WHITE PAPER:

The Impact of Extended Validation (EV) Certificates on Customer Confidence

As ecommerce expands, customer trust is essential to financial success, customer conversion, and business growth. However, cybercriminals have become increasingly adept at fooling customers into thinking they are visiting a legitimate website by using visual cues similar to real online trust markers. Customers need to be reassured that their confidential information is safe and protected from malicious activity. Without concrete proof that their data is protected, customers may abandon their shopping cart or other transaction when prompted to enter their sensitive information. DigiCert's EV SSL Certificates are specifically targeted at increasing customer confidence in ecommerce through specific, EV certificate-only browser cues.

In this white paper, you will see statistics illustrating exactly how prevalent cybercrime is and why online consumers should be cautious. You will also get a better understanding of why DigiCert EV Certificates give consumers the confidence they need to do business on your website.

CURRENT STATE OF WEB COMMERCE

As access to the Internet grows, more people are spending time online than ever before. Industry experts predict that online accounts will become the primary customer touchpoint within a decade. However, many people are still reluctant to conduct transactions online due to concerns about protecting financial information and increasing consumer awareness of online scams. The financial consequences of this reluctance are easy to measure:

- Shopping carts are abandoned, causing a loss in sales and revenue
- Click-through tracking shows that potential customers reach enrollment forms but do not fill them out
- Search analytics show that brands and company names are often hijacked to lure customers away from legitimate sites.

The average abandonment rate for online shopping carts is staggering. Recent studies reveal that between 59-65%[1] of all carts are abandoned. According to one Forrester study, 88%[2] of online shoppers say that they have abandoned an online shopping cart without completing a transaction.

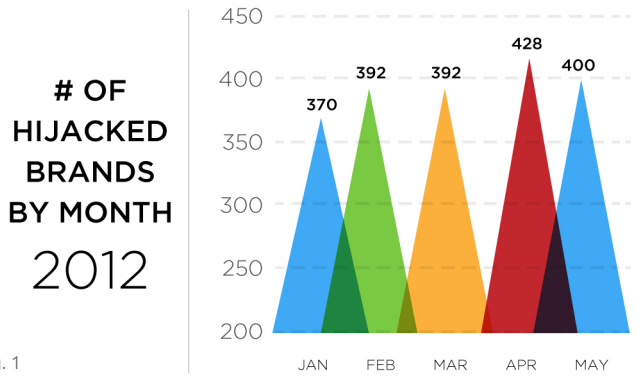

Fig. 1

Internet scams have become more coordinated and sophisticated, eroding the consumer trust essential to online

Fig. 2

business. In April 2012, the Anti-Phishing Working Group reported an all-time high of 428 brands targeted and hijacked by phishers[3]. In Q2 of 2012 the total number of URLs used to host phishing attacks was also at an all-time high of 175,229.

