eSecure

Secure and be Aware !

An e-zine from CySI

[Volume 1, Number 6]
March 2014

President's Column

Back to the Basics – Awareness

Thanks to the initiatives of Reserve Bank of India, banks and other concerned organisations, the public awareness on the risks in an electronic transaction has increased enormously. But given the rate at which e-commerce and e-banking is increasing and with more and more apps flooding the market with newer features, the users are always caught in a web, really a "world wide web – www" of confusion on how safe and secure a product is, how dependable the internet is and in case of any problem, where and how to report especially .with no such provider having an office in India with no helpline and with the only redress mechanism being the email, if any, provided.

Recently, a newspaper wanted my opinion on one of the apps provided in Google Play store advertising that the apps can be downloaded and used for doing mobile banking for the banks whose names and logos were also furnished. Customers reportedly downloaded the apps. Immediately, they found to their shock that the moment the apps have been downloaded and the moment they gave the account details, money has been withdrawn from their accounts, without ever their doing any remittance transaction at all. On checking up with the bank I found that the bank's website carries a caution message in the home page itself that Internet banking is not to be done from mobile devices, with apps downloaded from the Internet. Of course, the concerned bank here will take refuge under the fact that adequate warning has been given and awareness created and perhaps the legal requirement too has been fulfilled.

But the larger question remains how much is enough, how much is mandatory and how much is required from a social awareness and a customer security perspective. Such banks can and I am sure will (if not done already) raise

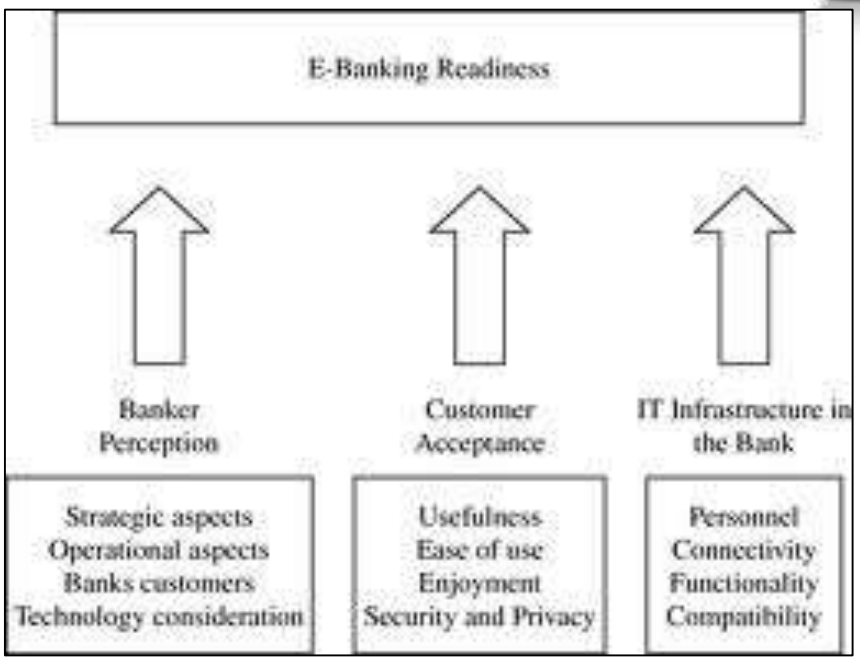
Editorial Board

This Issue

*****

a formal protest to the providers to remove the bank's name and logo from the list and avoid further damage to prospective victims. In an over enthusiasm to project themselves as more tech-savvy and customer-friendly in the competitive banking industry, banks are introducing more and more technology products with more and more features and in the process, gullible and innocent customers are sometimes caught unawares to identify what is absolutely essential, what is a comfort and what is purely avoidable and risky.

All this brings us back to the basics viz. Customer Awareness and User Knowledge – the purpose of our introducing the CSAP Cyber Security Awareness Program. It continues to be the most fundamental of our avowed objective that we in **CySI** have been striving for, in the past ten years of existence, as we complete a decade as Not-for-profit, socially-committed organization of dedicated tech-savvy individuals.



