Abstract

Phishing scheme is a new emerging security issue of computer crime or e-commerce crime in globalization. In this paper, the legal framework of Malaysia, United States of America, United Kingdom and Singapore are analyzed and followed by discussion on critical issues that rose due to phishing activities, inter alia, the threat and magnitude of problem, techniques and variants of phishing. The paper also emphasized on the factor why phishing succeed due to human factor and technical subterfuge. The result revealed that inadequacy of current legal framework is the main challenge to govern this epidemic. However, lack of awareness among consumers, crisis on merchants' responsibility and lack of intrusion reports and incentive arrangement contribute to phishing proliferating.

In Malaysia scenario, amendments to legal provisions and better enforcement should be implemented to address this problem. Malaysia should analyse a suitable legal response through the provisions in United States, United Kingdom and Singapore model, and also emulate technical measure taken by the countries. Due to inadequacy of the current legal aspects with regard to the problem of phishing in this country, Malaysia also should adopt the legal approach taken by the United Kingdom for example through UK Fraud Act and USA Anti-phishing Act which targeting the entire scam process from sending of the email to the creation of fraudulent sites. The law should also stipulate that the perpetrator must have the specific criminal purpose of committing a crime of fraud or identity theft before an offence is made out. Even though Malaysia is still in an infant stage, the government, corporations and consumers could not afford to neglect this frightening fraud. On the contrary, each party must work hand-in-hand to turn the tide against proliferating fraud. Last but not least, solution for phishing is likely to be a combination effort between education, technology, legislation and law enforcement

Abstrak

Phishing atau penipuan identiti adalah merupakan satu isu keselamatan baru yang melibatkan jenayah computer di peringkat antarabangsa. Dalam kajian ini, kedudukan undang-undang di Malaysia, Amerika Syarikat dan United Kingdom diperincikan, seterusnya perbincangan isu-isu kritikal yang timbul daripada aktiviti *phishing* termasuk ancaman dan tahap masalah, teknik dan jenis-jenisnya. Kertas ini juga menekankan faktor mengapa penipuan identiti ini berjaya disebabkan oleh faktor manusia dan masalah teknikal. Keputusan juga mendapati kekurangan kerangka undang-undang yang sedia ada merupakan cabaran kepada masalah ini. Walau bagaimanapun, kurang kesedaran di kalangan pengguna, krisis tanggungjawab pedagang internet, kekurangan laporan gangguan turut menyumbang kepada peningkatan jenayah siber ini.

Pada masa yang sama, di Malaysia, pendekatan pindaan perundangan berkaitan dan penguatkuasaan undang-undang dilihat penting, termasuk menerima pakai undang-undang yang telah digubal di Amerika, United Kingdom dan Singapura, dan pendekatan secara teknikal yang diamalkan. Oleh kerana kekurangan aspek perundangan berkaitan masalah ini, Malaysia wajar menganalisa undang-undang yang diamalkan di UK seperti Akta Penipuan dan Akta Anti-phishing Amerika Syarikat yang mensasarkan kepada keseluruhan proses ia bermula dari penghantaran emel hingga penciptaan laman web palsu, dan menyatakan penjenayah mesti mempunyai tujuan jenayah yang khusus untuk melakukan jenayah penipuan atau pemalsuan identiti sebelum kesalahan itu dilakukan.

Walaupun jenayah ini masih baru di Malaysia, namun kerajaan , syarikat dan pengguna tidak boleh mengabaikannya, sebaliknya harus bergandingan untuk mengurangkannya. Jalan penyelesaian kepada permasalahan ini dan melibatkan usaha bersama antara pendidikan, teknologi, perundangan dan penguatkuasaan.