White Paper

Hidden Dangers Lurking in E-Commerce-Reducing Fraud with the Right SSL Certificate

Symantec™

Norton™ SECURED
powered by Symantec

Hidden Dangers Lurking in E-Commerce- Reducing Fraud with the Right SSL Certificate

Contents

"Domain Validated (DV)" SSL Certificates pose a direct threat to consumers on the Internet. Cybercriminals frequently use DV SSL certificates to impersonate real ecommerce websites for the purpose of defrauding consumers. This paper will explain SSL, the different types of certificates, how cybercriminals use DV certificates to steal personal and financial data, and what can be done to thwart this tactic.

Introduction

Shopping online has now become almost second nature to most of us, but where did it all start, and what enabled it to grow to the levels that we see today? Reportedly[1] it was back in 1994, with the first known web purchase being a pepperoni pizza with mushrooms and extra cheese from Pizza Hut. When that first pizza was ordered – and, a year later, when online retail giant Amazon sold its first book (Douglas Hofstadter's 'Fluid Concepts & Creative Analogies: Computer Models of the Fundamental Mechanisms of Thought'[2]), it ushered in a torrent of activity. Two decades later, global e-commerce sales for 2013 have been calculated at upwards of $1.2 trillion[3]. What facilitated this tectonic shift in our shopping habits? Trust.

Trust in who we were shopping with, and trust that the purchase information we provided would be secured. Because as ever, where there is money there will always be criminals - eager to take advantage of the burgeoning opportunity.

But if trust is the grease that lubricated the online marketplace, what is the technical basis for that trust? The answer is in part solved with Secure Sockets Layer (SSL), and more specifically, digital certificates - a reliable technology which has worked well for decades, and can continue to do so. But for this to happen, it has to be deployed responsibly. Put simply, not all certificates are created equal – and today, some ingenious criminals have found a way to corrupt the very system that was designed to stop them. As a result we need to make sure that certificates are matched to their uses and that when people send their personal and financial information across the internet they can have confidence that the recipient is not a criminal.

In fact, research from Norton estimates the global price tag of consumer cybercrime now topping some US$113 billion annually[4] which is enough to host the 2012 London Olympics nearly 10 times over. The cost per cybercrime victim has shot up to USD$298: a 50% increase over 2012. In terms of the number of victims of such attacks, that's 378 million per year – averaging 1 million plus per day.

What is a Digital Certificate and what is SSL?

In order to transact business online, consumers and businesses needed a way of exchanging credit card numbers, passwords, and other personal information securely. SSL is the technology that protects much of the Internet and in essence it enables e-commerce. It "lights up" the padlock symbol in the browser to tell the consumer they are safe to send their credit card information to a vendor in a

[1] http://www.huffingtonpost.com/2013/09/09/pizza-hut_n_3894981.html
[2] http://askville.amazon.com/item-sold-Amazon-happen/AnswerViewer.do?requestId=2746620
[3] http://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-This-Year-Driven-by-Growth-Emerging-Markets/1010575
[4] 2013 Norton Cybercrime Report: go.symantec.com/norton-report-2013

manner which no one else but that recipient's site can decipher. All data sent via SSL is encrypted. Without SSL, you would be sending your credit card information (or password, bank account, social security number, address etc.) across a very public Internet in plain text. This is like sending bank details through the mail on the back of a postcard – and it could risk having that information stolen. SSL was invented by Netscape in the 1990s to provide encryption over the insecure Internet.

But there is a catch: encryption is only useful if you know who you are sending the data to, and you are confident that it is the only party that can decrypt it. This is where certificates come into play.

SSL and Digital Certificates: Securing Transactional Website Data

To enable encryption, websites use "digital certificates" which are issued by organizations called "Certification Authorities (CA)", the largest of which is Symantec (formerly VeriSign)[5]. A Certification Authority is a trusted third party that verifies details about an applicant using a variety of databases, telephone calls and other means. Note that a CA does NOT verify the trustworthiness of a business; its role is to verify that the business exists and to issue credentials (digital certificates).