More with such news, in the next issue! Best wishes and regards to every reader and hoping to get your feed-back,

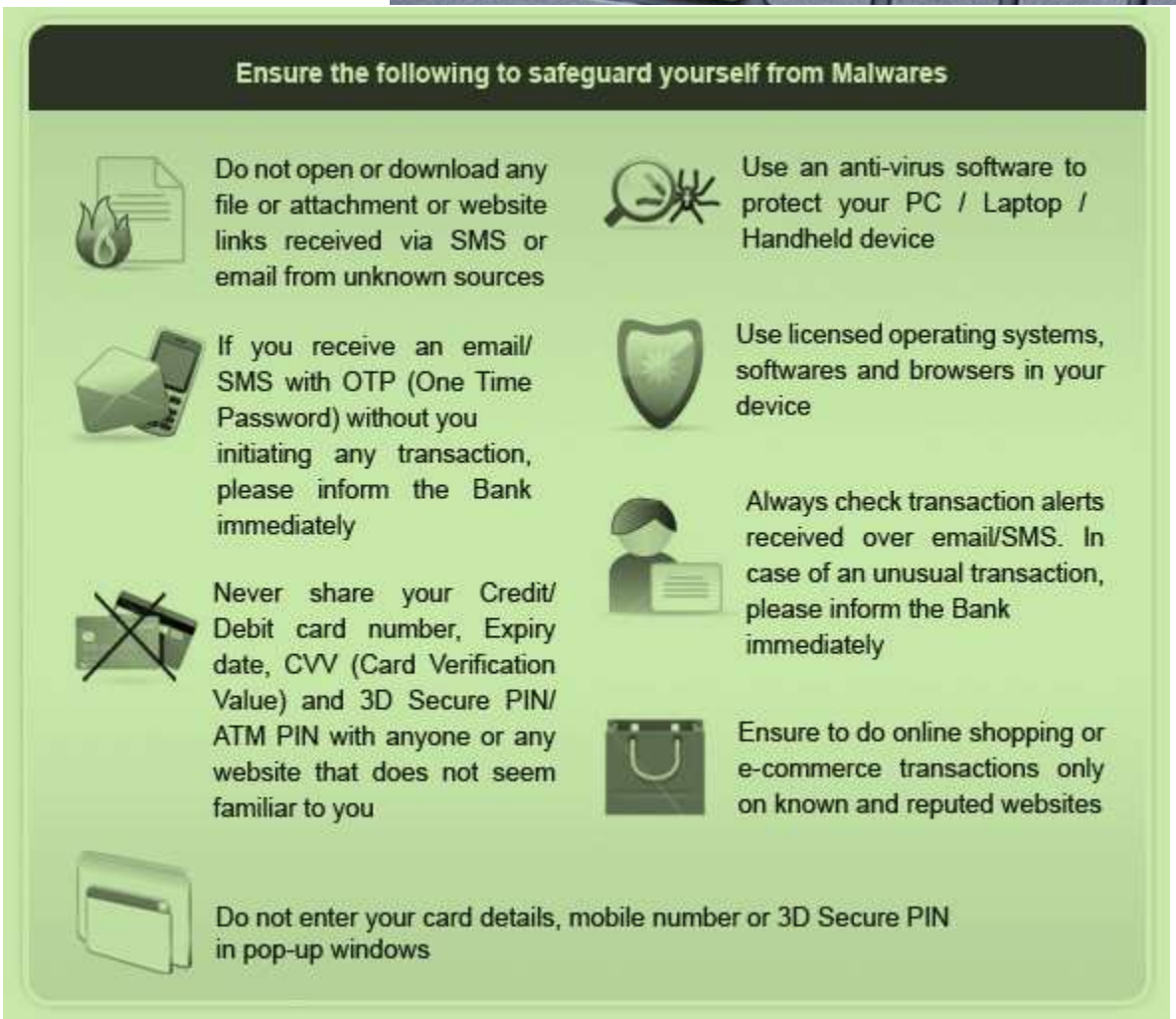
Rajendran V.

