eSecure

Secure and be Aware !

An e-zine from CySI

[Volume 1, Number 2]
November 2013

Editorial Board

This Issue

*****

CySI feels proud to inform all the that one of the Executive Committee Members and the Chief Editor of this ezine **Mr. Ramamurthy N,** has been awarded Ph.D. degree from University of Madras for his thesis titled "**Information Technology and Samskrit**".

Let us all join together in congratulating and wishing him all the very best in such endeavours in future.

Congrats **Dr. Ramamurthy N**

Presidential Address

Dear Readers

Mr. Rajendran V.

Basically a banker, now turned an advocate especially in cyber-crimes and banking technology, Guest Faculty and invited speaker in many Universities, colleges and Staff Training Centres of banks, Police Academies, etc., on Cyber Laws, Frauds in ATMs, Internet Banking etc., and Cyber Crimes and information security. Authored a book on IT Security published by Indian Institute of Banking and Finance and publishes articles.

It gives me immense pleasure to present the second issue of our ezine. After the release of the first issue, so much has happened. A wonderful workshop in Chennai on 9th November 2013, with the Hon'ble Dr. Justice Jyothimani (formerly Madras High Court and at present National Green Tribunal), the popular Lok Sabha M.P. Shri S.S. Ramasubbu and Dr C. Chellappan, Dean of Anna University were all part of the inauguration. It was a daylong event with very active participation from members, the speakers sharing their experiences and the participants glued to their seats posing questions till late in the evening, a little after 6 PM. After all, thirst for knowledge and enthusiasm defies fatigue.

Again, on the evening of 21st November 2013, the President and CEO of the Internet Security Alliance USA, Shri Larry Clinton is addressing CySI members and other selected guests and visitors. This meeting is certainly going to be a very informative one with lots of interactions.

I have received very encouraging and motivating feedback from the readers for our first issue. Many readers have requested us to share the latest in cyber-crimes and discuss the latest trends or any novel modus operandi in such crimes. Needless to say, crimes are as old as human beings. Crime and punishments have been spoken about in all ancient epics and mythological stories. And cyber-crimes are just electronic variants of age-old physical crimes, with some difference like the way they are committed, dependence on electronic gadgets and most often evidence lying in such gadgets serving as a tool in the act of crimes. This issue carries an interesting feature on electronic footprinting, i.e., one aspect of digital evidence and other interesting feature stories.

Let me take this opportunity to congratulate our Editor and EC Member Shri N Ramamurthy, on his successful completion of a doctorate from Madras University. Now we have a doctor to edit, compile and present. Hope you will like it. Please feel free to express your feedback. Criticisms and scope for improvement, please express at once.

Best wishes

Rajendran V

*****

Editor's Column

Dr. Ramamurthy N

Chief Editor of this magazine and active Executive **Committee Member** of CySI

Ramamurthy, is a versatile personality with unique blend of experience in various walks of Banking and related IT solutions. His specialty is continuous learning. His qualifications include – M.Sc., B.G.L., CISA, PMP, CGBL, Black Belt in Six-sigma and so on. Recently he was awarded with Ph.D. degree by the University of Madras for his thesis titled "Information Technology and Samskrit". He spreads his knowledge through consulting and teaching.

He has so far published nine books and seven books are in print. Some more books are in the pipe line. These books relate to religion, IT and Banking. He takes active role in religious activities in addition to IT security. Banking related roles.

Secure your Credit/ Debit/ ATM Card Transactions

Card fraud is a wide-ranging term for theft and fraud committed using a credit/ debit/ ATM card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Card fraud is also an adjunct to identity theft.

To have a secure transaction using our Credit/ Debit/ ATM cards, it is proposed to give an overview of the security features in a card, how fraud happens and how to prevent. This may be through a series of articles. Courtesy – Business Today and Mastercard.

Magnetic Strip - The film stripe on the back of a Card stores account information. The magnetic stripe does not contain personal information such as date of birth or mother's maiden name, etc.

