

eSecure



Secure and be Aware !

An e-zine from CySI

[Volume 1, Number 5]

February 2014

President's Column

Editorial Board

Banking on Technology! - While modern day bankers want to rely upon and bank on the strength of technology, it is banking *in* Technology that has gained more importance these days. No bank worth its name today, can afford to ignore the strength of technology. Technology products in



banking are increasing day by day and more and more innovative products (mostly in the form of schemes and plans of customers' deposits) are getting introduced wholly relying on technology and electronic

communication. Hence it has become imperative on the part of top management of banks to take care of customer service efficiently, speedily and simultaneously take care of the security of their money too.

In the context security of customers' deposits, the concept of Return on Investment should never be a point of discussion. Every organization keeps a fire extinguisher in its premises and never speaks of the RoI on such equipment. One only prays that one should never have an occasion to use such equipment. Similar is the case with Information Security spending.

It is unfortunate that recently the CEO of a leading private sector bank talking of introducing an enhanced security feature in Internet Banking, said that the spending on such initiatives are not advisable from cost perspective. Perhaps, absence of such a security initiative may trigger just one or two additional cyber-crime in the bank initially. But, the message that such a vulnerability exists and the bank is hesitant to spend on this front, is enough for a fraudster to exploit the same and target such customers in more number in the days to come.

Publishers: Cyber Society of India (CySI)

President of CySI -

Ex-officio Executive Editor:

Mr. Rajendran V

Editor: Dr. Ramamurthy N

Editorial Committee:

Mr. Kapaleeswaran V

Mr. Murugan R

Ms. Panchi S

Advisors:

Mr. Srinivasan K

Mr. Na Vijayashankar

This Issue

1. President's Column	1
2. Editorial	3
3. Cyber Updates	4
4. Dummy's Corner	5
5. Some Interesting Quotes/ Cartoons	6
6. e-Commerce - FAQs	7

It is also interesting to note that some customers feel comfortable if the bank asks them fewer questions and makes Internet Banking or other forms of electronic banking an easy one, though in reality, the easier the transaction is the less secure it would be.

Hence banks should not hesitate to put in place all information security initiatives in place like a 2-factor authentication, One Time Password or a Session Generated Password along with a system of compulsory change of password in a given period etc. True that such initiatives may initially, give some difficulty and inconvenience to the customers. The customers at the end of the day, however, will understand that it is after all, their money and all such measures are being taken for their security only. The users too should get used to an era of OTPs, Bio Metric Authentications, 2-Factor Authentications, stronger (read unguessable) passwords, frequent change of passwords etc.

Hoping to see you all with more news and views on Information Security in the next issue.

Rajendran V.

Achievement of Members of CySI

CySI is proud to share with our readers the news about the rare honour conferred on one of the founder members of CySI, Editorial Advisor and past-President of CySI Shri **Srinivasan K (PPS)**, by the former President of India Dr A.P.J. Abdul Kalam. On 13th February 2014, Shri PPS travelled from Mumbai to Nagpur in a five seater aircraft along with Dr Kalam, his Personal Assistant and guards. Dr Kalam addressed a 50,000-strong gathering of students and around 1000 faculty members drawn from various colleges in and around Nagpur, in a meeting organised by the Member of Parliament of Chandrapur Shri Hansraj Gangaram Ahir and coordinated by Shri PPS. Dr Kalam gave a motivating talk to the students on the importance of education and the social and cultural values of India.



Dr. **Ramamurthy N**, Editor of this ezine and a life member and a member of Executive Committee, of CySI has another feather in his cap. Four more books penned by him have been published:



1. Secrets of Mahashakti – Mystery of Chandi,
2. Advaita in Shaakta,
3. Number System in Sanskrit and
4. Vedic Mathematics

This takes his total published book count to 13. Three more books are in printing and more books on the anvil. His books are based on Spirituality, Banking, IT, Mathematics, etc. CySI wishes him more success in all his endeavours in spreading his knowledge, experience and expertise.

