

RESEARCH PAPER – RELATIVE INCIDENCE OF PHISHING AMONG DV, OV, AND EV ENCRYPTED WEBSITES

Chris Bailey and Kirk Hall, Entrust Datacard
Melih Abdulhayoğlu and Fatih Orhan, Comodo

September 13, 2017

Abstract: *To date, no one has developed reliable data showing whether there is a significant difference in the risk to users of phishing from encrypted sites using DV, OV, and EV digital certificates. Our initial study of such sites indicates that (1) EV websites are significantly safer for users than DV and OV websites, (2) OV websites are somewhat safer for users than DV websites, (3) the main reasons why some OV websites have phishing are (a) shared content sites with a single OV certificate for the site owner, where individual pages are then controlled by others and include phishing content, (b) shared OV certificates containing multiple SANs belonging to multiple independent site owners or even the same owner, and (c) compromised OV sites where the owner is unaware of the phishing content that has been placed on “orphan link” pages for the site.*

We propose certain steps to eliminate these OV phishing sites, and the adoption of common browser UI design elements that will alert users when they are at identity websites (OV and EV), which are safer and more trustworthy than anonymous (DV) websites. This data-driven research is at early states only, and will be expanded over time with additional public updates.

We are excited to present our initial data and research results to the Ensuring Web PKI Integrity Meet-Up at PayPal’s San Jose offices. This is only the start of our research, and we plan to present additional data in the near future and on a continuing basis as available.

1. Problem Addressed

The problem we are addressing through our research and data is the same as the subject of this meet-up: We are experiencing increased use of *trusted TLS endpoints* to engage in phishing distribution. The overall question is, how might we work together to reduce the time-to-assess the intentions of a website and to increase user awareness of website content “intent and safety”?

The Meet-Up Agenda covers a number of promising approaches to this problem, including possible improvements to the browser UI security indicators. Our research focuses on that element, and we have very promising preliminary data.

2. Our Initial Assumption

We know that phishing sites are moving from http to https in order to avoid browser warnings, and we know that tens of thousands of DV phishing sites have been created for major banks, credit card companies, and other high value targets. As discussed below, our data shows that roughly 12% of phishing sites today have a valid SSL/TLS certificate, and the vast majority of these are DV certificates.

The number of phishing sites with certificates will only grow in the coming months as we move to a 100% encrypted web.

Our initial assumption was that encrypted websites with anonymous DV certificates were used in the vast majority of fraudulent web activity as compared to organization vetted identity certificates (OV and EV), and therefore users would be *safer* at identity websites and should be trained to recognize the difference between anonymous and identity websites through a new browser UI.

What was the basis for our initial assumption? The simple fact that people generally won't commit bad acts if their identities are attached – they prefer anonymity for bad acts. Any website owner that takes the trouble to complete identity confirmation with a commercial CA for an OV or EV cert should be unwilling to use that cert on a phishing website because the site will be flagged and the cert may no longer be usable, whether or not revoked. In contrast, DV certs today are easier to get on an immediate, anonymous basis with minimum fraud checking, and can be replaced with little effort.

Does our initial data support our assumption that identity websites are safer for users than anonymous sites? Yes, and no – identity websites are safer (EV sites are absolutely safer), but some OV websites have been flagged for phishing. Why is this true, and what can be done to solve the problem?

