E-Government Program
OREGON.GOV

2020

Guidance on
Domains, Paths, Redirects & HTTPS/Transport Layer Security (TLS) Certificates

for E-Government Program Services

E-Government Program Guidance 1

Version 2.1
Date: November 24, 2020

For additional information, please contact**:**
Oregon.Egov@das.oregon.gov

ENTERPRISE
information services

DOMAINS, REDIRECTS & HTTPS/TLS CERTIFICATES

Introduction

This document outlines the E-Government Program's recommended guidance to state agency management and Single Points of Contacts (SPOCs) for making informed decisions on the use of paths and subdomains of the Oregon.gov domain, external vanity domains, and associated HTTPS/Transport Layer Security (TLS) certificate needs for websites served by E-Government Program services through NIC Oregon**.**

Oregon.gov custom paths and subdomains are a practical and secure way of providing easy to remember website URLs[1] for your agency's important pages or documents. **These paths and subdomain names are the preferred solution for state websites need to market shorter URLs.**

In the rare case where there is sound business justification, and the use of an external, vanity domain (e.g. .COM and .ORG) is acceptable; however this is not recommended as it incurs additional financial burden, technical overhead, and may confuse visitors whether the URL leads to an official government website. When deciding whether to use an Oregon.gov path, subdomain, or a vanity domain, consider whether your business needs can be met by a regular Oregon.gov page name or subsite name on your agency's website.

Historically, the E-Government Program has facilitated many custom Oregon.gov paths or subdomains, and external domain redirects. In July 2018, web browsers began recommending that sites use HTTPS/TLS certificates whenever possible. Visiting sites that are not HTTPS-enabled display indicators and may prompt full-page warnings that the website is not secure as a result. In addition, URLs previously set up to redirect from external, non-Oregon.gov domains (e.g. .COM and .ORG) that do not have a TLS certificate applied may display security errors[2]**.**

Our recommended guidance regarding paths, subdomains, and external vanity domains is being updated to better reflect current security standards established by Enterprise Information Services (EIS) Cyber Security Services. As a result, the E-Government Program will continue facilitating the creation of paths and subdomains on the Oregon.gov domain and provide HTTPS/TLS certificates and redirects to E-Government Program-hosted websites; however, the program will no longer renew or pay for any domains that are not a part of the Oregon.gov domain nor cover their TLS certificates.

To ensure your agency's business can continue uninterrupted, it must request a path or subdomain on the Oregon.gov domain or purchase a TLS certificate(s) for all its non-Oregon.gov (vanity) domains. Failure to provide a TLS certificate for an external vanity domain may result in a security warning to visitors.

[1] For additional information about URLs, see Appendix D.

[2] For a sample error message, see Appendix C.

Contents

Guidance

The E-Government Program recommends retiring the use of vanity domain names and strongly encourages the use of an Oregon.gov path (e.g. oregon.gov/yourpath) or subdomain name (e.g. yoursubdomain.oregon.gov). Unlike other top-level domains which are used by non-profits and commercial entities, visitors associate a .GOV domain with a government website. Government use of non-government domains causes confusion and mistrust of government services. There is also a large, annual cost for non-government domain names, whereas there is no cost to members of the E-Government Program who use an Oregon.gov custom path or subdomain.