Tamper-evident Signature Panel - The signature panel on the back of a Card helps guard against card fraud.

Personal Identification Number - As part of the card fraud protection, cardholders should choose their PIN which protects the transactions.

Card Verification/ Validation Code - The three-digit code indent printed on the signature panel of a Card enables business establishments to ensure that the cardholder has possession of the card during a phone or online transaction.

Hologram - A three-dimensional image with interlocking globes reflects light and appears to move when the card is rotated.

SecureCode - For an added layer of card fraud protection, cardholders should create a unique personal code known only to the cardholder and the issuing bank. This code is requested during the checkout process at participating online stores verifying the purchaser is indeed the cardholder. Cardholders can make purchases quickly and conveniently with a simple tap, rather than swiping or dipping their card. This adds a level of security since the card never leaves the cardholder's hand.

If fraud or a security compromise is suspected on a Card account, issuing bank works with the payment gateway and monitors the account for unusual activity and to notify the cardholder. Attacks on an account can range from the crude to the sophisticated and they can come at any point of time.

We will continue with some tips to secure our cards.

*****

Are You Cyber Monday Ready?

Dr. Ramamurthy N

What Is Cyber Monday?

Close on the heels of Black Friday (the largest shopping day in the U.S.), Cyber Monday is considered the biggest online shopping day of the year and it lands on Monday, December 2nd this year. Cyber Monday's popularity increased so much in recent years that many businesses have decided to extend it into Cyber Week by offering deals, events, and promotions for at least 5 full business days.

Tips to Get Ready for Cyber Monday

- Determine your message by differentiating yourself from the crowd. Consider your unique value proposition (what makes your offer honestly the best) and how you can present it in an engaging, personable way to your audience.
- Spread the word by considering how you will inform your current and prospective audience, such as emails, blogs, tweets, social media updates, pins, etc.
- Do not SPAM your audience. Find balance by ensuring you're providing quality, relevant, and valuable information that is welcome.
- Be smart and specific about your word choice. For example, "great deals" or "holiday sale" may not have as much impact as "Cyber Monday Deals," "Cyber Monday Specials," or "Cyber Week Deals."
- Use eye-catching, attractive titles to pull readers in and avoid gimmicky titles like "Don't Miss Your Chance!" or "You'll Wish You Didn't Miss This Opportunity!"
- Check, double check, and triple check to ensure you have a great call-to-action that clearly compels your visitor to act.
- Track your data using your goals as a guide. Knowing article views, bounce rates, social media engagement stats, peak traffic times, audience demographics, and more can help you measure your success and tweak your strategy for next year.

Some notable Cyber Monday Articles

- **Planning Your Editorial Calendar for the Holidays**
  The holidays can be overwhelming. Alleviate stress and avoid forgetting timely holiday articles by getting ready for December with an Editorial Calendar. Consider what your audience is celebrating, how you can break down each week into themes, and when you will launch.
- **Top 7 Article Templates to Get Ready for Cyber Monday**
  Need last-minute article ideas? Build your article portfolio in time for Cyber Monday and the holidays with these 7 article templates that are tailored to please any audience looking for information on the best products, DIY steps, tips, checklists and more.
- **Top 7 Tips to Social Media Holiday Buzz**
  Buzz is everything during the holiday season. Manage writing articles, creating social media buzz, and everything else by finding balance with these 7 tips to share your relevant articles, your seasonal side, nostalgia, seasonal information, promotions, and more.

Courtesy: http://blog.ezinearticles.com/2013/11/are-you-cyber-monday-ready-2.html

*****

Newest News

Ms. Panchi S.

Panchi has sixteen years of experience in Information technology. She possesses an M.Tech, M.Sc., CAIIB and PG cert in Cyber Law. She is also a CISA certified professional. She has also presented research papers in Indian Institute of Banking and Finance and won prizes. To her credit are some articles and publications in various magazines.

