



# USA TODAY

A GANNETT COMPANY



## FALL TV ratings

*Pan Am, Unforgettable among those showing promise, but comedy proves to be king, 1, 3D*

ABC

"The infrastructure baked into the Internet, which is based on trust, is starting to fall apart," says Michael Sutton, research vice president at security firm Zscaler.

CAs digitally certify account sign-ins, shopping and other pages where consumers type sensitive data. This sets up an encrypted connection to the Web browser, which displays the form for the consumer to fill out. The browser trusts only digitally signed pages.

A counterfeiter issued valid DigiNotar certificates for 531 faked pages. Some of the pages were crafted to expertly impersonate online properties of Google, Microsoft, Skype, Equifax, Twitter, Facebook and the CIA, among others, according to consulting firm Fox-IT.

This touched off a scramble to cut off the faked pages, which were difficult for consumers to spot as faked. The successful hacks demonstrated that it is possible to "impersonate any site on the Internet," says Josh Shaul, chief technical officer at security company AppSec.

No banks or payment-service websites were targeted, says Mikko Hypponen, chief researcher at anti-virus firm F-Secure. The hackers seem much more interested in harvesting personal data from e-mail services, social networks, credit bureaus, blogging sites and anonymity services.

The pressure is on CAs and browser makers to do more to identify and quickly eradicate counterfeit certificates and faked Web pages, security experts say. "No one knows where the next breach will occur," says Jeff Hudson, CEO of digital certificate management company Venafi.

Microsoft, maker of Internet Explorer, declined to comment, as did Apple, maker of the Safari browser. "The security of the Web is our collective responsibility," says Johnathan Nightingale, Mozilla's director of Firefox engineering.

# Hackers shake Web to the core

## Security at top levels questioned

By Byron Acohido  
USA TODAY

The keepers of the Internet have become acutely concerned about their ability to protect the most sensitive personal information such as account logons and credit card numbers.

Hackers cracked three companies that work with the most popular Web browsers to ensure the authenticity of Web pages where consumers type in sensitive information.

The hacked firms are among more than 650 digital certificate authorities (CAs) worldwide that ensure that Web pages are the real deal when displayed by Microsoft's Internet Explorer, Firefox, Opera, Apple's Safari and Google's Chrome. A hacker gained access to digital certificate supplier DigiNotar this summer and began issuing forged certificates for dozens of marquee companies.

Unable to cope with the fallout, the Dutch firm filed for bankruptcy last week. Two other digital certificate

**"No one knows where the next breach will occur, or whether it will occur."**

## Newsline

WEDNESDAY, SEPTEMBER 28, 2011