Currently there are three types of SSL certificates sold by most major Certificate Authorities – domain validated (DV), organizationally validated (OV) and extended validation certificates (EV)

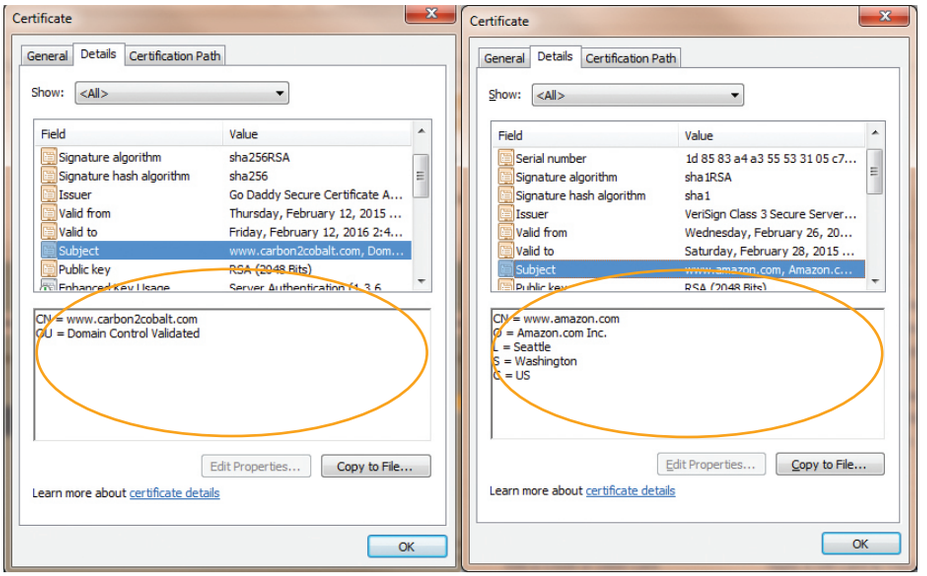
In the early days of the Internet, the only type of SSL certificate available was an "Organizationally Validated (OV)" certificate. With this type of certificate, the CA would validate certain business information along with the domain name to make sure the applicant "is who they say they are". For example, to purchase a website certificate for www.amazon.com, Amazon would send the CA some information from the webserver along with proof that this was a real company. In addition, the person requesting the certificate was validated as an employee of the company. The CA would validate this data (this could take 2-5 business days) and then issue the certificate to the website. The website then used this certificate to enable secure e-commerce using SSL.

This worked fine for many years but some organizations complained about the time involved to verify business details. They wondered if someone could come up with a quicker solution that still provided the necessary encryption. In the early 2000's, a new type of certificate appeared on the market called "Domain Validated (DV)". This certificate was issued very rapidly because it only required the applicant to prove the right to use a domain name – there was no validation of any other business information. For example, if someone purchased the domain www.myfavoritestore.com, then they could obtain a DV SSL certificate for that domain simply by applying to a Certificate Authority and responding to an email sent by the CA. Once the CA receives the response, the certificate is immediately issued. Then they could set up a website for MyFavoriteStore.com, and begin

[5]VeriSign was purchased by Symantec in 2010.

accepting credit cards securely. Consumers would see the padlock in the browser, indicating that all traffic is encrypted to the server.
Of course, the obvious problem here is that there is no validation done to demonstrate that MyFavoriteStore.com is actually a legitimate business - and not someone committing fraud.