Singapore Prime Minister's Website hacked

The official website of the prime minister's office of Singapore was hacked in the first week of November by apparent members of international hacker group. The attack came after Prime Minister Lee Hsien Loong vowed to hunt down culprits who launched cyber-attacks on Singapore, reported Xinhua. One of the sub page of the prime minister's office website was reported to be compromised". "A vulnerability in that sub-page was exploited to display pages from other sources. This vulnerability is known as cross-site scripting," it said. The sub-page of the website once showed a mocking headline "It's great to be Singaporean today" next to a Guy Fawkes mask, a symbol of anti-establishment defiance. This was a CSS Attack that happened on the Prime minister's website.

What is CSS Attack?

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls. 84% of the total attacks happenings in websites are Cross-site scripting attacks.

Youth arrested for making fake Facebook profile of woman

Cyberabad Police have arrested a youth from Bangalore on the charge of creating fake profile of a city-based woman on Facebook and threatening her for rejecting his love proposal. The youth besides creating the fake profile of the woman and uploading her photographs on Facebook, was chatting in her name with others. According to the police, he also made calls and sent messages to the victim and her family members threatening them with dire consequences for rejecting his love proposal. He seems to have even threatened her and her family members with dire consequences saying they should not look for other matches for her. This is a form of Cyber stalking.

What is CyberStalking?

Cyberstalking is the use of the Internet to stalk or harass an individual, a group of individuals, or an organization. It may include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, or gathering information that may be used to harass.

A cyberstalker may be an online stranger or a person whom the target knows. A cyberstalker may be anonymous and may solicit involvement of other people online who do not even know the target.

Cyber Lingo - Smurf attack

If a ping request is given to a complete network, say, 10.0.0.0, then it is a smurf attack. It is a type of DoS (Denial of Service) attack

Days & Dates

November 10 – World Science day for Peace and development

Established by UNESCO in 2001, World Science Day for Peace and Development is celebrated worldwide on 10 November each year. It offers an opportunity to demonstrate to the wider public why science is relevant to their daily lives and to engage them in debate on related issues.

