

May 10, 2016

CYBER CRIMES AND E-FRAUDS, A STARK REALITY IN THE VIRTUAL WORLD

Internet can be defined in many ways. It has its pros and cons and advantages galore but along with the opportunities it offers, it also is highly prone and susceptible to misuse, be it a simple thing like sending an e-mail or an online complex financial commercial transaction.

Some important terms that are common to internet are explained briefly:

Cybercrime

Cybercrime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the internet. For example; hate crimes, telemarketing and internet fraud, identity theft, and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the internet.

E-fraud

Any dishonest activity that involves the internet as the target or means of obtaining some financial reward.

Mobile Wallets

Mobile wallet refers to as mobile money, mobile money transfer, and mobile wallet generally refer to payment services operated under financial regulation and performed from or via a mobile device.

Invoicing Frauds

A contractor or supplier can commit fraud by knowingly submitting false, inflated or duplicate invoices with the intent to defraud, either acting alone or in collusion with contracting personnel as the result of corruption. "False invoices" refer to invoices for goods or services not rendered.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Bitcoin

A type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

E-mail spoofing

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

Domain name tweaking

Changing the domain name smartly with replacement of simple one two letters, without normal person figuring out in hurry.

Example – www.microsoft.com; www.microsotf.com; www.micrnsoft.com

Hardware hacking method

Hardware hacking means modifying a piece of existing electronics to use it in a way that it was not necessarily intended.

We also briefly discuss a recent case with respect to a cybercrime

A cyber criminal hacked into a Sharjah Bank website and held the Bank to ransom by leaking confidential data of clients on social networking and microblogging site Twitter every few hours. The criminal 'Hacker Buba', used a stolen picture of a bank staff and threatened the Bank that he will not stop leaking the data until the Bank pays him an undisclosed amount of ransom money in the digital currency Bitcoin in 7 days.

True to his word, Hacker Buba dumped tens of thousands of customers' transactions history online by posting the account statements of government entities and scores of UAE firms and individuals daily.

The Bank requested Twitter to suspend Hacker Buba's account but the reprieve was short-lived. The following day, he created a new identity and was back with a vengeance, uploading account statements of yet another customers of the Bank, in just one tweet attachment.

Earlier, Hacker Buba had sent warning text messages and emails to several customers of the Bank, saying their accounts were under his "control" and that they must pay him directly or get their Bank to do so failing which he would release their bank statements online. The Bank admitted the cyberattack and confirmed they had received the ransom note and the Bank had to pay Hacker Buba a ransom of \$3million!!.

There are many unsung heroes who safeguard our financial transactions from these greedy perpetrators including the Cyber Crime Cell's Role which is pivotal but highly burdened due to lack of infrastructure. Even when the trials for such crimes are conducted, the Judges do not possess the required technical knowledge for the same. Although, we may mention that various amendments have been made in the Indian Evidence Act to facilitate admission of electronic records as evidence.

One needs more awareness on the cybercrimes and laws encompassing the same as also some workshops and programs imparting the technical knowledge of the cyber world and practical knowledge with regard to implementation of these technical aspects in simpler terms in order that the stake holders may more efficiently understand the online transactions and modus operandi used by the menace creators in tandem with the relevant laws including the Indian Evidence Act, Indian Penal Code, the Information Technology Act, etc.

The contents hereof should not be construed as legal opinion. This provides general information existing at the time of preparation and is intended as a news update and ANB Legal neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained herein. It is recommended that professional advice be taken based on the specific facts and circumstances. The contents hereof do not substitute the need to refer to the original pronouncements.