3. Our Methodology

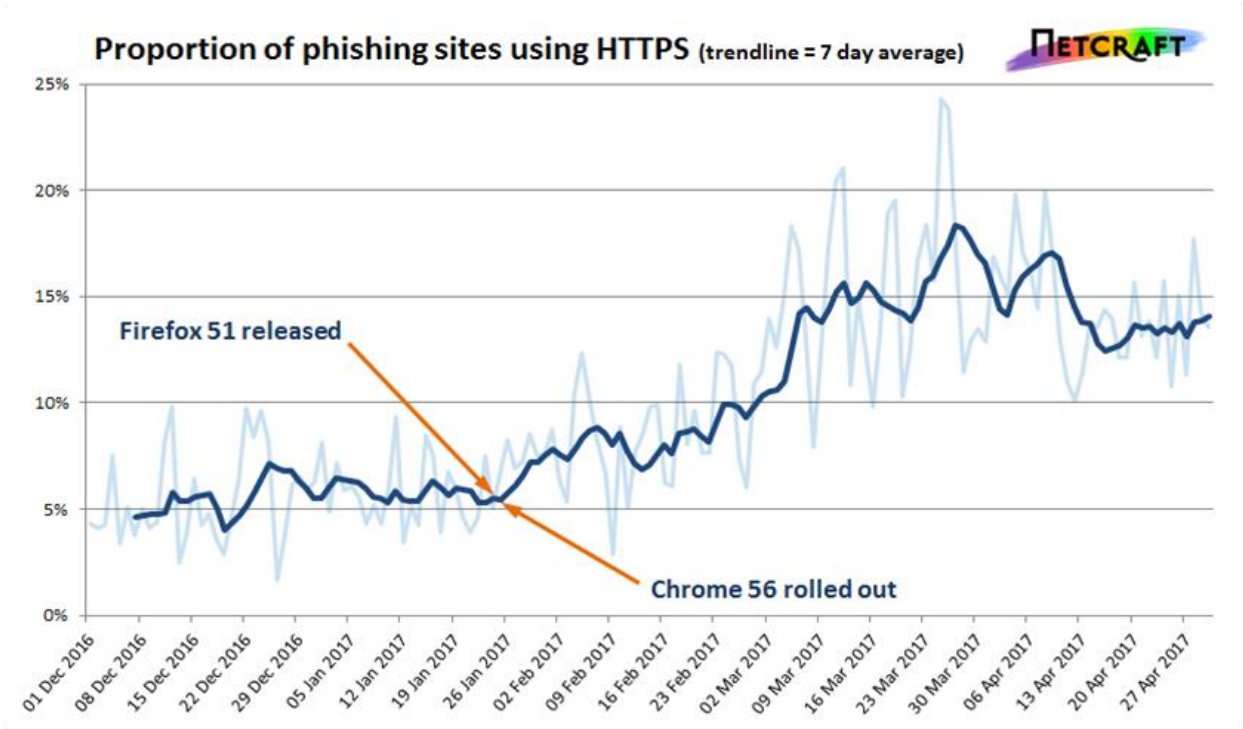
Entrust Datacard and Comodo have worked together to gather data from publicly trusted and valid SSL/TLS enabled phishing sites. This new service has only been running for a few days, but we have preliminary results. The sample that we have analyzed was collected between September 4, 2017 and September 9, 2017 totaling 58,061 records. We double-checked our phishing results against Google's Safe Browsing API and marked the site as phishing if the same URL appeared on both lists.

We were restricted in our study by an access limit for the Google Safe Browsing services that we were using to validate our own phishing results, so we were not able to compare all 58,061 records. (We believe this access issue will be resolved in future datasets.) We did get verification results back for 18,129 records from Safe Browsing. Of the 18,129 records, only 2,148 showed a valid SSL/TLS connection UI.

Total phishing records collected	58,061	
Matched against Google Safe Browsing list	18,129	31.2% records matched with Google safe site
Has a valid publically trusted SSL/TLS certificate	2,148	11.8% of matched sites have valid SSL/TLS certs

The sample size above is large enough to give us a confidence interval of +/- 3%. Additionally, the results above match very closely to the results that Netcraft found on the proportion of phishing sites using https from just a few months ago (see next page):¹

¹ <https://news.netcraft.com/archives/2017/05/17/phishing-sites-react-promptly-to-new-browser-changes.html>



[Reprinted with permission]

Finally, we determined the type of certificates (DV, OV, or EV) used on each of the encrypted phishing sites we found.

4. Our Data

Here are the results of our initial data which show the phishing sites we found with valid SSL/TLS certificates sorted by type, which we are first reporting in this study:

Cert Type	Number of Certs	Percent
EV	0	0.0%
OV	24	1.1%
DV	2124	98.9%
Total	2148	100.0%

Preliminary conclusion: Using these results, it seems our hypothesis that EV sites are safer than OV and DV sites is true. Also, our hypothesis that OV sites are safer than DV sites also appears to be true.

Further Analysis:

Reviewing the Data: DV websites make up the great majority of encrypted websites. How do these raw numbers look when compared to the entire population of certificates on the internet?

