on the Consultation Report on Review of Personal Data (Privacy) Ordinance published
Public Consultation on Review of the Personal Data (Privacy) Ordinance
Privacy Commissioner responds to Government's proposals on Review of the Personal Data (Privacy) Ordinance
Getting personal

Privacy Commissioner Issues New Guidelines

<web-link for this article>

Prompted by the recent serious public concern about the mishandling of customers' personal data by the Octopus group of companies, Hong Kong's Privacy Commissioner for Personal Data, Mr. Allan Chiang has published a new Guidance Note, titled "Guidance on the Collection and Use of Personal Data in Direct Marketing" providing data users with practical guidance on compliance with the requirements under the Personal Data (Privacy) Ordinance while engaging in the collection and use of personal data for direct marketing. It replaces the previous Fact Sheet, "Guidelines on Cold-Calling" and the Guidance Note on "Cross-Marketing Activities" previously issued by the Commissioner.

The note covers:

- Collection of personal data for direct marketing of products and services has to be related to the original purpose of data collection
- Personal data should not be excessively collected

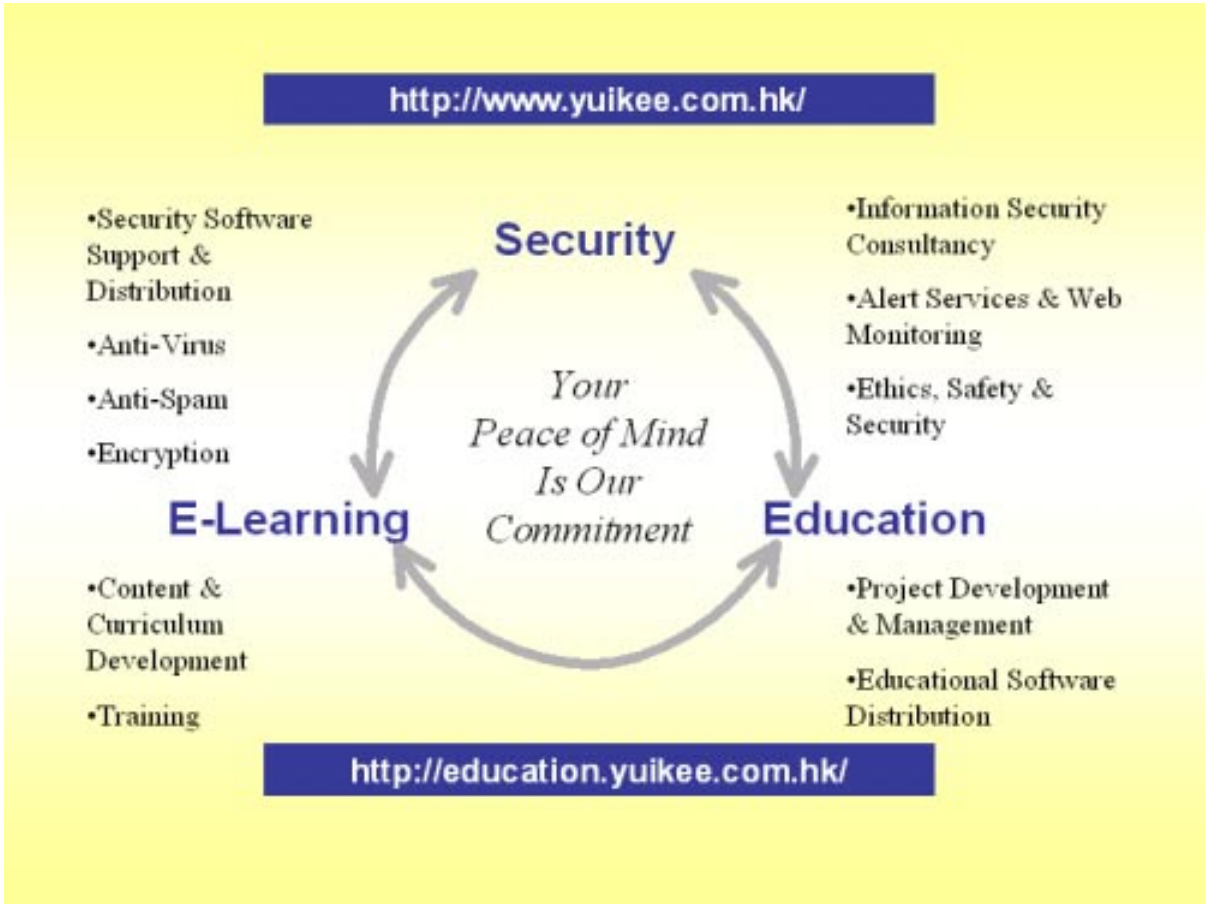
- Data subjects should be informed that it is voluntary for them to supply additional personal data required for direct marketing purposes
- Collection of personal data should be made by lawful and fair means, avoiding deceptive and misleading means and "bundled consent"
- A Personal Information Collection Statement ("PICS") should be effectively communicated to the data subject
- "Purpose of use" of personal data and "classes of data transferees" should be defined with a reasonable degree of certainty
- Recommends good practice for use of personal data collected from public registers for direct marketing
- Requirements for managing customers' opt-out requests under section 34(1) of the Ordinance:
- Control of direct marketing activities carried out by agent, contractors or business partners
- Recommended good practice for the maintenance of an opt-out list
- Guidance on data users transferring customers' personal data to a third party in return for monetary gains.

More Information

Privacy Commissioner publishes Guidance on the Collection and Use of Personal Data in Direct Marketing
Guidance on the Collection and Use of Personal Data in Direct Marketing
Toothless Privacy Commissioner Fails to Gum Octopus

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/