CCAOI™

Representing the ecosystem of Internet -Bharat Model

CCAOI Newsletter **June, 2012**

India Inc lines up seeking custom web addresses

With internet addresses being opened up to whatever you want it to be and not just plain old .com, several large Indian corporations are seeking custom web addresses such as .tata, .infosys or .reliance.

First phase of the fight for internet's new prime real estate came to an end on Thursday when internet's administrative body Internet Corporation for Assigned Names and Numbers (ICANN) shut down the application window for registering new generic extensions - say .bank or .mumbai. Names applied for will be revealed on June 13.

Applications for these names can only be made by internet domain name registrars accredited by ICANN. One such registrar, Directi.com - India's largest domain seller company - has invested $30 million in this new gold rush and has applied for such extensions as .Web, .Bank, .Online, .Hotel, .Music, .Loan and .News.

Such extensions are expected to be highly sought after by corporations operating financial services or media, entertainment and hospitality sectors. At least 25 large Indian corporations have applied for custom brand extensions, according to some ICANN accredited registrars from India that ET spoke to.

"This is once-in-a-lifetime opportunity that will change the way we use internet. It is not going to be available again. We have invested about $30 million and applied for 31 strings which we think can house attractive businesses in coming years," said Bhavin Turakhia, 32, chief executive at Directi.

Delhi-based Net4, an ICANN approved registrar, has applied on behalf of 17 large Indian corporates, who want to own their brand just like a .tata or .reliance.

"These are large corporations with market cap of at least Rs 25,000 crore. We can't disclose names due to non-disclosure agreements. Some of the corporate are also interested in making a business model out of their brand extensions," said Jasjit Sawhney, chairman and managing director of Net4.

Each application to ICANN costs about $1,85,000, in addition to $2,50,000 to be given as bank guarantees that a company can sustain the domain over next three years. So far, ICANN has reportedly made over $350 million in fees for applications filed.

Industry watchers also say that many small companies are applying in anticipation of the profit-making opportunity, much like cyber squatters of the 1990s, when individuals and firms would register unused domain names - celebrities, or brand names - that may be in demand in future.

"There is a likelihood of serious contenders for .Music or .Hotel domains. Large corporations may try to wipe out competition by offering generous amounts to smaller companies who may want to exit after making a profit," adds Sawhney.

For applicants it's a sunk cost if they get rejected, lose in the auction process, or don't make money on arbitrage, by December, this year.

Ditrecti's Turakhia is floating a new subsidiary Radix for the application process. In the race to acquire prime domains, he would be locking horns with the likes of the American Banking Association, which is in contention for the .Bank domain extension.

Source: Economic Times

World IPv6 Launch Unites Industry Leaders to Redefine the Global Internet

As leading websites, ISPs, and home router equipment manufacturers support IPv6 by default, it becomes the new normal for the Internet

To ensure the Internet can continue to grow and connect billions more people and devices around the world, thousands of companies and millions of websites have now permanently enabled the next generation of Internet Protocol (IPv6) for their products and services. Participants in World IPv6 Launch include the four most visited websites in the world – Google, Facebook, YouTube, and Yahoo! – as well as home router manufacturers and Internet Service Providers in more than 100 countries. By making IPv6 the “new normal,” these companies are enabling millions of end users to enjoy its benefits without having to do anything themselves.

World IPv6 Launch is organized by the Internet Society as part of its mission to ensure that the Internet remains open and accessible for everyone – including the other five billion people not yet connected to the Internet. "The support of IPv6 from these thousands of organizations delivers a critical message to the world: IPv6 is not just a 'nice to have'; it is ready for business today and will very soon be a 'must have,'" said Leslie Daigle, Chief Internet Technology Officer, Internet Society. "We believe that the commitment of these companies to deploy IPv6 will ensure that they remain industry leaders. Any company wishing to be effective in the new Internet should do the same."

The World IPv6 Day in 2011 was a 24-hour test that focused on websites. This year, World IPv6 Launch is a permanent commitment across the Internet industry, including ISPs and home networking equipment manufacturers around the world, laying the foundation to accelerate the deployment of IPv6 across the global Internet. Major websites are permanently enabling IPv6 starting 6 June 2012 at 0000 UTC on their main websites. ISPs will permanently enable IPv6 across a significant portion of their current and all new residential wireline subscribers. Home networking equipment manufacturers will enable IPv6 by default through their range of home router products, and recent commitments to IPv6 by companies beyond websites demonstrates a broader support of the new Internet Protocol.

This is imperative as the last blocks of the 4.3 billion IP addresses enabled by the current Internet Protocol (IPv4) were assigned to the Regional Internet Registries in February 2011. Already there is no remaining IPv4 address space to be distributed in the Asia Pacific region, and very soon the rest of the globe will follow. IPv4 address space is expected to run out in Europe this year, in the U.S. next year, and in Latin America and Africa in 2014. IPv6 provides more than 340 trillion, trillion, trillion addresses (an essentially unlimited number), which will help connect the billions of people that are not connected today, allow a wide range of devices to connect directly with one another, and help ensure the Internet can continue its current growth rate indefinitely.