Data Privacy Day

Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. Data Protection Day commemorates the January 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. Data Privacy Day is now a celebration for everyone, observed annually on January 28.



First time in India, **Data Privacy Day**, was celebrated by NASSCOM on January 28th 2014.

The importance of Data Privacy need not be stressed. In the recent episode in Korea, **Credit card details from almost half of all South Koreans have been stolen and sold to marketing firms.**

The data was stolen by a computer contractor working for a company called the Korea Credit Bureau that produces credit scores. The names, social security numbers and credit card details of 20 million South Koreans were copied by the IT worker. The

scale of the theft became apparent after the contractor at the center of the breach was arrested.

Unprotected data

Managers at the marketing firms which allegedly bought the data were also arrested. Early reports suggest that the contractor got hold of the giant trove of data – thanks to the access Korea Credit Bureau enjoys to databases run by three big South Korean credit card firms. The contractor stole the data by copying it to a USB stick.

Regulators are now looking into security measures at the three firms - to ensure safety of data. A task force has been set up to investigate the impact of the theft.

The three bosses of the credit card firms involved made a public apology for the breach. In a statement the Financial Services Commission, Korea's national financial regulator, said: "The credit card firms will cover any financial losses caused to their customers due to the latest accident."

This theft of consumer data is just the latest to hit South Korea. In 2012, two hackers were arrested for getting hold of the details of 8.7 million subscribers to KT Mobile.

Some of the ways to protect data:

- 1) Understanding nature of Threats, Trends and Technologies
- 2) To clearly understand the Opportunities and Challenges in the space
- 3) Evaluate the digital assets, etc., through Ethical hacking or otherwise
- 4) To have the best IS policy in tune with future roadmap of data privacy/ protection and ensure religiously implementing the policies and procedures.

Courtesy and for further reading: <http://www.bbc.co.uk/news/technology-25808189>

Dr. Ramamurthy N

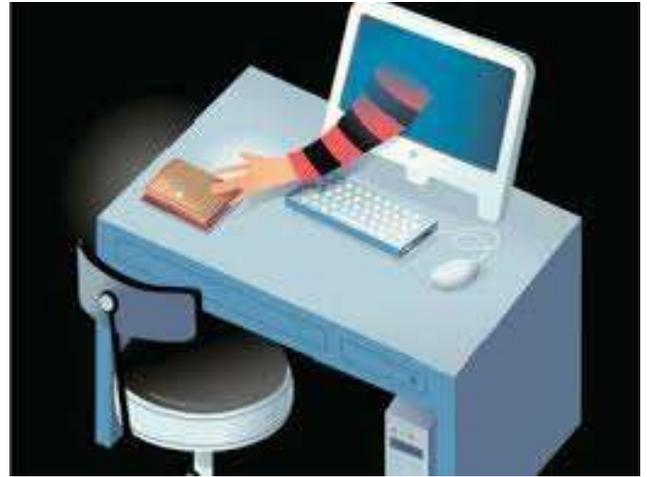
Cyber Updates

Online Bank Frauds on the Rise

Recently, there has been a rise in cases of hackers targeting bank accounts with huge balances, especially those belonging to celebrities. The Chennai, (Tamil Nadu, India) City Police have received many complaints about bank frauds, including from a famous sportsperson and from a well-known family involved in film production.

Reliable sources with the Bank said the sportsperson, who is also a television commentator and holds an account with the nationalised bank, lost ₹. 7.45 lakh towards the end of 2013, after a hacker sent two e-mails to the branch manager pretending to be the sportsperson.

“The culprit changed one alphabet in the sportsman’s name and sent an e-mail with the client’s bank account number and other details, asking for a transfer of money to a particular bank account. Treating the request as a genuine one, the manager approved the money transfer,” said a representative of the bank. A thorough probe is under way.



Similarly, online fraudsters also targeted the account of a woman who is part of a family involved in Tamil movie production for decades. A whopping amount of ₹. 27 lakh was siphoned from the victim’s account in a bank after the culprit hacked into the online bank account, and sent an e-mail to the bank representatives. Acting upon the email, the bank transferred the sum. Following a complaint to the city police, the bank took responsibility and refunded the money to the customer, police sources said.