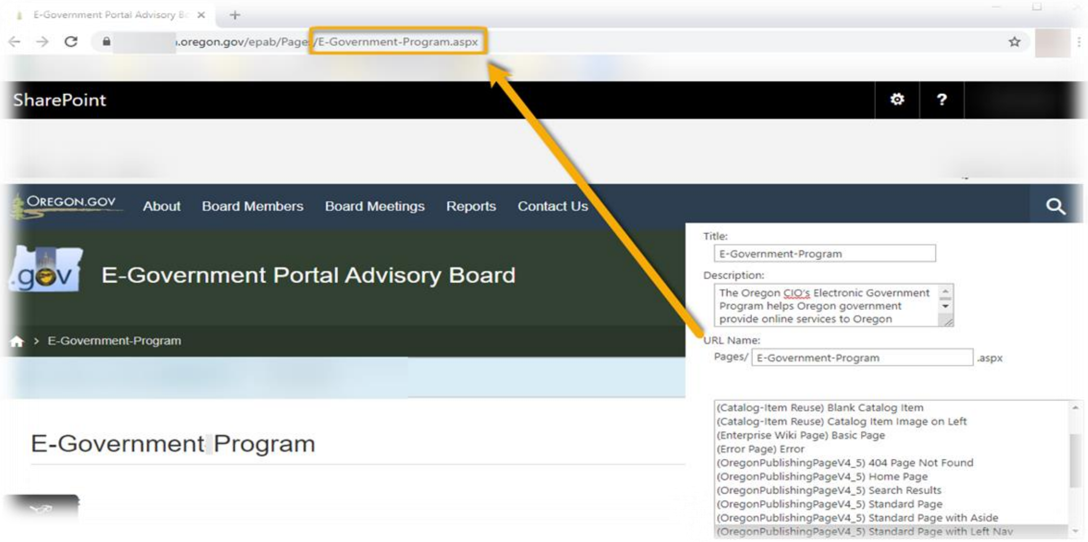
If agency's management and/or SPOC insist on the use of a non-Oregon.gov vanity domain name for business reasons (such as a domain/URL which is well-established), it is highly recommended to acquire a TLS certificate to ensure the safety and security of visitors' information. It is, however, recommended to begin a strategy to retire that domain/URL in favor of a custom Oregon.gov path or subdomain.

The following are **three recommended options**, and two other options which **are not** recommended:

OPTION 1: CREATE AN EFFECTIVE OREGON.GOV PAGE OR SUBSITE NAME

https://oregon.gov is the state's main website domain name. Surveys indicate it is widely recognized as the State of Oregon's official online presence. Therefore, when creating content, a well-chosen subsite or page name can avoid necessitating the use of a custom path, subdomain or vanity URL (see **Figure 1**) entirely. When deciding on a subsite or page name, choose a short, relevant series of words which either include the title of the subsite/page or its main topic, while avoiding using too many words. Always convert any spaces to hyphens, as this improves recognition, sharing, and search engine optimization. This option saves time and prevents the agency from having to submit a ticket and/or to purchase and maintain a TLS certificate for a subdomain or vanity domain name.