The figures below compare a browser view (Internet Explorer) of a Domain Validated certificate for the domain “carbon2cobalt.com” and an Organizationally Validated certificate for amazon.com:



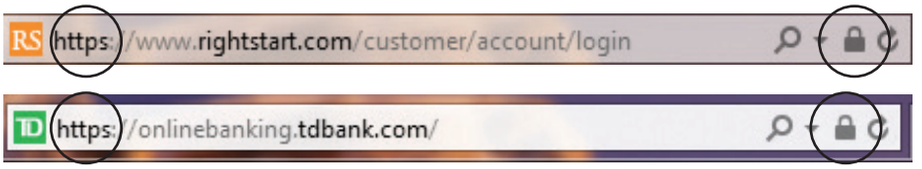
DV Certificate *OV Certificate*

(Screen shot obtained from Internet Explorer by clicking on browser lock in address bar, View certificates, Details tab and then Subject field)

As one can see, in the DV certificate, there is no information about the company other than the domain name (carbon2cobalt.com). There is no way to tell where this business is located or who owns it. The company name was never validated and hence is not shown. Contrast this to the OV certificate for amazon.com which shows the name of the company and its location. These items have been verified by the CA and are included inside the certificate.

Browsers do not distinguish this DV certificate from the OV certificates that undergo a more thorough vetting process (we’ll have more to say about that later). Both types of certificates show a lock on the screen. The two screen shots below depict two different websites. Both use SSL (as indicated by the lock) but which one used DV and which uses OV? Put differently – which one has shown only that it owns a domain name, and which has provided proof of its identity? It’s impossible to tell without clicking on the lock for more details, something few

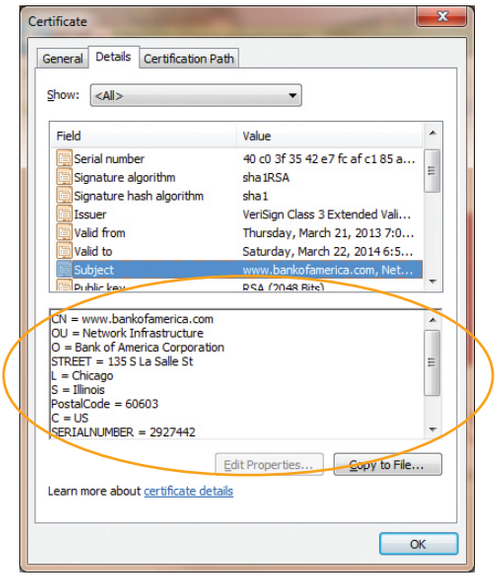
consumers ever do; most don't realize the information is there, much less how to make sense of it. It would be of immense value for the browsers to present that information (DV vs OV, business legitimacy info) in a consumer-friendly way, or for limitations to be developed for usage of DV certificates.



Thus, it is relatively easy for criminals to setup a fake website, obtain a DV certificate, and use the lock to falsely portray that the site is legitimate. Lured into a false sense of security, the criminals dupe consumers and steal their private data.