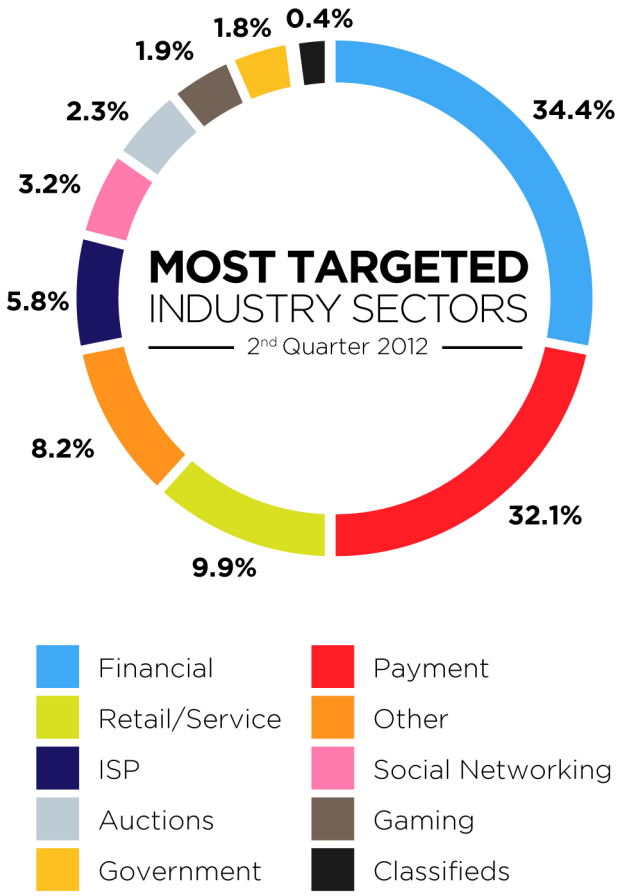

Fig. 3

HISTORY OF SSL CERTIFICATES

Most websites use SSL Certificates to encrypt data and assure their visitors they are an authentic site. SSL (Secure Sockets Layer) is a security technology that was invented to establish an encrypted link between a server and a client—typically a Web server (website) and a browser, or a mail server and a mail client (e.g., Outlook). SSL allows sensitive information (credit card numbers, social security numbers, login credentials, etc.) to be transmitted securely. The third party vendors that issue SSL Certificates are called Certificate Authorities, or CAs.

The creation of the SSL protocol provided consumers with a much needed boost in confidence and trust in ecommerce, and the online experience in general. But as the threat of phishing and pharming grow each day, online trust has eroded significantly.

In response to these sophisticated exploits, DigiCert and other leading CAs came together with browser providers like Microsoft and Mozilla to form the CA/B Forum. Their objective was to develop guidelines to improve how SSL worked, along with the associated validation process. The creation of Extended Validation or EV SSL Certificates was the first result of that effort. EV SSL Certificates undergo a more rigorous validation process, and subsequently display special EV certificate-only browser cues. EV SSL Certificates not only create an encrypted connection between a server and a browser, but verify that a trusted third party (the CA) has authenticated that organization's identity.

WHAT IS AN EXTENDED VALIDATION (EV) CERTIFICATE?

EV certificates are SSL Certificates which require a detailed and rigorous validation process. Any CA offering EV certificates must comply with a strict, security-minded validation process. This process includes:

- Verifying that the requestor has legal rights to use the domain
- Verifying that the requestor has properly authorized the issuance of the certificate
- Verifying the physical existence and legal status of the requestor
- Verifying that the identity of the entity matches official records

During this process, a representative from the CA will contact the requester at a verified phone number to confirm they requested the certificate and that they are authorized to receive the certificate. Maintaining this human element in the process provides an additional layer of defense against fraudulent or phishing-related activity.

To notify the user of an EV certificate on a website, browsers show specific visual cues for sites secured with EV certificates:

- Green in the address bar
- Company name and padlock in the address bar
- https:// at the beginning of the address
- Company information in the certificate details

HOW DO EV CERTIFICATES INCREASE CUSTOMER CONFIDENCE?

As detailed above, customer confidence in ecommerce decreases when users cannot tell the difference between real business and phony phishing websites. High-profile incidents of fraud and phishing scams have made users more concerned about protecting their information online. They may abandon their shopping cart or other transactions when prompted to enter sensitive information. Because of the additional visual cues that EV certificates provide, users are assured that they are on an authentic and validated website.

But the visual cues are only as strong as what they represent. The reason users can trust an EV certificate's browser cues is because the verification process for EV certificates is so rigorous. As EV certificates become more prevalent, users will begin to look for and trust the green bar. This is illustrated in the graphic below.

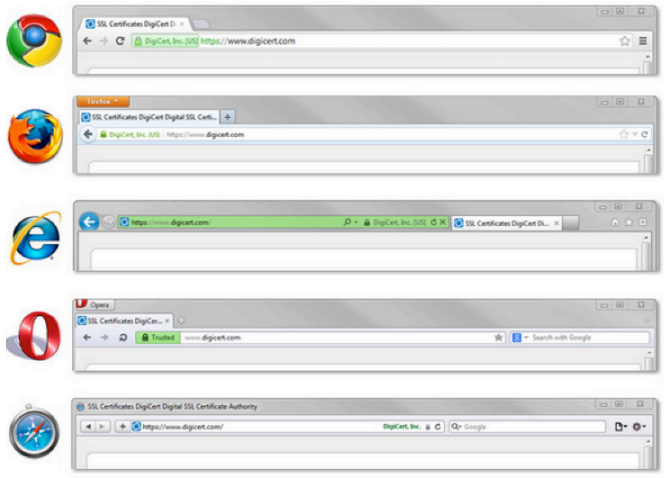

Fig. 4

WHY SHOULD I BUY AN EV CERTIFICATE?