Figure 1: Creating a marketable Oregon.gov page name



.oregon.gov/epab/Pages/E-Government-Program.aspx

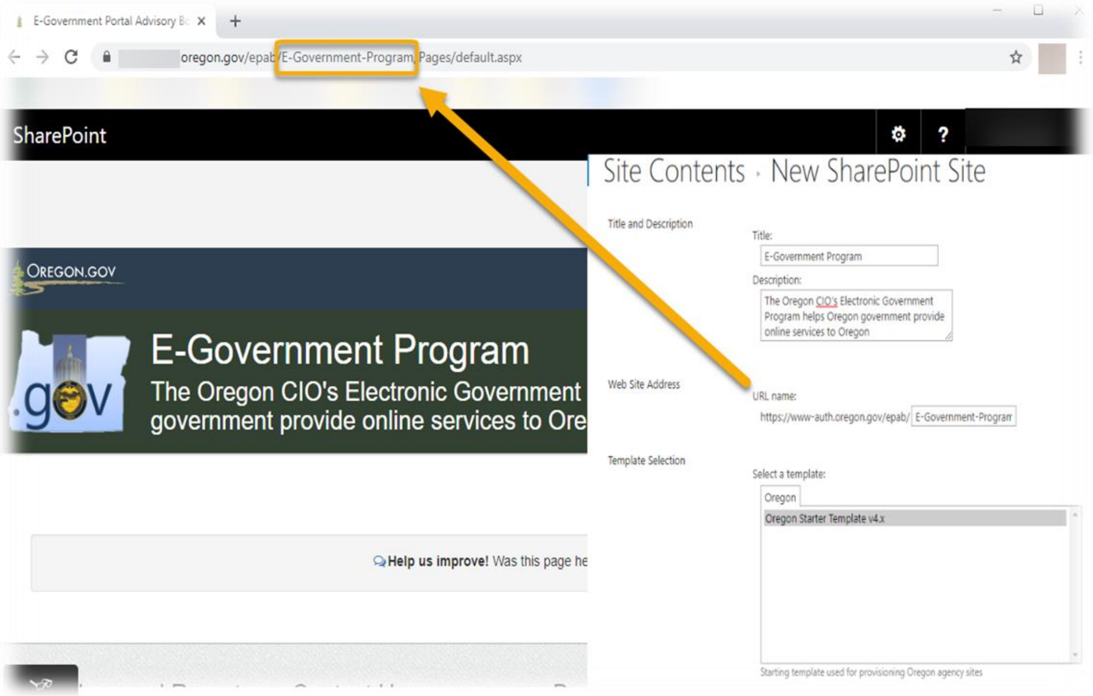
Title: E-Government-Program

Description: The Oregon CIO's Electronic Government Program helps Oregon government provide online services to Oregon

URL Name: Pages/ E-Government-Program .aspx

(Catalog-Item Reuse) Blank Catalog Item
(Catalog-Item Reuse) Catalog Item Image on Left
(Enterprise Wiki Page) Basic Page
(Error Page) Error
(OregonPublishingPageV4_5) 404 Page Not Found
(OregonPublishingPageV4_5) Home Page
(OregonPublishingPageV4_5) Search Results
(OregonPublishingPageV4_5) Standard Page
(OregonPublishingPageV4_5) Standard Page with Aside
(OregonPublishingPageV4_5) Standard Page with Left Nav

Figure 2: Creating a marketable Oregon.gov subsite


E-Government Portal Advisory Bo
SharePoint
OREGON.GOV
E-Government Program
The Oregon CIO's Electronic Government
government provide online services to Ore
Help us improve! Was this page he

oregon.gov/epab/E-Government-Program/Pages/default.aspx

Site Contents › New SharePoint Site

Title and Description

Title: E-Government Program

Description: The Oregon CIO's Electronic Government Program helps Oregon government provide online services to Oregon

Web Site Address

URL name: https://www-auth.oregon.gov/epab/ E-Government-Program

Template Selection

Select a template: Oregon

Oregon Starter Template v4.x

Starting template used for provisioning Oregon agency sites

OPTION 2 : REQUEST A CUSTOM OREGON.GOV PATH AND A REDIRECT (FROM THE E-GOVERNMENT SERVICE DESK)

If an agency requires a shorter URL than the full path to a page/document/subsite on its own website, it is best practice to first consider requesting a custom Oregon.gov path (*e.g. oregon.gov/yourpath*). Implementing an Oregon.gov custom path does not require an additional HTTPS/TLS certificate and visitors will associate the redirect with Oregon State Government. An agency can request a new, custom path at no cost barring it matches the following syntax: **oregon.gov/* and has not been previously reserved**.

To request a custom path, visit https://servicedesk.oregon.gov/redirect and open a new service desk ticket. Be sure to include the desired path and the page/document where the visitor should be redirected to. An example might be:

"Please create the custom path oregon.gov/[yourPathHere] and redirect it to oregon.gov/myAgency/pages/myPage.aspx."

Note: The custom path is not case sensitive; however, your destination may be. Contact your technical team or hosting provider for more details.

OPTION 3 : REQUEST A CUSTOM OREGON.GOV SUBDOMAIN NAME (FROM STATE DATA CENTER) AND A REDIRECT (FROM THE E-GOVERNMENT SERVICE DESK)

Another option for a shorter URL is the use of an Oregon.gov subdomain (e.g. yoursubdomain.oregon.gov). This option requires additional setup and it is appropriate for some scenarios. A likely scenario is when a custom subdomain must also support/enable the use of other custom paths (*see Option 2*). For example, https://servicedesk.oregon.gov is the homepage for the service desk and https://servicedesk.oregon.gov/redirects leads to a specific form on the service desk website. **Unless there is a business reason, Option 1 should be used when possible over Option 3.** Contact the E-Government Service Desk staff if you are unsure.

