03
2009

This Issue

digicert®
Your Success is Built on Trust™

New DigiCert Customers

Mozilla Messaging
Jimmy Johns Franchise
Mitsubishi Motors
Rabobank Nederland
Minnesota Senate
Petro Canada
Nikon Research Corporation

Updated PCI Compliance Requirements:

Changes have recently been made to the Payment Card Industry Data Security Standard (PCI DSS) which have made the use of SSL 2.0 a PCI DSS violation.

In order to remain fully compliant, site administrators must ensure that their servers only allow the more current SSL 3.0 / TLS 1.0 encryption ciphers.

These ciphers are not related to the SSL certificates themselves; rather, they are enabled by settings on the server. DigiCert SSL certificates are fully compatible with the SSL 3.0 and TLS 1.0 cipher suites, ensuring that your certificates use the latest technology and encryption strength.

DigiCert EV SSL Certificates Protect Users From SSLstrip and Man-in-the-Middle Attacks

On Wednesday, February 18 at the Black Hat conference in Washington, D.C., an independent hacker known as Moxie Marlinspike presented a software tool called SSLstrip designed to remove the SSL protection from websites using advanced man-in-the-middle attack methods.

Marlinspike demonstrated how the SSLstrip program can intercept connections between a web browser and a trusted website, then serve the web browser the contents of the trusted site without trusted SSL encryption. The webpage could potentially be loaded unsecured (http) or spoofed with a low-assurance SSL certificate on a fraudulent domain name, similar to a phishing attack.

SSLstrip could potentially be effective at stealing sensitive information including usernames, passwords, or credit card information in situations where man-in-the-middle attacks are possible such as in Onion Routing configurations and Wi-Fi networks.

SSLstrip does not demonstrate a weakness in SSL encryption, but rather takes advantage of users who fail to look for trusted SSL encryption when sending sensitive information over the Internet. This problem has been exacerbated by the use and distribution of low-assurance certificates.

In anticipation of such problems DigiCert joined with the other major Certification Authorities and Browser developers to establish Extended Validation Certificates. EV Certificates are all vetted rigorously to guarantee authenticity of websites and strong encryption.

EV certificates are recognized by major web browsers such as Internet Explorer, Firefox, Opera, Safari, and Chrome. All of these browsers distinguish EV-secured websites by easily identifiable means. For example, the website address bar of Internet Explorer 7 will turn green to certify that the user is connected to an EV-secured website.

“The proper use and recognition of EV certificates effectively resolves the weaknesses exposed by both phishing and man-in-the-middle attacks,” explained Christopher Skarda, DigiCert’s Vice President of Operations. “In this way, EV certificates help to protect users against identity theft. Also, EV certificates help online companies to establish the trust and protection that their customers have learned to expect.

For more information, call us toll free (Canada or US) at 1-800-896-7973 (International Customers please call us at +1-801-877-2100).

Visit us online at www.digicert.com (24-hour Live Chat service provided).

High Assurance SSL

Your Success is Built on Trust™. Your customers need to know that the website they are visiting is Authentic (the real deal) and that their private information is encrypted.

Identity-related theft using tactics such as Phishing are a real and serious threat to online business. DigiCert is a leading provider of High Assurance SSL Certificates and Identity Assurance Services all geared towards helping you build Trust online with your customers.

With trust comes increased sales -- this is a proven fact.

When you purchase an SSL certificate through DigiCert, we include industry-leading support via phone, email, and live chat 24 hours a day. We will be more than happy to help you with your certificate installation or troubleshoot any difficulties that may arise during the lifetime of your certificate.

Learn more about DigiCert SSL Services

DigiCert EV Expanded to Opera

DigiCert EV Supported in 100% of EV-enabled Browsers

By: Christopher Skarda, VP of Operations

With fraud and identity theft as the top concerns of today's online consumers, Extended Validation (EV) SSL can increase user trust for any online business.

DigiCert EV certificates are now supported in 100% of EV-enabled browsers with the recent addition of Opera. Opera is added to a list of browsers that support the "green bar" for DigiCert EV SSL that also includes Internet Explorer, Firefox, Safari, Chrome, and Flock.