*****

Editorial

Beware of Malware

Malware, short for malicious software, is a computer program designed by fraudsters to infiltrate and steal your sensitive data from PC, laptop or handheld device.



Courtesy ICICI Bank Ltd.

Dr. Ramamurthy N

*****

Cyber Attacks on the Rise in India

The ease of online banking and transactions has brought with it a significant rise in malicious attacks on digital devices and software systems. Most of these attacks, as recent instances of online thefts have demonstrated, have been in the banking and financial services domain.

According to reports the problem has become more complex with the proliferation of mobile devices and the users' preference towards transactions on the go. In addition, there is also laxity on the part of the users when it comes to following safe practices during such transactions, coupled with a significant lack of manpower with skills to handle the rising number of such attacks, the agencies' report.

India has seen significant increase in attacks against financials and government, with 34% and 43% of them reporting cyber threats and attacks respectively, up from last year's 15% and 19%, the report revealed.

Close to an alarming 75% participants displayed low levels or a lack of skill in error handling, while 73% participants were not adequately equipped with skills in file handling, the report revealed.

Experts have recognized that malicious file inclusions, malware distribution and distributed denial of service s (DDoS) attacks are known threats that can arise out of improper file handling and such threats are often used to synchronize attacks on websites or large networks, the report stated.

Source: http://timesofindia.indiatimes.com/tech/enterprise-it/security/Cyberattacks-on-the-rise-in-India/articleshow/31757791.cms?

Companies fear Cyber fatality after attack

The recent data breach at an U.S. retailer, in which the personal data of at least 70 million customers were stolen, is an all-too harsh warning of the global threat of cybercrime.

Economies, companies and citizens are all at risk from having data stolen and the consequent sudden financial loss, according to analysts.

Meanwhile, governments are highly concerned about cyber-attacks. The U.K. affords cybercrime the same threat status as terrorism, while FBI Director James Comey has said cyber-attacks are surpassing terrorism as the major threat in the U.S.

Companies unprepared for attacks

Cybercrime is on the rise. Nearly a third of the 1,900 global senior executives surveyed reported the **number of security incidents within their organization had increased** over the 12 months up to October 2013. CNBC's own Global CFO Council survey **showed 83 percent of respondents were worried about cyber-attacks**.

Although almost half of the companies surveyed said they planned to increase spending on security. Experts said firms failed to recognise the severity of the cyber-threat and were inadequately protected.

"This sort of thing is often delegated to the IT departments, when it should be discussed at a boardroom level", David Cook, solicitor advocate in the regulatory team at law firm Pannone, said in a phone interview. "More often than not, nobody has even bothered to look at the security vulnerabilities in a company until it's too late".

Virtual crimes can be committed in a number of ways, from simple spam emails containing viruses to complex attacks aiming to bring down a network. And the financial risk to the global economy is very real, **costing around $300 billion annually**, according to a report by the Washington-based Center for Strategic and International Studies.

With hackers continuously looking for new ways to attack, companies are left trailing behind. Ernest Hilbert, former FBI agent and head of cyber investigations for EMEA at risk consultancy Kroll, thinks companies should be proactive in order to counter hackers.

Is personal data safe?

Customers' personal information is one of the tastiest pieces of data for hackers to target, as credit card details, addresses and emails can potentially be accessed.

As companies grapple to strengthen their security, individual users who transfer data everyday must also be responsible, one expert said.

"We don't need the internet army to prevent this, we need a group of health professionals," he added.

Full report can be read at : http://www.cnbc.com/id/101338187

ATM Skimming:

Internet is like a double edged sword – one that can be used positively to learn the happenings across the world and can also be negatively used by Cyber rogues. Choosing the former option, we came across a new form of skimming device used in ATMs somewhere in the world. It may or may not happen; it might or might not have actually happened anywhere leave alone India and could be just a figment of imagination by someone too. But, the very fact that someone has thought about this opens up a possibility of someone else taking the clue.