Implementing an Oregon.gov subdomain does not require a new HTTPS/TLS certificate and visitors will associate the redirect with Oregon State Government. An agency can request a new subdomain at no cost as long as it matches the following syntax: ***.oregon.gov**. In order to request a subdomain, contact the State Data Center at https://www.oregonsdc.org. Be sure to include the desired subdomain name and the location of the CNAME[3] record. An example might be:

"Please create the subdomain [yourSubdomainHere].oregon.gov and create a CNAME record pointing it to prd-sp.oregon-gl.com."

[3] Canonical Name record (CNAME) is a type of resource record in the DNS that maps one domain name to another.

Upon receiving confirmation the requested subdomain name has been created by the State Data Center, the agency must also submit a redirect request to the E-Government Service Desk[4].

To request a redirect, visit https://servicedesk.oregon.gov/redirect and open a new service desk ticket. Be sure to include the newly-created subdomain name and the page/document where the visitor should be redirected. An example might be:

"I have received confirmation from the State Data Center that my new Oregon.gov subdomain name [yourSubdomainHere].oregon.gov has been created. Please create a new redirect rule to oregon.gov/myAgency/pages/myPage.aspx. I need this redirect in place by [MM/DD/YYYY]"

Redirect requests are fulfilled during maintenance windows which occur roughly every other week. Please plan for a two weeks for the redirect to be implemented.

OPTION 4 : PURCHASE A VANITY DOMAIN NAME AND HTTPS/TLS CERTIFICATE (BOTH INCUR AN ANNUAL COST)

Ultimately, the agency must make a business decision whether to create (or continue the use of) a vanity domain name. The E-Government Program does not recommend this approach and will only accommodate a redirect from external domain names when a TLS certificate is purchased **through the State Data Center**. TLS certificates purchased from external resources will not be installed on E-Government Program-affiliated web servers due to security risks. Failure to purchase a TLS certificate may result in the user experiencing a failure to redirect or a security warning during the redirect, depending on the choice of web browser. See Appendix C as an example of a Google Chrome browser security warning.

OPTION 5 : VANITY DOMAIN NAME WITHOUT HTTPS/TLS CERTIFICATE

The E-Government Program will no longer redirect vanity domain names without HTTPS/TLS certificates, because of security concerns. If the agency would like to keep HTTP redirects, the agency must institute their own redirect via their domain name registrar or through a server redirect managed by the agency or the State Data Center. In consultation with the State's Cyber Security Services, the E-Government Program does not recommend this option and encourages the agency to speak with its own Information Security professionals and its Senior IT Portfolio Manager from the Project Portfolio Performance (P3) team.

[4] For additional information on how to submit a ticket to the E-Government Service Desk Oregon Service Desk, see Appendix E.

Appendix A – Benefits of using HTTPS across your website[5]

WHAT IS HTTPS?

While you are probably familiar with the HTTP part of a URL, you may not be as familiar with HTTPS. The added 'S' stands for Secure. This means the website uses a protocol called Transport Layer Security (TLS) to encrypt information going between the site and the user's computer. If an attacker intercepts this information, they can't read or change it.

You may also hear people commonly refer to HTTPS as SSL, which is an outdated version of TLS.

WHAT HTTPS LOOKS LIKE IN A BROWSER

You can tell when a website's information is encrypted by looking at the address bar at the top of your browser. Depending on which browser you use, there may be a green padlock or shield icon on the left or right of the website address, and often the word 'secure' next to it. It is important to note that this means that your connection with the website is secure, rather than the website itself.

THE BENEFITS OF USING HTTPS

There are several benefits to adding HTTPS to your website, and it does not cost much to implement.

Trust in your website

The public recognizes that a website marked secure is more trustworthy than one without. It shows your website's visitors — and potential customers — that you take their privacy seriously. According to Google's security blog, 81 of the top 100 websites globally use HTTPS by default.