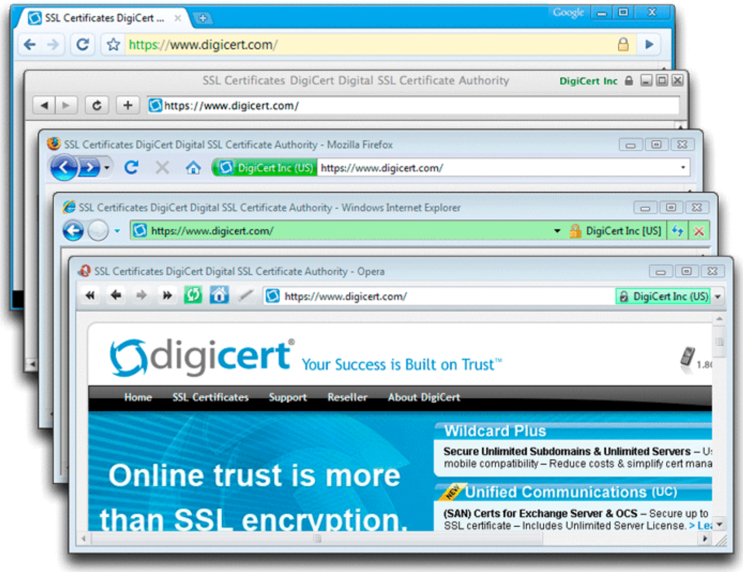
Because Extended Validation certificates require a more rigorous fraud-prevention and identity verification process than that of standard SSL certificates, the web browser address bar will turn green when users visit your site, verifying your authenticity and increasing trust.

Your success is built on trust. Increased trust means increased conversions, and confidence at checkout time.

For emerging companies, EV SSL certificates help to establish your online legitimacy. For high-profile businesses or organizations that are especially susceptible to phishing attacks, the green bar helps to protect your customers against fraud.

Your users need to know that their sensitive information is safe. Get increased confidence by securing your site with the strongest encryption in the industry.

More about DigiCert EV



SSL Certificates DigiCert ...
https://www.digicert.com/
SSL Certificates DigiCert Digital SSL Certificate Authority
DigiCert Inc
SSL Certificates DigiCert Digital SSL Certificate Authority - Mozilla Firefox
DigiCert Inc (US)
SSL Certificates DigiCert Digital SSL Certificate Authority - Windows Internet Explorer
DigiCert Inc [US]
SSL Certificates DigiCert Digital SSL Certificate Authority - Opera
digicert Your Success is Built on Trust™
Home SSL Certificates Support Reseller About DigiCert
Wildcard Plus
Secure Unlimited Subdomains & Unlimited Servers – U
mobile compatibility – Reduce costs & simplify cert mana
Online trust is more than SSL encryption.
Unified Communications (UC)
(SAN) Certs for Exchange Server & OCS – Secure up to
SSL certificate – Includes Unlimited Server License. > Le

Stimulus Package Impacts IT Sectors

$19 Billion for Health Care Technology

By: Travis Tidball, Director of Customer Relations

The much debated American Recovery and Reinvestment Act (ARRA), signed into law by President Barack Obama, contains over $150 billion in measures to revitilize health care in the United States of America.

Specifically, institutions that adopt Electronic Health Records (EHRs) will receive $17 billion as incentive payments via Medicare and Medicaid. Another $2 billion is allocated in the form of grants and loans to help institutions make the transition.

The adoption of electronic health records will greatly reduce the overhead costs associated with maintaining and protecting physical records, while making them more available when needed. In 2004, it was estimated that 1 in 7 hospitalizations occurred when medical records were not available.

SSL certificates should be used in all instances when these records are transferred, whether that be via the internet or a private network.

DigiCert SSL certificates provide strong encryption and authentication to ensure that such records will be transferred securely to the proper entities.tion, whether that be via the internet or a private network.

Screencasts Enhance Support Pages:

By: Travis Tidball, Director of Customer Relations

DigiCert has enhanced its support pages with new screencasts for generating CSRs and installing SSL certificates on Microsoft IIS 5/6x, IIS 7+, and Exchange 2007.

The screencasts will supplement DigiCert's text based instructions in order to improve the overall CSR generation and certificate installation experience.

Users report that it is very helpful to follow along a real person in addition to reading the standard support pages.

DigiCert asked its full-time technical support staff to pull double duty by performing the voice recordings along with their normal duties. Don't be surprised if you call in and reach the same Jared, Kyle, or Dan as you hear on the screencast!

The screencasts are available online at http://www.digicert.com/security-certificate-support.htm and by searching for DigiCert SSL Certificates at http://www.youtube.com.

As always, feel free to contact our support team directly by calling 800-896-7973 (Dial +1-801-701-2100 outside of US/Canada) or emailing support@digicert.com.

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
+1-866-842-0223 fax
www.digicert.com

Feedback? Article Suggestions? We want to know! Send an email to newsletter@digicert.com