For more information about World IPv6 Launch and the participating companies, as well as links to useful information for users and how other companies can participate in the continued deployment of IPv6, visit: http://www.worldipv6launch.org

Source: ISOC

E-ticket cancellations bring the railway department whooping 750 crore revenue

Reports reveal that e ticket cancellation is major source revenue for the Railway department, fetching them an annual sum of Rs. 750 crore, in between the period of 2005-2011. In addition this, the government earned Rs 30,094 crore from e-tickets from 2005 to April 2012.

In 2011, between March and December, the railways earned Rs 198 crore from cancellation charges of e-tickets. Ever since it began in 2005, e-ticketing has ballooned to make up about 40% of all rail ticket sales. Railway officials say that the convenience that booking and cancelling an e-ticket offers has seen more passengers making advance bookings that very often result in cancellations. In fact, one out of every three e-tickets sold is cancelled.

If a confirmed ticket is cancelled more than 24 hours before the scheduled departure of the train, the penalty is Rs 70 for an AC first-class ticket, Rs 60 for AC Tier-2, AC Tier-3 and AC chair car, Rs 40 for sleeper class and Rs 20 for a second-class ticket. In fact, even if a wait-listed ticket is not confirmed, the Railways go on to deduct Rs 20 before refunding the remaining sum.

Popular trains have long waiting lists of 700 or 800. Almost 95% of the wait-listed tickets do not get confirmed and therefore are automatically cancelled. What ordinarily happens is that most passengers book themselves on more than one train, others with flexible travel dates book tickets on different days if they are on the waiting list.

Source: eGov Online

Online filing of Income tax will be free from offline bit

From this year, those who prefer to file their income tax online might be freed from the rigmarole of the offline process, where you need to take a printout of what is called the ITR-V form, sign it, and mail it to the I-T department's centralized processing centre (CPC) in Bangalore.

According to sources, the law and information technology ministries were examining the matter, and a solution was likely to emerge soon. However, it is not quite clear though if the new system would be in place by June-July , when the bulk of individual filings happen.

In the last fiscal, 1.65 crore returns were filed online, but ITR-V forms of as many as 25 lakh people were not received by the CPC. Many forget to send the forms in the stipulated 120 days; in some cases, these get lost in the post.

The I-T authorities need to be absolutely certain about the identity of the person filing the form, which is why it currently mandates a physical signature. A digital signature is an option, but you need to pay to obtain a digital signature for yourself and that is not something everyone would want to do.

So the I-T department is looking at the option of what is called an electronic signature, where your identity is verified online through different ways, including a PIN that can be sent to one of your previously specified devices and which you can use to authenticate yourself.

Ever since CPC was established in 2009, online filing has seen a surge. The initiative is a collaboration of the I-T department with Infosys Technologies and TCS. TCS handles the frontend e-filing process, while Infosys handles the backend processing.

Source: eGov Online

Industry News

Google Chrome Just Passed Internet Explorer To Become The World's Most Popular Web Browser

After months of chipping away at its lead, Google Chrome has finally overtaken Internet Explorer to become most popular web browser worldwide.

Chrome's share of the market rose to 32.8% in the week ending May 20, while Internet Explorer's share of the market dropped to 31.9%, according to new data from StatCounter, via TheNextWeb. This marks the first full week that Chrome has beaten Explorer.

Google's browser had previously topped Explorer for a single day back in March.

Mozilla's Firefox is the third most popular browser with just more than a 25% of the market.

Source wwwbusinessinsider.com

Internet Security News

India readies firewall to fight cyber attacks
Govt To Deploy Agencies For Counter-Offensives

India is set to take steps to protect its cyber infrastructure and designate agencies for carrying out offensive cyber attacks on other countries. The move comes at a time when proof shows countries launching cyber attacks — not only for intelligence gathering — and many nations describing the attacks as an act of war.

According to sources, the National Security Council NSC) headed by Prime Minister Manmohan Singh would soon approve the comprehensive plan and designate the Defence Intelligence Agency (DIA) and National Technical Research Organization (NTRO) as agencies for carrying out offensive cyber operations, if necessary. All other intelligence agencies would be authorized to carry out intelligence gathering abroad, but not offensive operations, sources said.

The detailed policy for national cyber infrastructure protection is presently before the NSC awaiting its approval. The policy would identify all government agencies that would have a role in the protection of Indian cyber infrastructure and define their roles.

The move to not just define defensive mechanism but also designate agencies for offensive operations comes as New Delhi tackles repeated waves of cyber intrusions, though all of them are aimed at gathering information from critical networks. But the next stage, of an adversary carrying out offensive cyber attack, of bringing down a power grid, stalling air traffic control systems, or manipulating controls of a dam are now believed to be a real possibility.

Stuxnet, the cyber worm created by US's National Security Agency and Israeli military and specifically targeted at Iran's nuclear enrichment center at Natanz, was found to have infected Indian systems. "It was probably unintentional, but an intentional attack on India's critical infrastructure cannot be ruled out," says a senior official. "We haven't yet seen a cyber attack, but only intelligence gathering. An attack that can debilitate our infrastructure is what we must be prepared for," he said.