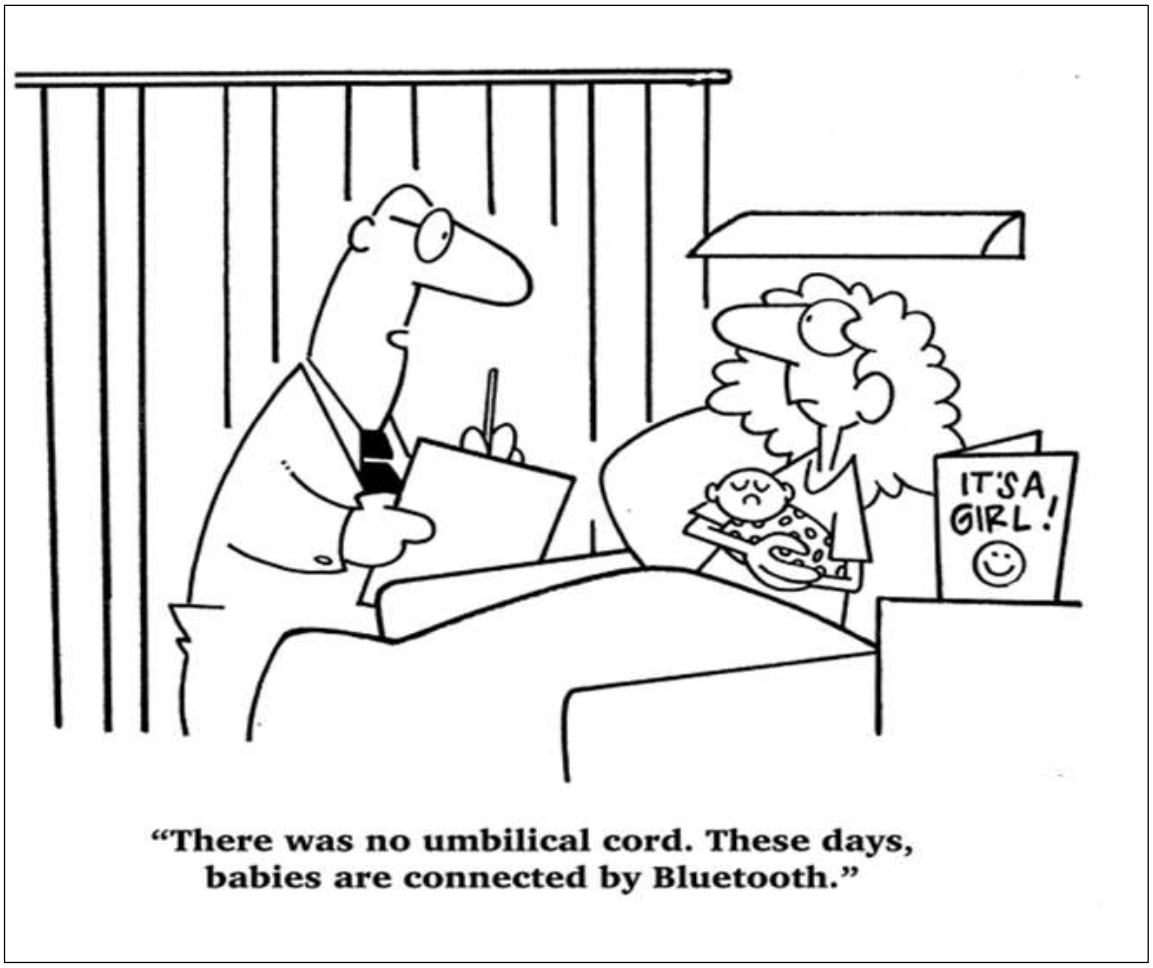
*****

Some Interesting Quotes/ Cartoons

Ramamurthy N

These may look like funny. But they carry lots of messages. Thanks to the Internet.

Technology Advancement!!!!!



Target Footprinting and the Cyber Laws

The collection of data by an attacker about the target's technology framework in order to access or secure access to the computer system is termed Target Footprinting (FP). This is the first step taken before committing the crime of gaining unlawful access to various websites, systems, networks, communication device, storage device, or for committing any other offence related to cyber space. It is estimated that 90% of an attacker's time is spent on footprinting activities!

What is FP? Just as in any conventional crime, say a theft, the criminal

first plans and gathers information on his target – gathers info on location of the building, looks for possible entrances, vulnerable time, exact location of the safe, availability of keys, tools to break open and finally look for exit zones and then proceeds to commit the offence. In a conventional crime, the attacker, in almost all cases is physically present at the site. A cyber-crime also takes place in the same way but with different tools and techniques often committed from a remote place away from the target location.

A sturdy definition of cyber-crime is an unlawful activity where computer is a tool, a target or both. The definition of 'computer' is exhaustive in law. In a cyber-crime it is impossible to attack blindly. Many times the attacker needs to be proficient in computer technology and may also need assistance of experts in various spheres of software & hardware technology and in the field of computer networking. In the absence of up-to-date technical support, not only the attempt fails, but also the attacker gets into risk of being exposed. This seems to be the major contrast to conventional crimes where it is sufficient, if only the attacker is a muscle man.

Sometimes, the target itself is selected through FP. A person would never let know in public his name, residing place or family details, but would never hesitate to even pass across several seats in his office or in public places important info on his network, mail ids or even passwords . We see this state even among bank employees.

We shall discuss on sources, methods & tools of FP and its implications, how criminal liability arises and the applicability of Cyber Law on the subject in the second part of the article in the next issue.

*****

Ms. Padma R.

Padma is a graduate in Arts with Psychology as one of the majors from Bangalore University. She later graduated in Law from Bangalore University. She has an experience of practice in Civil courts for 12 years.

She is now the CEO of a Small Scale Industry in Coimbatore. She has to her credit a Diploma in Cyber Laws, a PG Programme in Information Technology Act and a PG Programme in Cyber Crimes Prosecution and Defense. She has a keen interest in pursuing education. She is an active member of CySI.

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.