However, some scammers take advantage of this by adding HTTPS to their website, to make it seem more legitimate. Remember that the green padlock shows that information is sent securely between the site and your computer. It does not mean that the website is safe.

No browser warnings

If your website does not have HTTPS, your visitors may get a warning message telling them that your site is not secure.

For example, when you visit a website or web page that doesn't use HTTPS on Chrome, it warns you that the connection isn't secure. A 'not secure' message displays in the address bar next to the URL. Chrome

[5] "Benefits of Using HTTPS across Your Website." *CERT NZ*, www.cert.govt.nz/business/guides/secure-your-website/benefits-of-making-your-website-use-https/.

started showing this message in October 2017, and Google's security blog reported that visits to these pages dropped by 23% over the following six months.

Improved security

Information on a webpage goes through several points between a browser and a web server. An attacker could intercept the information at any of the points along this path. By encrypting the information using TLS, you can stop them:

- Stealing your customer's data, or
- putting their own data onto your website.

If your site uses HTTP instead of HTTPS, an attacker could insert ads or malware into any of your webpages without your knowledge. Your customers could also unintentionally download this malware to their computers. This is known as a 'man-in-the-middle' attack.

Better search ranking

Search engines include the use of HTTPS as a factor when they are ranking your website in search results. This means that using HTTPS gives your website a boost in search results over similar sites that do not.

As more sites implement HTTPS over time, it will become obvious if your website does not have it — and it'll be harder for your customers to find.

IMPLEMENTING HTTPS

To make your website use TLS you will need a digital certificate, called a TLS certificate (also commonly referred to as an SSL certificate).

If you have technical support staff, talk with them about moving to HTTPS. If you manage your own website, ask your hosting company if they provide SSL/TLS certificates. If they do, they can probably help you implement it as well.

They will need to:

- Get and implement an SSL/TLS certificate for you
- Add a permanent redirect to your site (from HTTP to HTTPS)
- Update any links to third party scripts to include HTTPS.

You will need to:

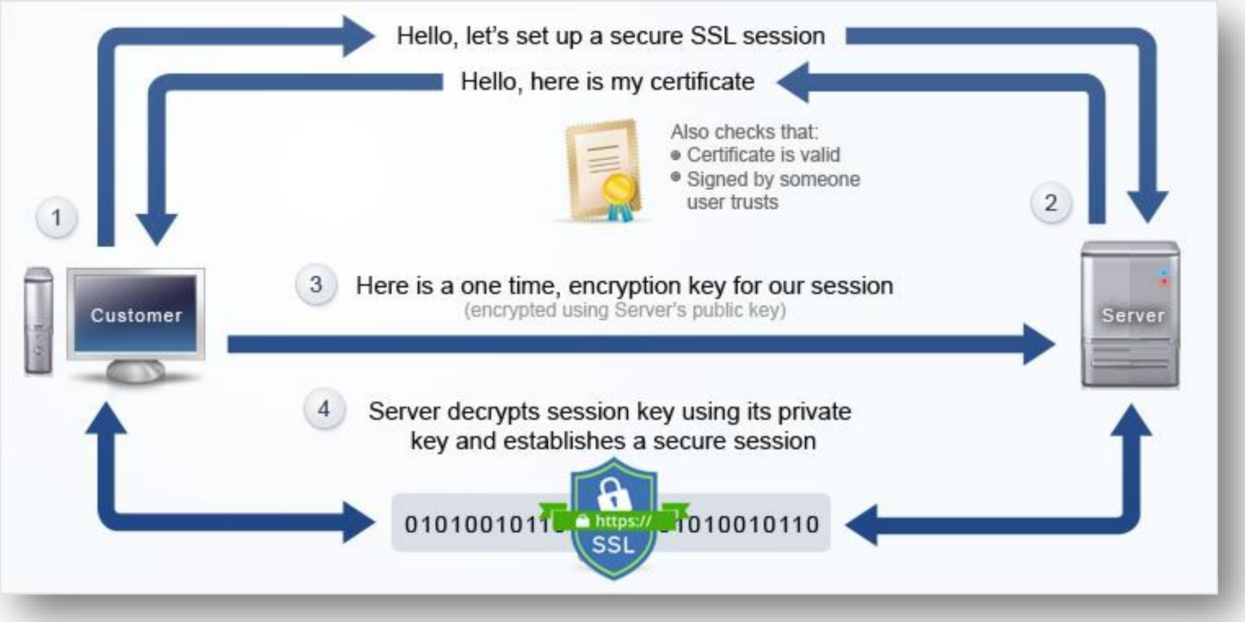
- Update any links inside the content to include HTTPS. This includes links to images, downloads, and tools
- Set a reminder for a month before the certificate expires. This will make sure you renew it in plenty of time, and avoid letting it run out.

