

# Internet upgraded to foil cyber crooks

July 29 2010, by Glenn Chapman

---



The Internet has undergone a "critical" upgrade that promises to stop cyber criminals from using fake websites that dupe people into downloading viruses or revealing personal data.

The Internet has undergone a key upgrade that promises to stop cyber criminals from using fake websites that dupe people into downloading viruses or revealing personal data.

The agency in charge of managing Internet addresses teamed with online security services firm [VeriSign](#) and the US Department of Commerce to give websites encrypted identification to prove they are legitimate.

"This is, by any measure, an historic development," ICANN chief executive Rod Beckstrom said while breaking the news at a premier Black Hat [computer security](#) conference in Las Vegas on Wednesday.

"This security upgrade matters to everyone who uses a computer, and that means most of us."

The Domain Name System Security Extensions, referred to as DNSSEC, basically adds a secret, identifying code to each website address.

The domain name system is where the world's Internet addresses are registered and plays a key role in enabling computers around the world to speak with one another online.

Applications commonly used on the Internet can be tailored to essentially check the ID of a website to make certain it is what it claims to be, according to Dan Kaminsky, a hacker turned computer security specialist.

For example, web browser software such as [Google](#) or Bing could be adapted to tell whether a bank log-in page is authentic.

"When a user receives an email from a bank they should know it came from a bank," Kaminsky said. "This is something we needed as engineers to make this a reality."

A frightening structural flaw in the foundation of the Internet revealed by Kaminsky at Black Hat here two years earlier led to the "biggest structural" upgrade to Web in decades, according to Beckstrom.

"I can't say I really knew what I was getting into when I broke that whole DNS thing," Kaminsky quipped as he took part in a press conference announcing the Internet improvement.

Kaminsky is chief scientist at New York start-up Recursion Ventures and worked with [ICANN](#) and VeriSign on the the Internet upgrade.

Internet engineers have been toiling on DNSSEC for 18 years, but technical and political obstacles stalled progress, Internet Engineering Task Force chairman Russ Housely said in a video call from a meeting of the group in the Netherlands.

"It can be thought of as tamper-proof packaging for the domain name structure," Housely said.

"The whole Internet engineering community is excited by this development."

He added that IETF members at the meeting toasted the announcement with champagne which "I assure you is not a common occurrence at a gathering of engineers."

It will take time for Internet firms to take advantage of DNSSEC and for it to be applied to local domains in every country, according to Kaminsky.

"We are on Day One of a multi-year journey," Kaminsky said.

DNSSEC strips [cyber criminals](#) of being able to do attacks that involve manipulating code to redirect people from legitimate websites to fake pages rigged with malicious code or asking for passwords and other valuable data.

"This provides a high level of protection with minimal disruption," said VeriSign chief executive Mark McLaughlin.

"It is not a panacea for everything, but it is a good start."

(c) 2010 AFP

Citation: Internet upgraded to foil cyber crooks (2010, July 29) retrieved 25 April 2024 from <https://phys.org/news/2010-07-internet-foil-cyber-crooks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.