The Internet Corporation for Assigned Names and Numbers

ICANN

NEWS RELEASE

Brussels ♦ Sydney ♦ Washington ♦ Los Angeles

FOR IMMEDIATE RELEASE
July 28, 2010

Global Upgrade Makes Internet More Secure

Helps defend users against specific types of cyber crime

The security of the global Internet has been bolstered by a historic collaboration between government and the private sector. ICANN has joined the U.S. Department of Commerce and VeriSign Inc. to add security at the top of the domain name system – the technical infrastructure behind the Internet's "phone book" - to protect Internet users from certain forms of online fraud.

"A cyber criminal can steal your money or your personal data without you even knowing it. Cyber crime doesn't respect national boundaries," said Rod Beckstrom, President and CEO of ICANN. "This upgrade will help disrupt the plans of criminals around the world who hope to exploit this crucial part of the Internet infrastructure to steal from unsuspecting people."

With the Internet's pervasive role in daily life expanding rapidly, finding viable solutions to cyber crime is imperative. Deployment of Domain Name System Security Extensions, or DNSSEC, at the "root" of the Internet has laid the foundation for a new generation of innovative cyber security solutions by creating a global authentication platform - a common source of trust in the validity of Internet addresses.

Once fully deployed, DNSSEC will help prevent criminals from redirecting users to fake websites that can be used to perpetrate cyber crimes.

The domain name system is where all Internet addresses are stored, and the unique nature of those addresses is fundamental to ensuring that computers around the world can speak to each other. Working silently in the background, the domain name system is consulted up to a trillion times each day by the world's 1.8 billion Internet users. By using sophisticated public key cryptography, DNSSEC increases trust in the integrity of that process.

Stopping certain cyber crimes
DNSSEC is a powerful tool to combat cyber crimes that have no organizational or national borders. Cyber crime covers a wide range of illegal activities that includes online fraud, money laundering and identity theft. DNSSEC will specifically protect against two types of attack known as "cache poisoning" and "man-in-the-middle attacks" that can be used to distribute malicious software and commit fraud.

Cache poisoning
When you type an address into your browser, you are sent to that site and the domain name system saves, or caches, the information so your next request for that address will be processed faster. If your request is

diverted to a false address, you might end up at a malicious site that infects your computer with viruses, worms, Trojan horses or spyware. These can lead to fraud and the theft of personal or sensitive information. If the request came from a service provider, thousands of people can be affected when the false information is sent on to the provider's customers. Once the fake information is saved on your machine, your DNS cache information is considered *poisoned*.

Man-in-the-middle attacks
In a man-in-the-middle attack, a criminal intercepts one-to-one communications then continues to communicate with the second party while masquerading as the first. For instance, a criminal could divert an online communication from a customer to a bank and then, pretending to be the customer, use the information to empty the victim's bank account.

What DNSSEC does
It will eventually allow Internet users to know with certainty that they have been directed to the website they intended.

What it doesn't do
DNSSEC isn't an antidote to all Internet security problems. It does not ensure confidentiality of data or protect against denial of service or many other attacks. The best way to protect yourself online is still to use common sense.

"DNSSEC is not a silver bullet to stop every cyber crime. But it will have a real and positive impact on the security of the Internet. This is one important step forward in the fight against cyber crime," according to Beckstrom.

Decades of engineering work
The Internet is a global resource and its bottom-up cooperative nature has once again proven key to achieving a significant improvement. "The Internet will be more secure because the Internet Engineering Task Force (IETF) devoted decades to solving the technical challenges," stated Steve Crocker, member of the ICANN Board of Directors and chair of ICANN's Security and Stability Advisory Committee.

###

To read about DNSSEC at the root of the Internet, go here: http://www.root-dnssec.org.

To read technical information about DNSSEC, go here: http://www.dnssec.net.

To read about DNSSEC deployment, go here: http://www.dnssec-deployment.org.

MEDIA CONTACTS:

Brad White – Director of Global Media Affairs
Washington, DC USA
Ph: +1 310.301.3884
brad.white@icann.org

Michele Jourdan – Media & Marketing Coordinator
Los Angeles, CA USA
Ph. +1 310.301.5831
michele.jourdan@icann.org

ICANN's mission is to ensure a stable, secure and unified global Internet. To reach another person on the Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet. ICANN was formed in 1998. It is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. ICANN doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet. ***For more information please visit: www.icann.org.***