Appendix B - Definitions

TRANSPORT LAYER SECURITY

Transport Layer Security, or TLS, is an updated, more secure, version of a Security Socket Layer (SSL). TLS is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website (see **Figure 3**). A visitor to a web page will know it has a TLS if it includes *https://* in the URL. See Appendix A for additional information regarding the benefits of using HTTPS.

Figure 3: How TLS works

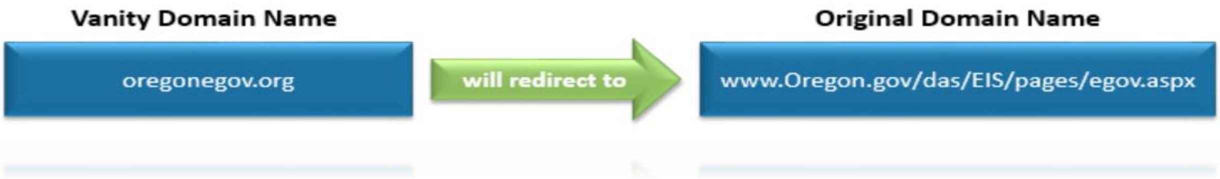

Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
Certificate is valid
Signed by someone user trusts
1
2
Customer
Server
3
Here is a one time, encryption key for our session
(encrypted using Server's public key)
4
Server decrypts session key using its private key and establishes a secure session
0101001011
1010010110
https://
SSL

©TosHost LTD

VANITY DOMAIN NAME

The core function of a vanity domain name is to help simplify a complicated URL. The goal is to help the potential visitors to remember the site URL (see **Figure 4**).