Certificate Type	Phishing Sites in Sample	Percent of Total Phishing Sites in Sample	Total Cert Population ²	Percent of Total Cert Population
EV	0	0.0%	186,483	0.85%
OV	24	1.1%	1,151,470	5.22%
DV	2124	98.9%	20,724,383	93.94%
Total	2148		22,062,336	

When we compare the certificate type for the phishing sites in our *sample* against the entire certificate population on the *internet*, the results are revealing:

Certificate Type	(1) Representation of Certificate Type in <u>Total Certificate Population</u>	(2) Representation of Certificate Type Among <u>Phishing Sites in Our Sample</u>
EV	0.85%	0.0%
OV	5.22%	1.1%
DV	93.94%	98.9%

If phishing sites were equally distributed among each of the three certificate types, we would expect the numbers in Columns (1) and (2) to be the *same* – but they’re not.

Instead, this table shows that the percentage of OV phishing sites in our sample was only 1.1% of all phishing sites in the sample, versus what we might have expected (5.22%) based on the representation of OV certs among the total cert population on the internet. This means the number of OV phishing sites in our sample is only 21% of what we might have expected based on the number of OV certificates in the population generally (1.1%/5.22%), so OV sites are safer for users.

Likewise, the percentage of EV phishing sites in our sample was actually 0% versus the EV population of 0.85% among the total cert population on the internet – meaning, the number of EV phishing sites is significantly underrepresented in our sample and much safer for users.

In contrast, the percentage of DV phishing sites in our sample was actually 98.9% versus what we would have expected (93.94%) based on the representation of DV certs among the total cert population on the internet – meaning, the number of DV phishing sites is 105% of the number we would have expected (98.9%/93.94%). Of course, the DV numbers are skewed because they now represent the overwhelming number of certs on the internet.

Based on these comparisons, OV and EV sites today are much safer for users than DV sites. They can be made even safer by the measures we propose below.

Why are we finding phishing for these organization validated (OV) sites?

² Based on Netcraft valid certificate population by certificate type as of August 2017.

We have provided certificate data for the 24 OV sites found to be hosting phishing on [Appendix A](#). There are two chief reasons for OV phishing sites:

Reason 1: Of the 24 OV phishing sites found, 18 (75%) are shared content sites with OV certs that allow users to post phishing content, or shared certificate sites where multiple SANs are listed and one of more of the independent sites included as SANS is flagged for phishing. Here is the breakdown by OV Cert Subject name in our sample:

OV Cert Subject Name	Number of hosted phishing pages found on shared content sites
blogspot.com (various)	6
bontrade.com	4
annova.biz	2
amazonaws.com	1
ixsecure.com	1
designmysite.pro	1
utbilling.com	1
kmajormusic.com	1
tribe-hotel.com	1
Total	18

The reason these 18 sites were marked for phishing breaks down as follows:

Reason marked for phishing	Number of sites
Shared content sites	9
Shared certificate sites	9
Total	18

Here is the data in of one of the shared certificate phishing websites as an example. The Subject in the OV certificate is Incapsula Inc., but the cert then includes 61 SANs (including many wildcards). Incapsula offers various web services, including content delivery – so we assume 60 of the 61 SANs in its OV cert are for customer websites not owned or controlled by Incapsula. In this way, a shared certificate is like a shared content website – a single OV cert will cover multiple independent sites or pages that are not monitored by the Subject of the OV cert (here, Incapsula) and many of which contain phishing material.

In this case, the included SANs bontrade.com was marked for phishing. While using a shared cert is a very efficient way of encrypting multiple independent websites, it isn't really justified when most or all of the SANs in the shared OV cert are actually independent websites – a DV cert would be more appropriate.