Taken from Internet and reproduced for the benefit of the common man.

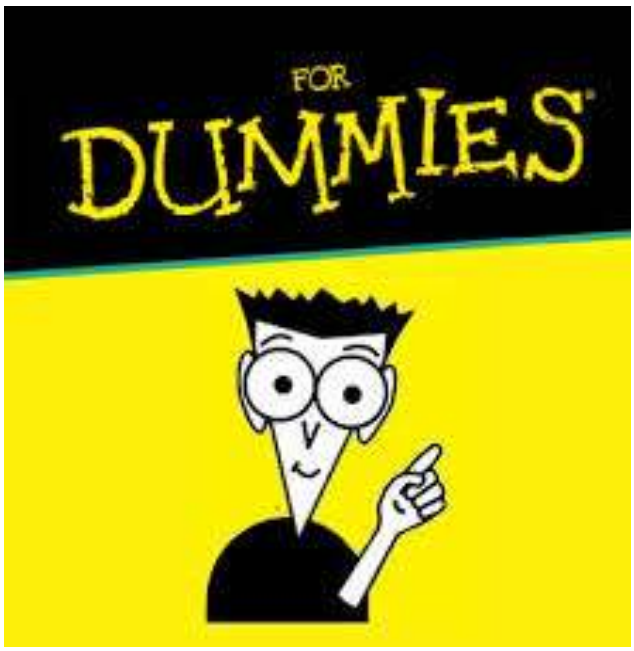
Kapaleeswaran V

*****

Dummies' Corner

The below questions may seem silly, but they carry lot of messages. They are meant for laymen and not for experts.

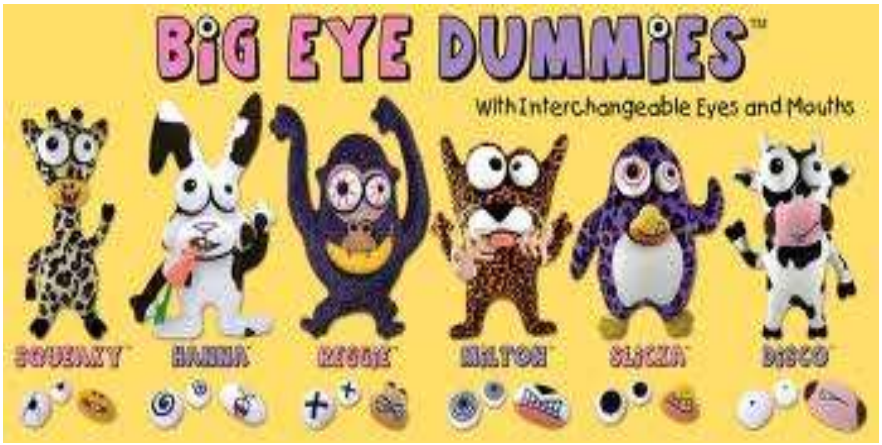
Question 1. *Whenever I fill petrol for my car and pay with my card, the petrol station employee takes it inside a room and returns it only after a few minutes. Is there any risk involved in parting with my card? I noticed this in a hotel also recently. Can I give the card to such persons? Is it possible for them to misuse my card?*



Answer: It is one of the basic Dos and Don'ts while using a credit/debit card is that NEVER part with your card and never be away from your card. You are exposing yourself to the risk of card skimming or card cloning i.e a technology by which the magnetic stripe information (where the important card information are stored and which is read by the swiping device) can be copied with the help of a skimmer and later with an encoder, the same data can be copied on to a new blank card. Duplicate cards, which are not PIN enabled (i.e. those which do not ask for a PIN, in addition to swiping) are made ready so easily and online purchases can be made from such card. You will know only when you receive the SMS from the bank. Hence, it is always absolutely safe and essential that you follow the card, whenever it is taken for swiping and ensure that the swiping is done only once and that too in one device only. Nowadays such skimming (cloning) devices are available in a small portable and easy to carry sizes also.

