Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)

CCAOI

Security Newsletter **30th September, 2010**

As internet is becoming an integral part of our lives, it is important that we are aware of the threats we face in the Cyberspace. The need of the hour is to be aware and adequately equipped to protect ourselves online.

Keeping this in view, with the support of ***Indian Computer Emergency Response Team (Certin), Department of Information Technology, VeriSign India and Sify Technologies Ltd.*** *we are releasing the third edition of our* ***fortnightly Security Newsletter.***

Role of Educators and Online Child Protection

As a medium, internet provides easy access to all kind of sites and information and the curious nature of children draws them to it. COP reports 90% of teens and young adults. Though the potential about the beneficial part of internet is undisputed, yet in recent times it has also raised new and disturbing issues, of online abuse.

Despite all this many countries have no clear cut laws to protect the children, educators and parents are unaware of this danger. The need of the hour is to educate not only these vulnerable youngsters on how they can protect themselves online but also the parents and educators.

As children spend a large portion of their time in school, the school authorities and educators can play a major role in protecting and educating them against internet abuse. Parents on their part too, expect the school authorities to protect and provide their children with adequate knowledge.

School authorities should expand their professional understanding of the problem of the online dangers for youngsters; develop the ability to recognize the indicators of abuse and deal with prevention and support activities within the school and community.

The role of the school in sharing information with other professionals and providing support for the child and family is very important. School-based activities and school-community partnership programs for preventing abuse and neglect should be an ongoing process.

Today it is important for teachers to understand the tremendous opportunities and challenges this medium offer and educate their students accordingly.

To prevent and reduce the occurrence of online child abuse, educational institutes could adhere to the following best practices:

- The teachers in educational Institutes should be technology savvy.
- Each Institute should have a Internet literacy curriculum which includes topics like :
  - Cyber Safety – How to recognize and avoid sexual solicitation, child predators and other sexual risks
  - Cyber Security – How to recognize and avoid identity theft and Internet fraud
- Cyber Citizenship – How to be a responsible cyber citizen
- Each school hold regular discussions and interaction with students on safety over internet, fostering a sense of openness for children to speak out
- Each school should have a cell to help students who have become a victim of online abuse.

Critical Internet Security Technology

An important Internet security technology that has been more than a decade in the making is now live and protecting users, thanks to the concerted efforts of Internet stakeholders and critical infrastructure providers. In July, VeriSign joined with U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN) to deploy DNS Security Extensions (DNSSEC) at the root of the DNS.

Properly implemented, DNSSEC protects users against a particularly dangerous threat known as “DNS cache poisoning,” or more commonly, a “man-in-the-middle” attack, by allowing DNS traffic to be cryptographically signed. Because the root-server-system lies at the heart of the DNS, implementing DNSSEC at the root level provides a critical anchor to support DNSSEC deployments further out in the network. So while a handful of individual domains were DNSSEC-enabled prior to July, the signing of the root marks the real start of the DNSSEC era on the Internet.

That era may be starting just in time, according to a recent study, which found that businesses are experiencing a growing number of DNS-based attacks and are investing more time and resources in protecting their critical infrastructure.

In DNSSEC Ready for Prime Time, a Forrester white paper commissioned by VeriSign, researchers found that DNS-based attacks are now commonplace and that while DNSSEC may not yet be widely understood, the majority of business IT leaders who do know about it plan to deploy the technology on their networks.

The study, which polled 297 IT decision-makers, revealed that DNS Security is a top-line concern for companies and organizations as they work to protect their assets and networks from attacks. A vast majority of respondents (88 percent) said that they were either already allocating budget for DNS security measures or would do so in the near future. That widespread commitment to DNS security probably has a lot to do with the prevalence of DNS-related attacks, which 51 percent of respondents reported experiencing.

Of those who had experienced DNS-based attacks, 38 percent said that they had experienced man-in-the-middle attacks, which DNSSEC is specifically intended to prevent. While man-in-the-middle attacks were not the most common attacks reported by IT leaders, they were associated with the most significant financial losses.

With so many factors pointing towards the need for widespread DNSSEC adoption, one of the greatest obstacles lies in building awareness of the technology and its value.

Secure Cybercafé - with Sify mylife

The government and other regulatory bodies have started taking strict measures to control cyber crime and anti social activities from cyber cafes. Sify as a corporate also feels responsible to contribute to the cause of social security and have therefore developed a unique and effective solution for cyber cafés – **Sify mylife**.

The key highlight of Sify mylife is the Know Your Customer (KYC) platform - a proven cyber security and customer database management tool which enables you to comply with all cyber security norms and keeps you geared for any regulatory or user-information demands from government/ regulatory bodies.

Know Your Customer equips you with the following features:

- **Customer Registration**:
  Every customer will be required to do a one-time registration in your cyber café and share the required details as per the KYC standard - name, address, mobile number, photograph and photo Id proof. The data will be stored in the sify cloud for all future reference and records.

- **User Id and Password**:

Every customer will be provided a unique User Id and password to access the Internet and any other related services on sify mylife. This will also allow you to track all transactions made by each customer at your cyber café.

- **Usage session capture**:
  KYC provides Customer Authentication and Session Details Capture and Storage during each and every access. All the customer data is stored in the Sify servers, thus addressing your worries of storing data in a local PC.

- **All India single log in**:
  A customer can walk into any Sify powered cyber café and use his/ her unique User Id and password to access services. However, balance transfer and usage will not be allowed between different cyber cafés.

- **Server based solution:**
  Unlike in the case of other cyber security solutions, in sify mylife all your customer and cafe data is stored on Sify servers with multiple redundancies built in to ensure data safety and security. This means that even if your PC hard-disc crashes, your data will be safe and can be furnished whenever demanded by the police/ regulatory bodies.

In addition to a robust KYC platform, Sify Mylife also empowers you to offer a host of value added services to your customers at your cyber café – they can book travel tickets, pay utility bills (electricity, taxes, insurance premiums etc.), recharge mobile and DTH, use personal banking services, access educational content, make economical ISD calls, take online examinations and do a lot more at your cyber café.

Cyber Café Association of India (CCAOI), 258 Okhla Industrial Estate, Okhla Phase III, New Delhi – 110020.
Visit us online at: www.ccaoi.in
For any comments/suggestions email: info@ccaoi.in