News of such frauds and the relative reports apart, the issue poses a larger question: “Authenticity of email account”? Experts have always spoken about “Confidentiality, Integrity and Availability” as the three main pillars of Information Security and nowadays “Non Reputability’ and added to it, Authenticity, Accountability, etc., are also studied along. Emails in their present form, without a digital signature are not authentic ones and it is always ab-initio risky and unreliable to act upon an email communication of some criticality or those involving financial nature. Perhaps users of email especially those in the Banking and Financial Sector Industry should be very well made aware of the implications of relying upon an email for any critical and formal transaction.

Source: <http://www.thehindu.com/news/cities/chennai/online-bank-frauds-on-the-rise/article5654075.ece?>

Passwords and Passing Words

US security firm SplashData has announced, its annual list of the 25 most common passwords found on the Internet after analysing millions of stolen passwords posted online in 2013. The list of frequently used passwords shows that many people continue to put themselves at risk by using weak, easily guessable passwords. Some other passwords in the top ten include "qwerty," "abc123," "111111," and "iloveyou."

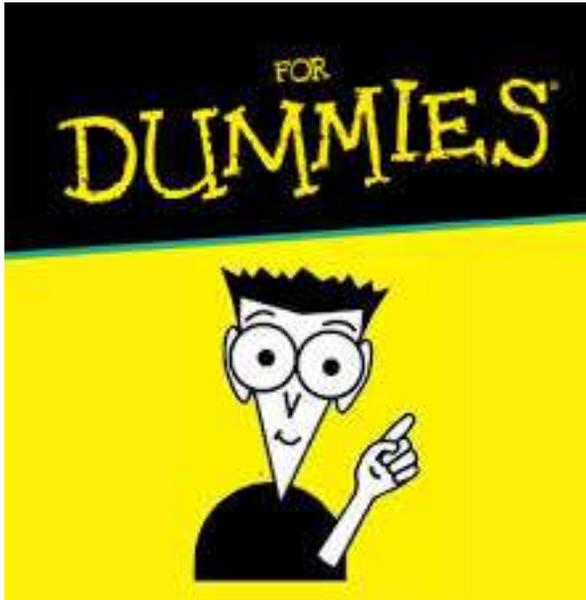
For example, new to this year's list are simple and easily guessable passwords like "1234" at 16th spot, "12345" at number 20, and "000000" at 25th position.

Source: <http://www.financialexpress.com/news/123456-worst-password-of-2013/1219631?rhnews?SocialMedia>

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.



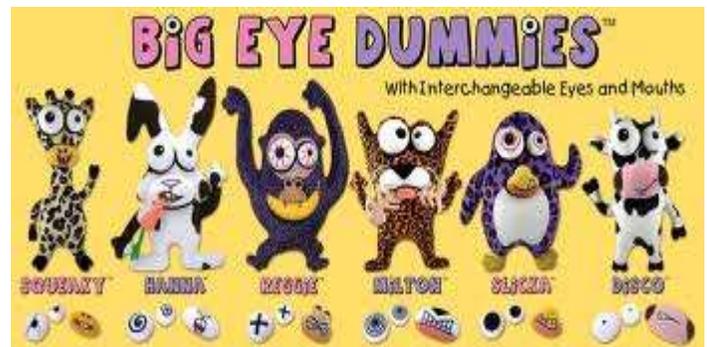
Question 1. *I received an email from my family friend that he is struck in some African country and that he requires some financial help. Can I send money to the address given in the Email?*

Answer: This is one of the hoax and con mails doing rounds in the recent days. The thumb rule is: Never believe anything that is received as an email, asking for any confidential information or funds of any type. If your friend is really struck somewhere, he would either call you or send information otherwise and not ask for money to be sent to some third party unrelated beneficiary's account. By a technological process called email spoofing (i.e. sending an email from some other id and making it appear to the receiver as something else i.e. like yourfriend@xxx.com etc.) the sender makes you believe that the mail is from your friend only. Since the fraudsters are stationed abroad and work as a network. Sometimes, even the money you send to will be for the credit of somebody else's account acting as an intermediary (called

'money mule') who just receive the money and retain a small portion say around 10% towards their charges and give the major amount to the fraudsters. Thus, even when nabbed, only these intermediaries mostly from the uneducated and lower income group segment falling for small but quick money will be caught!

