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

CCAOI
Cyber Cafe Association of India

Security Newsletter   20ᵗʰ August, 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. According to **Indian Computer Emergency Response Team (CERT-In),** *3,089 Indian websites with domain ".in" were hacked and defaced in 2009 as compared to 2,642 websites in 2008 — a significant rise of 17 per cent. In 2007, 1,693 websites with ".in" domain were defaced.*

A few days back the office of NSA was attacked on the same day when Google and other finance and US defence establishments reported attack from hackers in China. Our former national security adviser (NSA), Mr. M.K. Narayanan, had said a few days back that the Chinese hackers had tried to penetrate computers of his office.

Thus, 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 launching a* **fortnightly Security Newsletter.**

We are thankful to Dr Gulshan Rai, DG Certin without whose encouragement and support this newsletter would not have been possible.

"We are concerned about the security of our online users and we welcome such initiatives to inculcate Safe Surfing amongst all the internet users in the country both young and old" says Dr. Rai.

Realising the Benefits of Online Security

Despite targeted education efforts by banks and online retailers alerting customers not to share their personal information online, internet users globally continue to fall victim to phishing attacks. Criminals worldwide are constantly developing new scams to trap the internet-savvy who won't fall for the old "click here to verify your account" email scam. Today, phishing scams are becoming more sophisticated, and e-criminals continue to develop scams targeting the most vulnerable.

A recent research conducted by VeriSign revealed that scare tactics by fraudsters remain an effective form of phishing through sneaky strategies such as imitation websites trying to phish personal details. This strategy is one that has shown to work successfully (to the detriment of consumers) across all demographics[1].

Rather than asking, "How do I stop internet crime?" businesses today need to ask, "How do I stop internet crime affecting my business?" The first step towards this is to understand the kind of security measures and warning signs businesses and their customers increasingly need to look for online.

VeriSign®

sify ■ keeping you ahead

---

[1] The online survey was commissioned by VeriSign and conducted by YouGov on 21-27 May, 2009. The survey asked more than 8,000 respondents across nine countries to "spot the difference" between real and fake Web sites from VeriSign's recently launched the Phish or no Phish (www.phish-no-phish.com) challenge.

VeriSign, the trusted provider of Internet infrastructure services for the networked world, has compiled a list of key security tips to help businesses plan their own security strategy:

1) **Visual cues:** Consumers need to protect themselves from "phishing sites" which are fake websites set up by criminals to steal personal information. Simple visual cues can demonstrate that your site is safe and open for business, such as the "https" in the URL address or the green address bar in the Web browser. These cues tell customers that a website owner has invested in digital certificates which verify that a site is legitimate and that the customer information will be encrypted during transactions.

2) **Too much information:** Phishing sites frequently lure consumers through "urgent" e-mail alerts and then request personal information organizations should already have or information they clearly do not need for account activity. These messages alert customers to account problems, account status changes, special sales offers or even the need for special security software downloads. These messages also include links to fake websites in order to get customers to input personal information

   Retailer sites generally do not need more than a name, shipping address, billing address, credit card type, card number and expiration date. Consumers should become suspicious whenever social security numbers or bank routing numbers are requested for. Retailers do not need to execute customer downloads to upgrade site security. As a business rule, you should only collect what you need for the purpose of the transaction at hand.

3) **Two-factor authentication:** Online businesses are increasingly using "two-factor" authentication to provide access to end users' accounts. This combines something the consumer knows, such as a username and password, with something the consumer has, such as a unique one-time security code. This code is typically generated by a small plastic token, credit card-shaped smart card, or SMS-enabled mobile device. Two-factor-protected sites require both the username and password combination coupled with the one-time code, the theft of one will be useless without the other.

4) **Checking in:** Customers should have readily accessible ways to raise security concerns with an online retailer. Online businesses should make phone numbers, instant messaging attendants or feedback forms easily accessible. Concerned queries from customers should be addressed in a time-sensitive manner.

5) **Checking out:** Given that checkout is when online deals are completed, it is very important to use that interaction to nurture trust. Most well-run websites—such as Amazon or eBay—send printable order and shipping confirmation e-mails. These features assure customers that someone is watching out for them throughout the transaction.

6) **Education:** Finally, businesses should take on the responsibility of educating their customers on what to look for as they transact online. This takes online security beyond the measures you put in place and builds trusted relationship between merchants and consumers that will pay dividends far beyond today's purchases.

   Businesses need to earn their online customers' trust and confidence to be successful, especially in tough economic times when consumers are jittery and competitors are just a click away.

   Many businesses today are enjoying increased customer confidence and great online sales results by implementing a security solution called Extended Validation (EV) SSL Certificates. These certificates provide an easy and reliable way to verify that a website is authentic and provides a secure environment for users conducting transactions. EV SSL Certificates provide immediate visual cues to web users using the latest web browsers that currently support EV SSL. The address bar turns green, a padlock icon appears next to the address and a new field displays to the right of the URL in the browser. This field contains the name of the organization that owns the site as well as the security provider that issued the certificate, such as VeriSign.