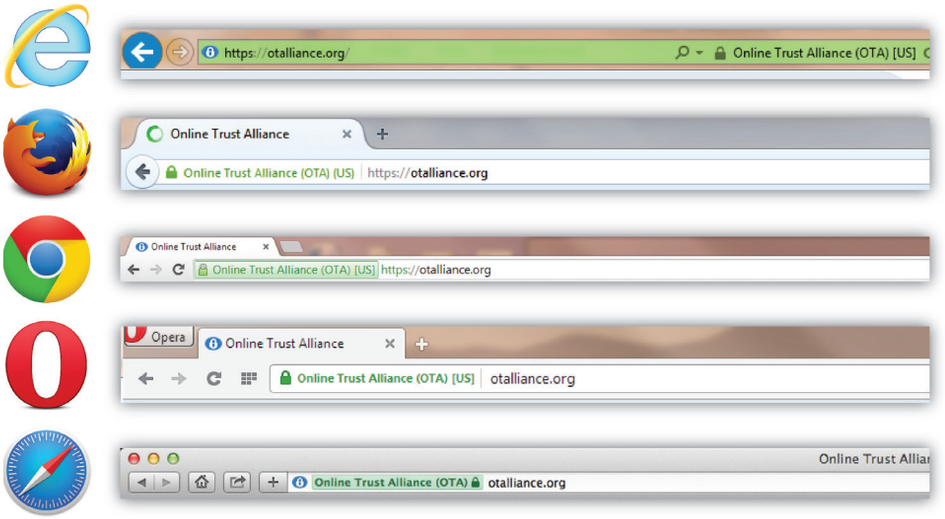
EV SSL Certificates

In response to complaints from various parties, as well as to strengthen authentication processes and Internet security, certificate authorities and browsers formed an industry association called the "CA/Browser Forum" in 2006 to address matters such as this. Early participants of this forum included Microsoft, Symantec, Comodo, Entrust and Mozilla. The first product of this group was specifications for a new type of certificate called "Extended Validation (EV)". In this case the CA performs enhanced vetting of the applicant to increase the level of confidence in the business. The browser display is enhanced and one can readily see the difference. Below is an example of an EV certificate:



In this example, it is clear that this certificate (and website) belongs to Bank of America in Chicago, IL. This information has been verified by the CA through a vetting process which included examination of corporate documents, checking of applicant individual identity and checking information with a third party database.

In addition all browsers give visual indicators, usually a green lock or address bar, to indicate that the website is using an EV certificate. This makes it much easier for the consumer to know that the identity of the website has been thoroughly verified. All browsers show the organization name to the left or right of the URL. The figure below shows how EV certificates are indicated in popular browsers. Enhanced vetting makes EV certificates much harder to obtain.



EV Certificates help establish the legitimacy of a business claiming to operate a website, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using Certificates.
2. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
3. Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the subject.

Because of the strict vetting procedures that a CA uses to check the information about the applicant, the issuance of EV certificates usually takes longer than other types of certificates.

Compared to the DV certificate, much more information is included, enough in fact to determine who the company is that is seeking the certificate. All of this information was verified by the Certificate Authority.

The CA/Browser Forum spent considerable time coming up with Baseline Requirements which specifically define DV, OV and EV certificates. Prior to these requirements, CAs would choose what vetting they would perform for each type

of certificate, meaning that a purchaser could select their CA on the basis of the rigorousness (or lack thereof) of the CA's authentication process. Now, adherence is required to these Baseline Requirements by all CAs, whether they are members of the Forum or not. The Baseline Requirements were approved by all members of the CA/Browser forum including Certificate Authorities and Browsers.

Why not DV certificates for ecommerce? What's the problem with DV certificates?

It's quite simple: in the earlier example, MyFavoriteStore.com isn't a real business. It's a fake website set up by a phisher. How is this possible? Let's walk through the steps:

1. The fraudster purchases the domain from a domain registrar using fake information and a stolen credit card. The registrar issued the domain name "myfavoritestore.com" to the fraudster.
2. Once he has the rights to the domain, the fraudster applies for a domain validated certificate from a CA. The CA only checks to see if the applicant can reply to an email to that domain. Once they reply, the CA issues the certificate.
3. The fraudster creates webpages that portend to sell popular items of general interest as well as a shopping cart and credit card acceptance pages.
4. Consumers are drawn to this site via bogus email messages or false advertising.
5. Once on the site, the consumer sees the padlock and assumes the site is valid so they enter their credit card information to make the purchase.
6. The fraudster steals the credit card data and the consumer receives no goods. When they look at the SSL certificate to get more data on the website, they find nothing but a domain name. There is no verified address or other business information.

Due to the lack of information in DV certificates as well as the ease in obtaining them, they have been successfully used by fraudsters to lure consumers into divulging private data such as account usernames/passwords and credit card information. A recent Netcraft study showed that 78% of SSL certificates found on servers hosting fraudulent websites were domain validated. While the majority were not obtained exclusively for phishing, those with misleading domains were subject only to domain validation[6]. The most interesting "targets" for fraudsters are popular sites where e-commerce is transacted such as Paypal, Apple, Visa, MasterCard and various foreign banks. An Apple ID has recently become a "high value" target. Fraudsters will setup a fake Apple website using a DV certificate to lure users. With such a credential, a fraudster can lock or locate a phone, make purchases on iTunes and gather information about the victim.