Question 2. *When I was entering my office, a guy who claimed to have lost his documents including his ID card, came along with me after my swiping the card. Is taking him along with me correct or anything wrong with my act?*

Answer: This kind of entry is called 'tailgating' i.e. entering like a tail in somebody else's identity. In a physical premises with a swiping card entry for employees, if someone swipes his card and before the door closes, if the next person enters it is 'tailgating' and the person who swiped his card will be perhaps blissfully unaware that the system has taken his entry alone on records and not that of the next person who has also entered. Sometimes in organizations, the access card user may swipe his card and let the other person enter, without he himself entering too, to avoid the hassle of getting a temporary visitor pass enabling the new comer to enter. In a computerised environment too such unauthorized access is possible, when a person enters his log in id and password and does some data entry and before he logs out or is otherwise busy not attending to his computer, somebody else does a data entry. Such access called tailgating in a logical access is a very serious issue in information security and is the cause for most of the cyber-crimes involving data theft, data diddling and data manipulation.



Answers by **Rajendran V**

Some Interesting Quotes/ Cartoons

This may look funny, but it carries lots of messages. Thanks to the Internet.

Despite all logic telling me otherwise, some part of me still believes that clicking the link again will make it load faster.

If your password is your name...you deserve to be hacked.

Shutting down the computer and then realizing you need it again...

Some tips to be cautious with ATMs: Courtesy **Kumkumam**, Tamil weekly.

- Please do not keep the ATM card and corresponding PIN together. Possibly remember the PIN and do not have it in a paper or so.
- In case, if any third party assistance, including the bank officials, is sought for using ATMs, please change the PIN immediately.
- While entering the PIN please cover the keyboard of the ATM with your full body.
- After the completion of the transaction, please ensure that the cancel button is pressed.
- If the cash is not dispensed by the ATM, but your account is debited, please contact the call center or the nearest branch immediately. Please



remember the complaint number given. As per the extant rules the Bank has to arrange for re-crediting the amount within seven days. Else for each day of delay, the Bank has to pay ₹ 100/- as penalty. However, this rule is applicable only if the customer informs the bank within 30 days of the incident.

- Unless it is absolutely necessary, please avoid using the ATM during nights.
- If any sticky objects are seen in the slot while inserting the ATM card or if any suspicious wires are connected please avoid using the ATM and inform the concerned.

e-Commerce - FAQs

Q My Company carries on entire business correspondence and transactions through internet. Is it proper? What precautions should I take?

A There is absolute legal recognition for carrying on business through internet. Before starting correspondence, agree upon the e mail id / website or any other mode of electronic exchange of data and payments.

Some companies do not give their addresses in their websites. Get to know the physical address, telephone numbers of the principal place of business before starting actual transactions.

Do not just start corresponding to an id based on a business card or a letterhead lying with you for a long time. Verify with the party once again.

Have a regular backup of important data.

Q Are there any rules regarding attribution of electronic mails?

A. The IT Act does not impose the use of any particular procedure with regard to sending and receiving electronic data or with regard to acknowledgement and attribution of data. The Law acts only as a guideline. The parties are free to agree upon terms and conditions with regard to mode and use of electronic contracts. The Indian Contract Act applies to electronic contracts also. The popular term 'offer and acceptance' is the essence of any contract. It would be wise to mutually agree upon all aspects with regard to electronic data exchange. The IT Act applies only when there are no prior agreed terms between parties.

Q A person sells goods online. I would like to buy them. On enquiry I got a mail that there is no registered office. How do I proceed?

A. You may proceed after getting the address of his residence which will be deemed to be the place of his business.



Compiled by Ms. **Padma R.**



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