Subject: C=US, ST=Delaware, L=Dover, O=**Incapsula Inc**, CN=incapsula.com

X509v3 Subject Alternative Name:

DNS:incapsula.com, DNS:*.aidatraconis.com, DNS:*.aisfl.com, DNS:*.alltoosimple.com, DNS:*.awakenthroughmindfulness.com, DNS:*.bontrade.com, DNS:*.chakra-consciousness.com, DNS:*.cupidintimates.com, DNS:*.emergencycallservice.com, DNS:*.eta.com, DNS:*.fastfocuscareers.com, DNS:*.fitcoachjessica.com, DNS:*.floatlab.com, DNS:*.hg counseling.com, DNS:*.johnsbigdeck.com, DNS:*.manifestabsolutelyanything.com, DNS:*.manifestabsolutelyanything.net, DNS:*.manifestalltoday.com, DNS:*.marlowesmemphis.com, DNS:*.northtexasenergy.net, DNS:*.nutrientgap.org, DNS:*.pathways-care.org, DNS:*.scootebike.com, DNS:*.scriptfruit.com, DNS:*.stephaniestover.com, DNS:*.stgalileo.com, DNS:*.stormteamusa.com, DNS:*.t2hproperties.com, DNS:*.thatslosangeles.net, DNS:*.trinetnetwork.com, DNS:*.wedgwoodbc.org, DNS:*.whales.net, DNS:aidatraconis.com, DNS:aisfl.com, DNS:alltoosimple.com, DNS:awakenthroughmindfulness.com, DNS:bontrade.com, DNS:chakra-consciousness.com, DNS:cupidintimates.com, DNS:emergencycallservice.com, DNS:eta.com, DNS:fastfocuscareers.com, DNS:fitcoachjessica.com, DNS:floatlab.com, DNS:hg counseling.com, DNS:johnsbigdeck.com, DNS:manifestabsolutelyanything.com, DNS:manifestabsolutelyanything.net, DNS:manifestalltoday.com, DNS:marlowesmemphis.com, DNS:northtexasenergy.net, DNS:nutrientgap.org, DNS:pathways-care.org, DNS:scootebike.com, DNS:scriptfruit.com, DNS:stephaniestover.com, DNS:stgalileo.com, DNS:stormteamusa.com, DNS:trinetnetwork.com, DNS:wedgwoodbc.org, DNS:whales.net

Here is a second example to consider. The six blogspot.com OV phishing sites in our sample all come from *one* certificate, but this is a *different* type of shared certificate than the example above (see cert data below). In this case, it's likely that all of the 155 SANs in this single OV cert belong to the Subject of the cert (Google, Inc.), rather than multiple independent SANs owners like the previous example.

However, several of the SANs in this single cert are hosting phishing content. If this cert were revoked as a result of the phishing content on some of the 155 SANs and a DV cert were substituted instead, *all* 155 of the SANs would be moved from OV to DV status at the same time. This is the type of certificate that probably should always be issued as a DV certificate from the start as a matter of good practice.

Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=misc-sni.blogspot.com

X509v3 Subject Alternative Name:

DNS:misc-sni.blogspot.com, DNS:*.au.daily.alpha.blogspot.com, DNS:*.au.gaia.alpha.blogspot.com, DNS:*.au.prod.alpha.blogspot.com, DNS:*.au.weekly.alpha.blogspot.com, DNS:*.blogspot.ae, DNS:*.blogspot.al, DNS:*.blogspot.am, DNS:*.blogspot.ba, DNS:*.blogspot.be, DNS:*.blogspot.bg, DNS:*.blogspot.ca, DNS:*.blogspot.ch, DNS:*.blogspot.cl, DNS:*.blogspot.co.at, DNS:*.blogspot.co.id, DNS:*.blogspot.co.il, DNS:*.blogspot.co.ke, DNS:*.blogspot.co.nz, DNS:*.blogspot.co.uk, DNS:*.blogspot.co.za, DNS:*.blogspot.com, DNS:*.blogspot.com.ar, DNS:*.blogspot.com.au, DNS:*.blogspot.com.br, DNS:*.blogspot.com.by, DNS:*.blogspot.com.co, DNS:*.blogspot.com.cy, DNS:*.blogspot.com.ee, DNS:*.blogspot.com.eg, DNS:*.blogspot.com.es, DNS:*.blogspot.com.mt, DNS:*.blogspot.com.ng, DNS:*.blogspot.com.tr, DNS:*.blogspot.com.uy, DNS:*.blogspot.cz, DNS:*.blogspot.de, DNS:*.blogspot.dk, DNS:*.blogspot.fi, DNS:*.blogspot.fr, DNS:*.blogspot.gr, DNS:*.blogspot.hk, DNS:*.blogspot.hr, DNS:*.blogspot.hu, DNS:*.blogspot.ie, DNS:*.blogspot.in, DNS:*.blogspot.is, DNS:*.blogspot.it, DNS:*.blogspot.jp, DNS:*.blogspot.kr,