An EV certificate lets your visitors complete secure transactions with confidence, decreasing cart abandonment rates. An EV certificate also puts your organization in a leadership position. If your site has the green bar and your competitor's site does not, you have a competitive advantage by appearing to be more trusted. For businesses with a high profile brand, using EV certificates is one of the best defenses against phishing scams. When customers see the green bar and the name of your security vendor they can interact with you online without fear and their confidence in ecommerce grows.

Why Buy an EV SSL Certificate from DigiCert?

The Certificate Authority (CA) you select will impact ease-of-use, speed of issuance, uptime, OCSP/CRL latency, and a variety of features that can make your network more secure and simple to manage. DigiCert® has been providing SSL Certificates and SSL management tools for over a decade and assisted in developing the Extended Validation Certificate in addition to working with Microsoft to develop and promote the use of Subject Alternate Names in SSL Certificates. DigiCert has an award-winning in-house technical support team and some of the fastest certificate issuance times—with EV certificates typically issued in a matter of hours! Experience the "DigiCert difference" for yourself by calling 1-800-896-7973 or visiting www.digicert.com.

EXTENDED VALIDATION

TECH-ED SURVEY FINDINGS

In a recent study, Tech-Ed taught 384 people that companies with EV SSL Certificates on their website go through a more rigorous validation process than those with standard SSL Certificates. They also taught them that sites secured with EV SSL Certificates could be identified by their green bar. After completing the study, Tech-Ed found the following:

Out of the participants Tech-ED surveyed

100% *Would **prefer** doing business with a company that has an EV SSL Certificate*

67% *Would **not** buy from an unfamiliar website that didn't have an EV SSL Certificate*

59% *Would **stop doing business** with a site if they noticed it lost the green bar temporarily*

When asked whether they would enter their credit card number on a site that was secured by a regular SSL Certificate:

28% *Said they were **most likely** to enter their details*

35% *Said they were **somewhat likely** to enter their details*

19% *Said they **probably wouldn't** enter their details*

18% *Said they **wouldn't** enter their details*

When asked the same question about a site secured by an EV SSL Certificate:

87% *Said they were **most likely** to enter their details*

10% *Said they were **somewhat likely** to enter their details*

3% *Said they **probably wouldn't** enter their details*

0% *Said they **wouldn't** enter their details*

Fig. 5

CORPORATE HEADQUARTERS
2600 West Executive Parkway Suite #500
Lehi, Utah 84043

TECHNICAL SUPPORT
support@digicert.com
Direct Phone: 1-801-701-9600
Spanish: 1-801-701-9601
Spanish Website: www.digicert.com/es/

TELEPHONE & FAX
Toll Free: 1-800-896-7973
Fax: 1-801-705-0481
Media & PR: 1-801-877-2123

EMAIL
Sales & Marketing: sales@digicert.com
Corporate Office: admin@digicert.com
Enterprise/Managed PKI: enterprise@digicert.com
Partner Information: channel@digicert.com

www.digicert.com
www.facebook.com/digicert
www.twitter.com/digicert (@digicert)
www.digicert.com/newsroom.htm
support@digicert.com

Figs. 1, 3: Anti-Phishing Working Group (2012). Phishing Activity Trends Report.
(1) Baymard Institute (2011). E-Commerce Checkout Usability.
(2) Forrester (2010). Understanding Shopping Cart Abandonment.
(3) Anti-Phishing Working Group (2012). Phishing Activity Trends Report.
Fig. 2: Invesp (2012). Shopping Cart Abandonment Rate Statistics.
Fig. 5: Tech-ED (2007). Extended Validation.