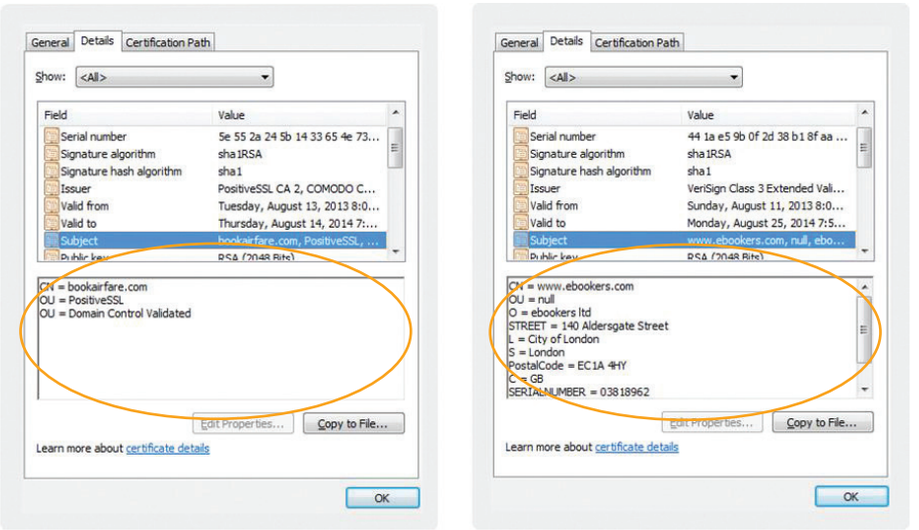
However, it's not only large companies that are targets. Small and medium sized businesses are also frequent targets because of their limited Information Technology sophistication. User credentials gleaned from a "hacked" small business could be used to impersonate a consumer at another website. This is because user names, passwords, and other credential information are frequently "re-used" by a consumer which makes it easy for hackers to try the same passwords at different websites.

[6]Netcraft study of 2,355 phishing sites that had implemented SSL

Recent research commissioned by Symantec showed that more than 1/3 of e-commerce websites are using DV certificates[7]. This is not a surprise, given the relative ease, speed and low expense of obtaining such a certificate. While all CAs must perform a basic "fraud check" on DV certificate applications, fraudsters are adapting their methods to circumvent these checks. For example, the name "Paypal" is a common fraud target and hence CAs will have automated checks to look for similar names in applications such as "pay-pal", "securepaypal", "p@ypal", etc. But recently, a certificate was issued to paypol-france.com which was then used to launch a phishing attack to steal user credentials. It's not clear how many users were fooled into divulging personal details. It would be much more difficult for a fraudster to obtain an OV or EV certificate for such a name.

Consumer safety with OV and EV

Compare the two certificates below. On the left is a certificate for the website "bookairfare.com" and on the right for "ebookers.com". A consumer who searched for cheap airfares via a search engine might be directed to these two websites but how would they know which business has been verified? By examining the certificate on the left, no business information is listed which means that it is a DV certificate. Contrast that with the certificate on the right which contains extensive, validated business data. While the business on the left is presumed authentic, no data has been validated, meaning that it could also be a fraud site[8].



Why risk of fraud with DV is higher

Criminals will commonly create fraudulent websites for the purposes of ID theft and account takeover. To add legitimacy to the website, they will add extensive graphics to mimic the real website and obtain an SSL certificate, which gives the user a visual indicator of security. As stated previously, a DV certificate is relatively easy to obtain. Once the fraudster has purchased the rights to a domain, they can apply