DNS:*.blogspot.li, DNS:*.blogspot.lt, DNS:*.blogspot.lu, DNS:*.blogspot.md, DNS:*.blogspot.mk, DNS:*.blogspot.mx, DNS:*.blogspot.my, DNS:*.blogspot.nl, DNS:*.blogspot.no, DNS:*.blogspot.pe, DNS:*.blogspot.pt, DNS:*.blogspot.qa, DNS:*.blogspot.ro, DNS:*.blogspot.rs, DNS:*.blogspot.ru, DNS:*.blogspot.se, DNS:*.blogspot.sg, DNS:*.blogspot.si, DNS:*.blogspot.sk, DNS:*.blogspot.sn, DNS:*.blogspot.tw, DNS:*.blogspot.ug, DNS:*.blogspot.vn, DNS:*.blogspot.com, DNS:*.daily.alpha.blogspot.com, DNS:*.gaia.alpha.blogspot.com, DNS:*.in.daily.alpha.blogspot.com, DNS:*.in.gaia.alpha.blogspot.com, DNS:*.in.prod.alpha.blogspot.com, DNS:*.in.weekly.alpha.blogspot.com, DNS:*.prod.alpha.blogspot.com, DNS:*.weekly.alpha.blogspot.com, DNS:blogspot.ae, DNS:blogspot.al, DNS:blogspot.am, DNS:blogspot.ba, DNS:blogspot.be, DNS:blogspot.bg, DNS:blogspot.ca, DNS:blogspot.ch, DNS:blogspot.cl, DNS:blogspot.co.at, DNS:blogspot.co.id, DNS:blogspot.co.il, DNS:blogspot.co.ke, DNS:blogspot.co.nz, DNS:blogspot.co.uk, DNS:blogspot.co.za, DNS:blogspot.com, DNS:blogspot.com.ar, DNS:blogspot.com.au, DNS:blogspot.com.br, DNS:blogspot.com.by, DNS:blogspot.com.co, DNS:blogspot.com.cy, DNS:blogspot.com.ee, DNS:blogspot.com.eg, DNS:blogspot.com.es, DNS:blogspot.com.mt, DNS:blogspot.com.ng, DNS:blogspot.com.tr, DNS:blogspot.com.uy, DNS:blogspot.cz, DNS:blogspot.de, DNS:blogspot.dk, DNS:blogspot.fi, DNS:blogspot.fr, DNS:blogspot.gr, DNS:blogspot.hk, DNS:blogspot.hr, DNS:blogspot.hu, DNS:blogspot.ie, DNS:blogspot.in, DNS:blogspot.is, DNS:blogspot.it, DNS:blogspot.jp, DNS:blogspot.kr, DNS:blogspot.li, DNS:blogspot.lt, DNS:blogspot.lu, DNS:blogspot.md, DNS:blogspot.mk, DNS:blogspot.mx, DNS:blogspot.my, DNS:blogspot.nl, DNS:blogspot.no, DNS:blogspot.pe, DNS:blogspot.pt, DNS:blogspot.qa, DNS:blogspot.ro, DNS:blogspot.rs, DNS:blogspot.ru, DNS:blogspot.se, DNS:blogspot.sg, DNS:blogspot.si, DNS:blogspot.sk, DNS:blogspot.sn, DNS:blogspot.tw, DNS:blogspot.ug, DNS:blogspot.vn, DNS:blogspot.com, DNS:daily.alpha.blogspot.com, DNS:gaia.alpha.blogspot.com, DNS:prod.alpha.blogspot.com, DNS:weekly.alpha.blogspot.com

Possible solution: There is really no good reason for a shared content site to have an OV or EV certificate, or for multiple independent sites to have a single shared OV or EV certificate, as the individual pages on the site (or the multiple SANs in the shared cert) are independent and under the control of *others* not named as the Subject of the identity cert. A shared cert with SANs owned by a single owner is different, but if some of the SANs are hosting phishing content then an OV or EV cert may also be inappropriate.