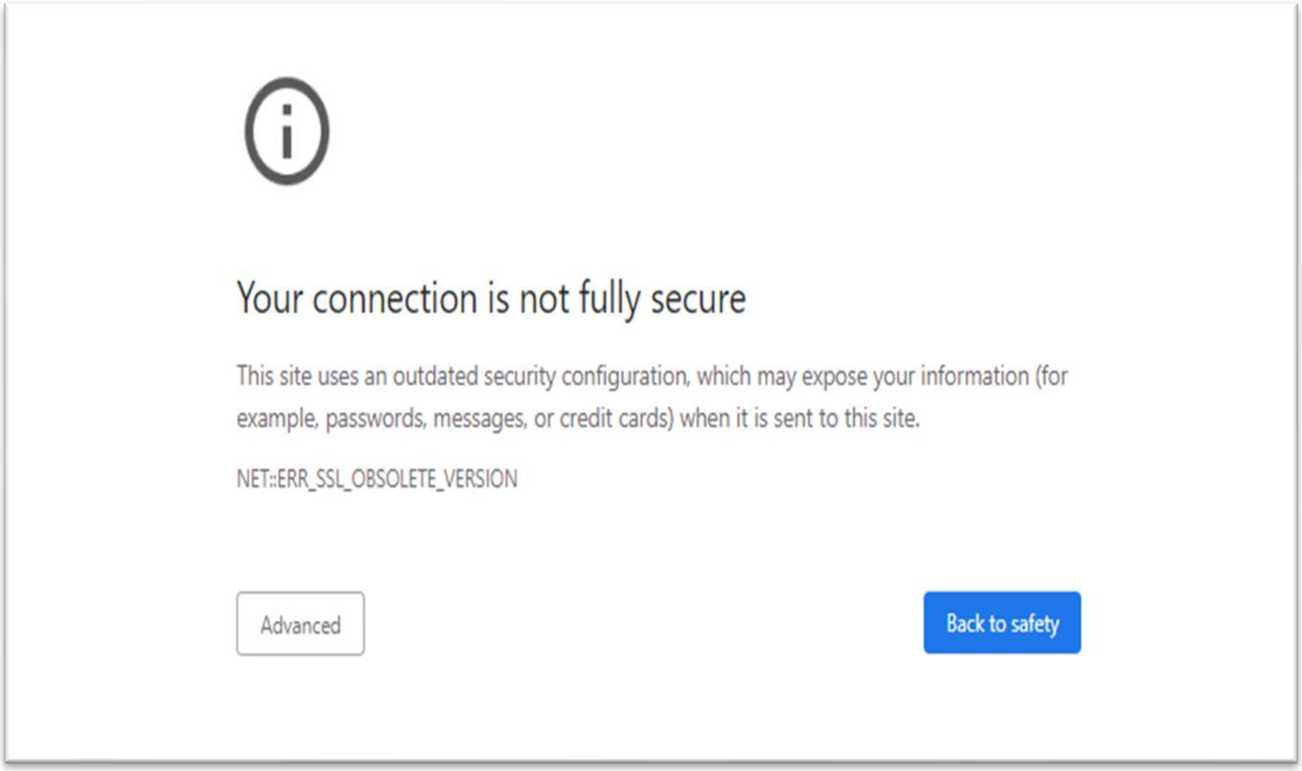
Figure 4: Example of a vanity domain name



Appendix C – Sample Error Message

If the vanity domain does not have a TLS certificate, visitors may experience an error message. For example, as seen in **Figure 5**, in order for visitors to be successfully redirected from https://www.error.org to the original domain name, www.error.org needs to have a valid TLS certificate.

Figure 5: Example of sample error message if vanity domain does not have a TLS certificate



Your connection is not fully secure

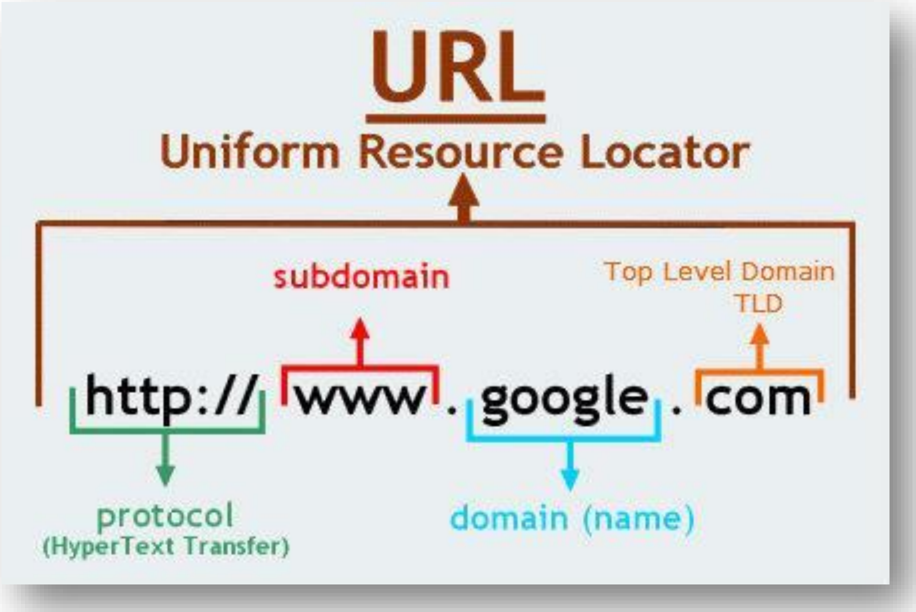
This site uses an outdated security configuration, which may expose your information (for example, passwords, messages, or credit cards) when it is sent to this site.