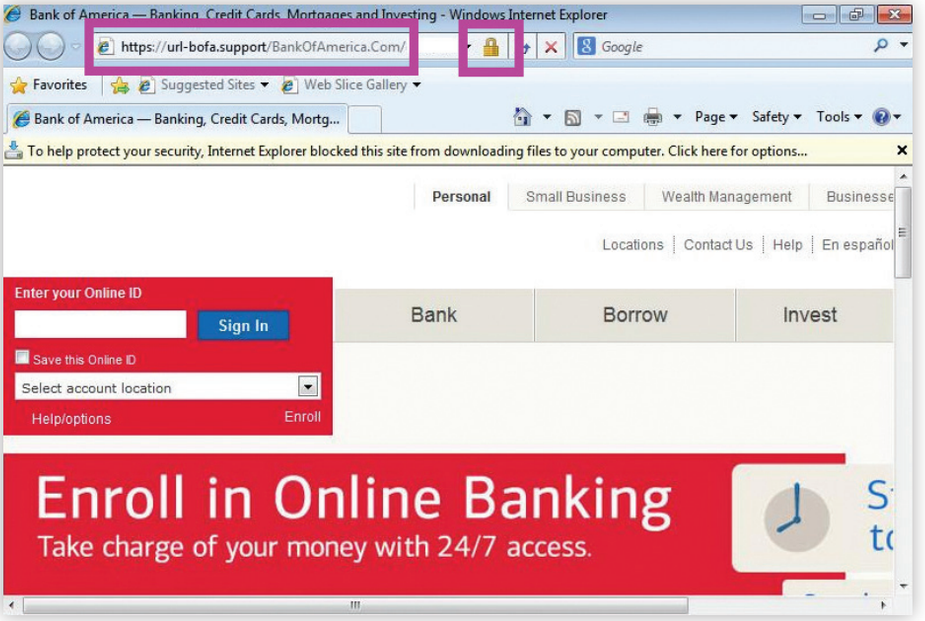
[7]Research performed by buySAFE, Inc. on behalf of Symantec
[8]This particular site is not known to be a fraud site.

for a DV certificate and receive it within minutes. The website is then setup and the fraudster will begin directing unsuspecting consumers to the site. Consumers will see the padlock (which DV certificates enable) and proceed to enter private data which can be distributed through the criminal network.

The figure below shows an example of a phishing email and the associated website one is taken to after clicking on the embedded link[9].

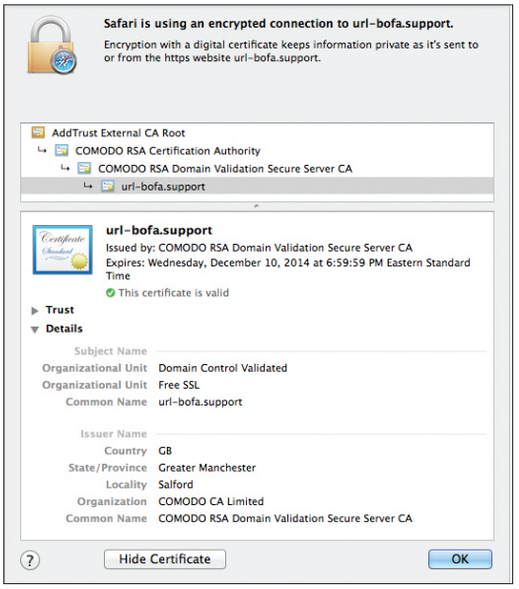
```
Dear Customer,

You have a new message waiting for you in your secure message center.

Please, click the link below to read now,


https://url-bofa.support/BankOfAmerica.Com


Thanks

Bank of America Email, 8th Floor-NC1-002-08-25, 101 South Tryon St.,
Charlotte, NC 28255-0001


Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2014 Bank of America Corporation. All rights reserved.
```

The site has a convincing web page and shows the lock:



[9]https://isc.sans.edu/forums/diary/httpsyourfakebanksupport+--+TLD+confusion+starts/18651

Examination of the SSL certificate reveals that it is a DV certificate:



That cybercriminals go to the trouble of obtaining SSL certificates demonstrates that users have become conditioned to look for the padlock or “https” before conducting a transaction. Many of these fraudulent sites are up for only days or hours, which means that unlike legitimate business which only have to apply for certs once every few years, the criminals are doing so constantly. They would not expend the effort and resources if there was no value in doing so.

The website, SSL Blacklist (www.sslbl.abuse.ch) provides a list of SSL sites that are associated with malware or botnet activities. A review of their most recent 5 months of data indicates that all of the SSL certificates blacklisted are either DV or self-signed (self-signed or untrusted certificates incur a browser warning, which fraudsters would likely avoid). This further shows the ease of obtaining these DV certificates is attractive to cybercriminals.