Question 2. *I have reasons to believe that my email account has been broken into- what is to be done please?*

Answer: Whenever in doubt that your email account has been hacked or you suspect that somebody has accessed your email account, please change the password immediately to a stronger one i.e. with a number, a character preferably partly with upper case and a special character (like @ or $ or % etc.). If you suspect serious data spying involving financial or reputational or other forms of losses, because of such activity, please report it to the cyber crime police. The police have the technology to trace the details of such hacker or criminal or any person with such unauthorized access.



Answers by ***Rajendran V***

*****

The IT Act – Some Basics

Sec 66 B of the Information Technology Act deals with punishment for dishonestly receiving stolen computer resource or communication device.

A simple analysis of this Section constitutes the following.

- A person dishonestly receiving or retaining any stolen computer resource or communication device.
- That person to have knowledge or having reason to believe the same to be stolen.

In the presence of both the above conditions, that person shall be liable under this Section and shall be punished with imprisonment for a term which may extend upto three years or with fine which may extend upto one lakh rupees or with both.

The terms “computer resource” and “communication device” have very wide scope and they encompass many things - hardware, software, output device, the output, storage devices, a printer, instruments such as cables, switches etc.

Even a data, a formal representation of information, knowledge, facts, concepts or instructions intended to be processed, being processed or has been processed in a computer system or a network come under the definition.

One thing may not fit into the classification of 'computer' under some laws but well within the meaning of 'computer' under the Information Technology Act. A classic example of such a situation would be the reported case of Diebold Systems Pvt. Ltd. Vs. Commissioner of Commercial Taxes in the High Court Of Karnataka. The question arose whether an ATM machine could be classified under 'computer terminal' or under 'electronic goods' under the Commercial Taxes Act. It was extensively argued and was decided that ATM was not a 'computer' and so could be brought only under 'electronic goods'. But under the Information Technology Act, an ATM can well be brought under the definition of a computer.

Now let us examine the terms 'receives' or 'retains'. A person may either buy, borrow, steal, rob, extort, receive as gift or just receive and retain in his possession of any computer resource or communication device. In any of above case, it would amount to receiving or retaining.

The essence of this Section is the dishonest element attached to receiving or retaining computer resource or communication device. The intent to cause wrongful loss to one person or wrongful gain to another person is essential for this Section to attract.

Let us analyse a scenario: Suppose X after stealing a mobile phone, sells it to Z at a price much lower than the market rate, Z could also be liable as there is every possibility that Z has reason to believe that the device is a stolen property. This Section apart, there are other provisions in the Act where a person may unwittingly become liable for charges both civil and criminal and would be burdened with proving his innocence. Suppose X sells the device to Z at the market rate saying that he wants to sell the same and buy a newer version, Z may not be liable under this part of the section. It would always be advisable to buy any computer resource with proper supporting documents.