NET::ERR_SSL_OBSOLETE_VERSION

Appendix D – Uniform Resource Locator (URL)

Anytime someone clicks a link on a website or types in a web address into the browser, it is a Uniform Resource Locator (URL). A web browser requests pages from web servers by using a URL.

Figure 6: Uniform Resource Locator syntax rules

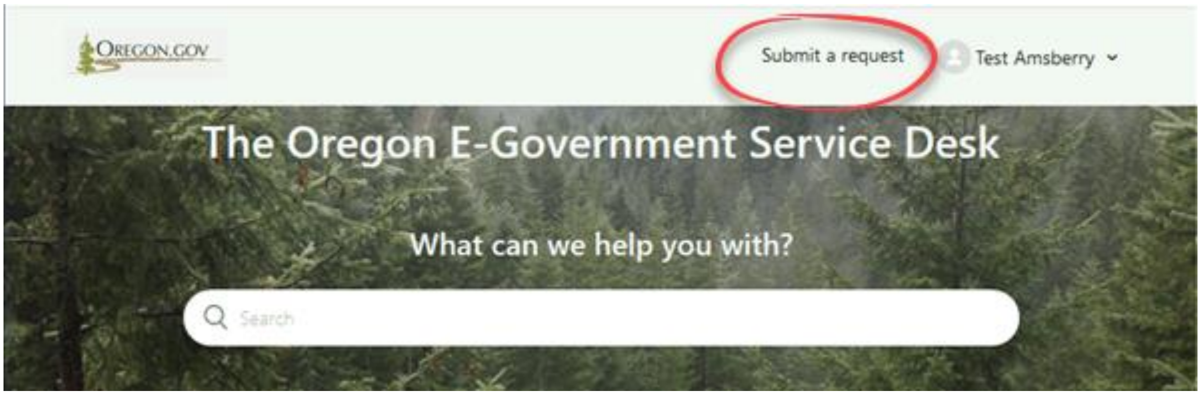


©CodebridgePlus

Appendix E – Submitting an E-Government Service Desk Request

You will need a Service Desk login and password to submit a request. You can set one up from the main login screen at https://servicedesk.oregon.gov if you do not already have one.

Once logged in, use the 'Submit a request' link in the upper right of the homepage.


OREGON.GOV
Submit a request
Test Amsberry
The Oregon E-Government Service Desk
What can we help you with?
Search

Complete the ticket form labeled Redirect Request and select “Submit.” This creates a ticket at the E-Government Service Desk. You will receive automatic email notifications when the ticket is created and whenever it is updated. You can review the status of your submitted tickets at any time by selecting your name in the upper right corner and selecting the “My Activities” menu option.

Frequently Asked Questions

Does buying one TLS certificate cover all of the vanity domains?

No. TLS certificates are usually provided for a single top-level domain (as well as its www subdomain variant); however, some special certificates (commonly called wildcard certificates) cover a single domain its subdomains. For example, the wildcard TLS certificate purchased for Oregon.gov its www.Oregon.gov variant and all subdomains of oregon.gov such as govspace.oregon.gov, data.oregon.gov, etc. TLS certificates with multi-domain (SAN) certificates may be purchased, but these are non-standard offerings.

Can an agency request an Oregon.gov subdomain that our vanity domain name already redirects to?

Yes.

How much does a TLS certificate cost?

Pricing from TLS certificates can vary. You will want to contact your agency helpdesk to inquire about the pricing options. Please understand that there is an annual cost to any TLS certificate in addition to its initial cost.

For web sites that are not hosted on Oregon.gov, but that need a vanity domain name, would programs purchase and manage it themselves?

Yes. Agency programs would continue to purchase and manage these types of vanity domain names.

If we switch to the Oregon.gov domain, will there be a temporary redirect if visitors type in the old address?

Yes, but it will display an insecure warning.