SSL Certificates at a glance

The figure below compares the 3 types of SSL certificates available in the market:

Cert Type	Domain validated?	https Encrypted?	Identity Validation	Address Validated?	Pad Lock Displayed in Browser User Interface?	Green address bar and other special treatment?	Typical relative price
DV	Yes	Yes	None	No	Yes	No	$
OV	Yes	Yes	Good	Yes	Yes	No	$ $
EV	Yes	Yes	Strong	Yes	Yes	Yes	$ $ $

As stated earlier, DV certificates do not provide any information about the business. Their use is limited to encryption ONLY. **There are valid use cases for DV certificates including non- ecommerce uses or sites that have a low probability of a phishing attack (i.e. no financial gain by attacker).**

Moving from a DV certificate to an OV or EV certificate does involve additional expense to the website operator but the difference is surprisingly small. The chart below compares the retail prices of DV, OV and EV certificates among the top providers (as of August 2014):

Cert Type	RapidSSL	GoDaddy	Comodo	Digicert	GeoTrust/ Thawte	Globalsign	Symantec
DV	$49	$69	$79	N/A	$149	$249	N/A
OV	N/A	$99	$99	$175	$199	$349	$399
EV	N/A	$199	$449	$295	$299	$899	$995

Competitive retail prices for 1 year validity SSL certificates. Note that some providers add other services to their prices for increased value.

For a relatively small amount of additional money (compared to a DV certificate), a legitimate business conducting e-commerce could purchase an OV or EV certificate. This would prove to the consumer that the business has been validated and provide address and other contact information in the certificate which the consumer could use in case of questions or problems.

In addition, EV certificates provide another benefit: a visual cue (green bar) in the browser tells the consumer that the business has gone through the effort to obtain this certificate, the information has been verified by the CA, and there is a higher probability that online trust can be established.

Summary

"On the Internet, nobody knows you're a dog."

[10]

As the cartoon above highlights – on the Internet, it is easy to pretend to be someone you are not. Looking at the way we all interact online, it's important to understand the threat landscape and help the industry take the required action. The fact is that e-commerce can prove to be extremely compulsive – buy something now! With cost, time until delivery, and returns policy often highest up the agenda, security is typically an afterthought at most. It's no wonder that the cyber criminals have moved in en masse, lured by the easy pickings and riches to be had. And it's this movement that makes security and particularly the use of security online more important today than ever before.

[10]Cartoon by Peter Steiner and published by The New Yorker July 5, 1993 (licensed with permission of Conde Nast)

E-Commerce plays an important role in the US and global economy. The US, with its technology leadership, has an opportunity to improve the security situation with respect to Internet e-commerce.

As more people spend time online, it's everyone's responsibility to demand more from the sites that we visit. With almost 25,000 suspected phishing sites likely using valid SSL certificates in the year leading up to March 2014[11], the foundations of trusted commerce could be undermined. Phishing is essentially an online con game and phishers can been seen as tech-savvy con artists and identity thieves. They use SPAM, malicious web sites, email messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts. The website element is key here – if consumers do not know which site to trust then there is a real problem.

Ideally what the industry needs to do is ensure that if consumers are spending money online, they should be able to trust the site they are shopping on. To do this the industry needs to make a step change to the type of SSL certificates that help make e-commerce trustworthy.

Recommendation

We recommend that e-commerce websites, at a minimum use an OV or EV certificate to secure their website and to convey valid authentication information. Simply put, DV certificates can be easily obtained by fraudsters, are used in phishing, and are currently implemented in about 1/3 of all e-commerce websites. E-commerce companies that accept credit card data and ship products via online purchases should be required to use a minimum of an OV certificate. DV certificates are just not appropriate for this purpose due to the high risk of fraud.

E-Commerce needs relate to an environment where 552 million identities were exposed in 2013[12]. Once identities are stolen, they are used by attackers to compromise other accounts, through password reset features on websites. Depending on the stolen information, they could use the data to make bank transfers to accounts under their control or create fraudulent credit cards.