CERT-IN (Computer Emergency Response Team India) would be responsible for protection of most of the cyber space, while NTRO would be tasked to protect the critical infrastructure such as important government networks. NTRO would be tasked to create the National Critical Information Infrastructure Protection Centre (NCIPC), which would be a commandand-control centre for monitoring the critical infrastructure. It would be a round-theclock centre, providing real time response to cyber security breaches.

The proposal before NSC also envisages creation of sectoral CERTs in order to respond quickly to protect power distribution networks, Air Traffic Controls, traffic networks and other areas that heavily dependent on networked systems, and thus are susceptible to attacks.

The policy suggests that the defence forces would be responsible for their own networks' protection.

NTRO and Intelligence Bureau (IB) would primarily be responsible for security of various government networks. While NTRO would operate through NCIPC, IB would be mainly looking at the physical security of networks. State polices, CBI, NIA etc would be tasked to do follow up action, if any intrusions are detected.

Source : TNN

Kaspersky Lab has announced the discovery of a highly sophisticated malicious program that is actively being used as a cyber weapon attacking entities in several countries. The complexity and functionality of the newly discovered malicious program exceed those of all other cyber menaces known to date.

The malware was discovered by Kaspersky Lab's experts during an investigation prompted by the International Telecommunication Union (ITU). The malicious program, detected as Worm.Win32.Flame by Kaspersky Lab's security products, is designed to carry out cyber espionage.

Eugene Kaspersky, CEO & Co-Founder, Kaspersky Lab, said, "The risk of cyber warfare has been one of the most serious topics in the field of information security for several years now. Stuxnet and Duqu belonged to a single chain of attacks, which raised cyberwar-related concerns worldwide. The Flame malware looks to be another phase in this war, and it is important to understand that such cyber weapons can easily be used against any country. Unlike with conventional warfare, the more developed countries are actually the most vulnerable in this case."

Alexander Gostev, Chief Security Expert, Kaspersky Lab, said, "The preliminary findings of the research, conducted upon an urgent request from ITU, confirm the highly targeted nature of this malicious program. One of the most alarming facts is that the Flame cyber-attack campaign is currently in its active phase, and its operator is consistently surveilling infected systems, collecting information and targeting new systems to accomplish its unknown goals."

Source: VAR India

Hacking: Experts call for code
Say It's Never Ethical In Law; Unregulated Courses A Threat

Cooking, sketching, horse riding, swimming — there is no dearth of skills that one can pick up in handy, bite-sized courses during summer. Now you can add computer hacking to that list.

Advertised as 'ethical hacking', the courses claim to teach you how to hack passwords and social networking accounts — all to protect your system better, of course. But cyber lawyer Pavan Duggal says that under law, there is no such thing as 'ethical hacking' and institutes offering such courses need to be regulated.

Faridabad-based Brains Booster, which claims to have an IIM alumnus as faculty, offers an "exclusive" summer 'Hacking Course'. In its promotional pamphlet, the institute claims to teach how to "hack Facebook account in less than 1 minute" and even how to "run your virus when anyone opens your pen drive". Byte Code Cyber Securities in Delhi lists 'Yahoo Hacking and Google Hacking' and 'Wi-Fi Hacking' on their website as part of their 60-hour ethical hacking course. And Appin, with more than 100 centres nationwide, has a six-week course in 'information security and ethical hacking'. All these courses cost upwards of Rs 6,000.

The institutes maintain that they function within the purview of law. "Unless you know how hackers and viruses work, how will you protect your system?" argues Suvam Patwari of Brains Booster. Appin, which claims to have served Intelligence Bureau, makes the same point. "We are also in the

service trade. We handle cyber and data security for corporate offices as well," says Devendra Awasthi, centre manager at an Appin branch.

However, with a cyber criminal and an ethical hacker requiring similar skill sets, it pays to be careful about the laws. The additional DCP of the economic offences wing, S D Mishra, says the Delhi Police cyber crime cell has never received a complaint against such institutes. They have, however, made arrests in the past in cases that involved the hacking of bank websites.

Duggal points out that hacking is punishable under Section 66 of the IT Act, 2000, with three years' imprisonment and/or up to Rs 5 lakh fine. If a contaminant (virus) is created and released into a computer system or network, the victim can sue the hacker for damages up to Rs 15 crore per intervention.

Duggal says the courses exploit a loophole in the IT Act. "The IT Act has no provisions to penalize those who encourage various kinds of cybercrimes. There is no such thing as 'ethical hacking' under law. This needs to be regulated, otherwise these courses will keep mushrooming," he says.

Computer security expert Ankit Fadia recommends caution for aspirants. "It is impossible to hack into a Facebook account as quickly as these institutes claim. It's only a marketing ploy and the students will be disappointed. It is the responsibility of the training institute to teach from the perspective of data security rather than hacking a friend's Facebook account," says Fadia, author of 'The Unofficial Guide To Ethical Hacking' and 'How To Unblock Everything on the Internet'.

Protector or provocateur — the jury is still out on ethical hacking. But now you know what some folks are doing this summer.

Source: TNN