For this reason, the shared content site/shared cert owner's name probably should *not* show in the Subject field of the certificate encrypting those pages and sites – instead, we should limit shared-content sites and shared certificates to DV certs only and not permit these independent pages/sites to operate under a single OV cert. In this test, *that simple step would have removed 18 of 24 OV phishing sites (75%) from the study*, and greatly reduced the number and percentage of OV phishing sites in the population of encrypted sites, thereby making OV sites even safer for users than today.

Reason 2: Of the remaining six OV phishing sites we found, *all* had been compromised. A phisher had taken over part of the site's directory and posted phishing content on the site where owner would not notice - the phishing URLs appeared to be "orphaned" URLs that are not reachable by scanning the site. We assume that none of these six website owners have posted the phishing content themselves or are aware it's there. Also, we found more than one phishing URL for some of the sites at different times, so

it's possible that these sites are compromised for weeks or months at a time and used over and over again (different pages) by phishers without the site owner ever being aware.

Possible solution: Once a compromised OV site is found, the owner could be notified and told that its OV cert will be revoked but can be replaced immediately with a DV cert. Once the site has been hardened and made more secure (without phishing content), the owner can reapply for another OV or EV cert.

Our original assumption that identity websites (OV and EV) don't want to be phishing sites appears to be borne out by this initial data. We found no EV sites with phishing in our sample,³ and the limited OV sites with problems appear to fall into the two categories of shared content sites/shared certificates (where the owners presumably are not policing the content that is posted), or compromised sites (where the owners likely are not aware that a phisher has taken over a portion of the site and is using it as a base for a phishing page). Presumably, we can get the cooperation of these website owners once we let them know how their sites are being misused.

5. Second Part of the Solution

The data indicates that identity sites (OV and EV) are much safer and more trustworthy for users than DV sites, but how can users *know* when they are at an identity site? The current browser UIs don't show any difference between DV and OV sites, and many users are unaware of how to identify an EV site today. Plus, there is great variation in the UI among browsers, leading to user confusion. See <https://casecurity.org/browser-ui-security-indicators/>





Our proposed solution is to create a unified set of UI design principles that would be adopted by the browsers (subject to their own unique designs) that would tell users when they are at identity sites (the safer sites), and to work on widespread user education. Here are the basic elements:

- Unencrypted http sites and broken https sites would display **warnings** in the UI
- DV sites would no longer receive the “padlock” or any other words or symbols in the UI – they would have no UI security symbol, and would be treated as the new normal / new minimum security state. *This by itself is potentially the most effective thing we can do to protect users from phishing in the short term.*
- The padlock would be reserved for identity sites (OV and EV), with OV sites showing a basic black (hollowed out) icon and showing the current URL. EV sites would show a **green solid padlock, confirmed identity data, and country of operation** in the URL bar to indicate they are the very safest websites for users.

Here is a possible prototype of these new unified set of UI design principles that would implement this reassignment of current symbols and build upon the greater safety of identity websites. This plan could

³ It's likely that some EV sites have been compromised by phishers and will be found in future samples – see this Netcraft article from 2011: <https://news.netcraft.com/archives/2011/12/30/phishing-sites-using-extended-validation-ssl.html> - but the incidence of website compromise is probably less that for OV websites because EV certs tend to be used by larger enterprises, and they may have websites that are better protected against compromise. Also, shared content sites tend not to use EV certs.

be implemented in stages, with the padlock and other text removed *now* for DV sites, and other new icons and text applied over time to OV and EV sites.

Universal Browser UI – Ideal for Desktop and Mobile	
HTTPS EV	 Citigroup Inc. 
HTTPS OV	 bing.com
HTTPS DV & Minor Security Issues	example.com
HTTP & Broken HTTPS	 Not secure

Once browsers agree to a universal UI for Desktop and Mobile environments, then the ecosystem can move forward to help users understand what to look for as they interact with a web site.