Requiring OV or better for e-commerce is about:

1. Facilitating trade and commerce
2. Making the Internet safer
3. Helping legitimate small businesses better establish online credibility
4. Protecting consumers
5. Reducing fraud
6. Building trust

Requiring OV for e-commerce significantly increases the cost and time needed for fraudsters to obtain a certificate because:

1. OV requires a business be established which means they would have to go through the steps to register a business

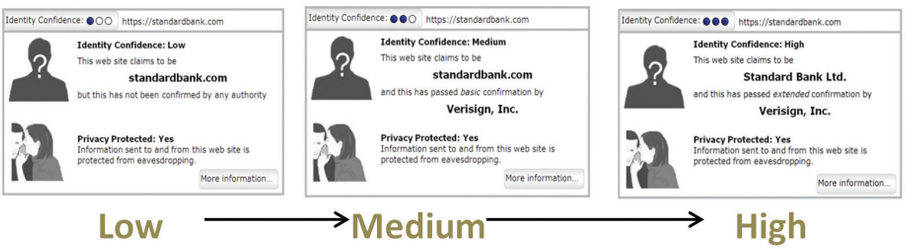
[11] Data produced by Symantec research
[12] Symantec 2014 Internet Security Threat Report Vol. 19

2. OV requires a phone call verification or information from publicly available data sources, the latter which is unlikely given fraudsters do not like to bind themselves to a physical location

However, this does NOT increase the time required for legitimate businesses to obtain an OV certificate.

End users have the right to expect certain levels of security when shopping online. Requiring an online merchant to use an OV or EV certificate will help protect consumers from fraud while requiring very minimal additional cost to the merchant. There are certainly good uses for DV certificates such as web blogs and non-critical login sites where the ability to steal money or personal data is trivial and would not be attractive to cybercriminals. E-commerce however, does not fall into that category.

Browsers can also play a role in helping users identify the types of certificates used on websites by surfacing this information to the forefront. As stated earlier browsers do not readily distinguish DV and OV certificates because they believe users cannot comprehend the difference. While some studies show users can be overwhelmed with information that they then choose to ignore[13], others make the case for an easy to understand pictorial coupled with simplified language to give users the information they need. Consider research performed by Carleton University in Ontario, Canada[14] which showed users three sample displays. The displays below are sample indicators designed to show users that while their traffic is encrypted (Privacy Protected), there are 3 different and distinct levels of authentication which are easily conveyed. The left most pictorial could correspond to a DV certificate since identity confidence is low. The middle warning where identity confidence is medium corresponds to an OV certificate and the right display represents an EV certificate where identity confidence is high. The research showed a substantial improvement in user understanding of warnings presented in this fashion.



We support additional research to determine the types of browser warnings that are effective for most end users.

We have shown two ways in which fraud with DV certificates can be reduced: by requiring that OV or EV certificates be used for e-commerce websites, and how browsers can improve the user interface related to certificate types. It's time for the community to come together and cooperatively address the issues highlighted in this paper.

[13]The Emperor's New Security Indicators, 2007; Schechter, Dhamija, Ozment, Fischer
[14]Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study, www.scs.carleton.ca/~paulv/papers/ccsw09.pdf

More Information

Visit our website

https://www.symantec.com/ssl-certificates

To speak with a Product Specialist

North America: +1(866) 893-6565 or +1(520) 477-3135; SSL_EnterpriseSales_NA@symantec.com
U.K.and Ireland: +0800 032 2101; sslsales-uk@symantec.com
Rest of EMEA: +353 1 793 9053 or +41 (0) 26 429 7929; sslsales-ch@symantec.com
Asia Pacific: +61 3 9674 5500; ssl_sales_APAC@symantec.com

To speak with a Product Specialist outside the U.S.

To speak with additional product specialists around the world, visit our website for specific offices and contact numbers.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions.Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems.Our industry leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world.More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

UID: 243/01/15