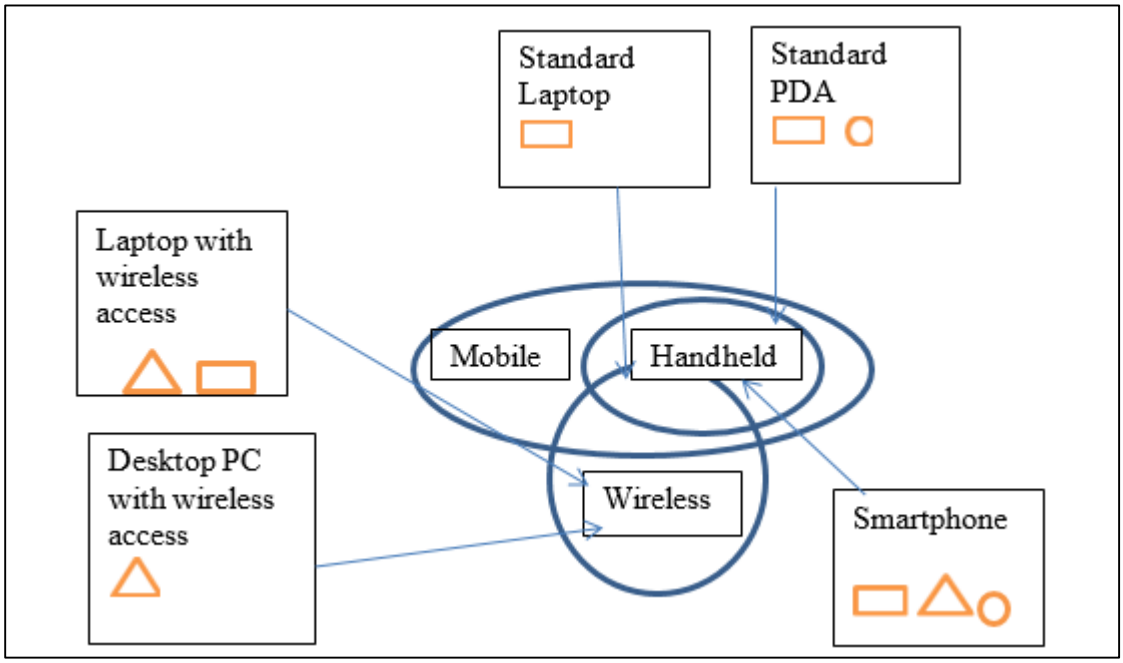
The application of this Act, still being in the infant stage, will take time for understanding. Reporting of incidents are low and as such case laws are very few compared to conventional crimes.

Ms. ***Padma R***.

*****

Proliferation of Mobile and Wireless Devices

In the modern days, the study of security cannot be complete without this topic. Use of mobile handheld devices, wireless computing and wireless network are much rising in importance day by leading to a better understanding of the technology involved in mobile computing and wireless network, at least from a layman's perspective. As the use of mobile phone increases thanks to the rising need for mobility of human beings, the security in such communication also assumes greater significance. We use laptops, PDA (Personnel Digital Assistant like a palmtop computer) and mobile phone. Even the simplest of handheld devices needs enough computing power to run small applications, play games, music and make voice call. Let us first have a clear of the key terms, mobile computing, wireless computing, and handheld device. Wireless means transferring information between computing devices such as PDA, etc. For example lasers are used in wireless data transfer between buildings, but cannot be used in mobile communication.



Constraints of encryption, laymen's approach:

What is cryptography? It is a combination of all methods used to ensure secrecy and authenticity of information, cipher and its stream. This helps you to provide accountability, fairness, accuracy and confidentiality. It can also prevent frauds in e-commerce and assure the validity of your financial transactions. It can keep away vandals/ criminals by alerting the webpage and prevent industrial competitors from reading confidential documents. Cryptography not only lends authenticity to your communication but also provides the sender a satisfaction that his/her message or communication has reached the person intended to. Interestingly, though cryptography as a subject in communication and technology may sound new, as a subject and as a concept, it is quite old and historic. One of the earliest reference to cryptography can be dated back to around 300 BC when Kautilya alias Chanakya in his much acclaimed administrative treatise "Artha shastra" refers to the use of cryptographic communication between rulers and other specific stake holders and underlines its significance.

To be continued:

Dr. Sankara Gomathi

*****

Pictures are added to the articles of this ezine for effective reading/ understanding. Most of the pictures are taken from Internet. Our editorial board wishes to convey its thanks for the courtesy of whoever has taken strains to draw and uploaded the pictures.

This ezine and all the previous issues, as well, can be read from our web-site http://cysi.in/.

The contents in this ezine are meant for sharing of knowledge and hence readers are requested to circulate this ezine in full or in part to anyone they like. Probably the readers may like to acknowledge CySI while reproducing the articles.

Readers are requested to send their feedback, articles, jokes, etc., to ezine@cysi.in.

Let us meet in the next issue with more thought-provoking articles.

Disclaimer:

Neither CySI nor the members of the Editorial Committee/ Board owns any responsibility for the views expressed by the authors in the articles. The views expressed are the concerned author's individual views only.

Editorial Board