6. Conclusion

We support a 100% encrypted web and see an opportunity to bring multiple players together to address these issues, including CAs, website owners, browsers, enterprises, and other service providers. Agreeing on common browser UI changes and dropping the DV UI will give the ecosystem a proactive way to better determine if a site is phishing or not for almost 99% of all phishing activity. Also, by stopping the practice of issuing OV or EV certificates to shared websites (including shared OV certs with multiple SANs), we could begin to address roughly 75% of the remaining problem.

All decisions about security in browsers, including a common UI, should be data-driven and research based, with the research carefully designed to ask the right questions that will help us make the right decisions for user security. We want to contribute to this data-driven effort by compiling useful data on about the relative safety of identity websites and anonymous websites, and then designing the best methods for alerting users on the nature of the sites they are visiting. These early results are encouraging, and give us some good guidance on an effective plan to reduce website phishing.

For more information on using identity to protect users, see studies at <https://casecurity.org/identity/>

APPENDIX A

URL	Cert Issuer	Cert Type	Phishing Reason
1. https://artistsdollars.c13.ixsecure.com/ctent/dropbox/proposal/	COMODO RSA Organization Validation Secure Server CA	OV	Shared Content
2. https://s3-us-west-2.amazonaws.com/fg-business-data/sellerpermit/207085/SEXYBVDS%20INVOICE.html	DigiCert Baltimore CA-2 G2	OV	Shared Content
3. https://8y5k0e42h2nywfgme9vrszw78.designmysite.pro/	GeoTrust SSL CA - G3	OV	Shared Content
4. https://2egjddcdf23.blogspot.de/	Google Internet Authority G2	OV	Shared Content
5. https://clicktoenjoy15.blogspot.com.es/	Google Internet Authority G3	OV	Shared Content
6. https://clicktoenjoy15.blogspot.com.tr/	Google Internet Authority G3	OV	Shared Content
7. https://beingames4u.blogspot.com.eg/2017/01/2017-16_1.html	Google Internet Authority G3	OV	Shared Content
8. https://berita-tanahmelayu.blogspot.ru/2015/09/nabil-rajalawak-terima-jemputan.html	Google Internet Authority G3	OV	Shared Content
9. https://jaixpalcsinghzrajivi.blogspot.de/	Google Internet Authority G3	OV	Shared Content
10. https://bontrade.com/drvdox/google/01ae4acb1722618be50b731e69548e5f/	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
11. https://utbilling.com/admin/ckeditor/kcfinder/upload/files/paypalmain.html	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
12. https://www.annova.biz/boxMrenewal.php	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
13. https://www.annova.biz/boxMrenewal.php?Email=abc@example.com&.rand=13vqcr8bp0gud&lc=1033&id=64855&mkt=en-us&cbcxt=mai&snsc=1	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
14. https://www.bontrade.com/drvdox/google/01ae4acb1722618be50b731e69548e5f/verification.php	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
15. https://www.bontrade.com/drvdox/google/1c3988328589afafd54f4b4fb623e12f/verification.php	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
16. https://kmajormusic.com/SMG/ay01/ay01/ay01/index.html	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
17. https://www.tribe-hotel.com/u26/account/USAA%20%20Welcome%20to%20USAA.htm	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
18. https://www.bontrade.com/drvdox/google/b5af28183e67a15cd3c97dbf0f40a081/verification.php	GlobalSign CloudSSL CA - SHA256 - G3	OV	Shared Certificate
19. https://www.intracomer.com.mx/intranet/archFtpApache/832_36.htm	Symantec Class 3 Secure Server CA - G4	OV	Compromised
20. https://www.ilona.com/older/Gdocrox/Gdoccc/	USERTrust RSA Organization Validation Secure Server CA	OV	Compromised
21. https://www.ilona.com/older/Gdocrox/Gdoccc/index.php	USERTrust RSA Organization Validation Secure Server CA	OV	Compromised
22. https://www.ilona.com/wcmilona/wp-includes/SimplePie/Data/	USERTrust RSA Organization Validation Secure Server CA	OV	Compromised

23. https://www.ilona.com/wcmilona/wp-includes/SimplePie/Data/f1c21a18c910166820e80259bd6e91bb/	USERTrust RSA Organization Validation Secure Server CA	OV	Compromised
24. https://ilona.com/older/Gdocrox/Gdoccc/	USERTrust RSA Organization Validation Secure Server CA	OV	Compromised