InfoSec – April 2019

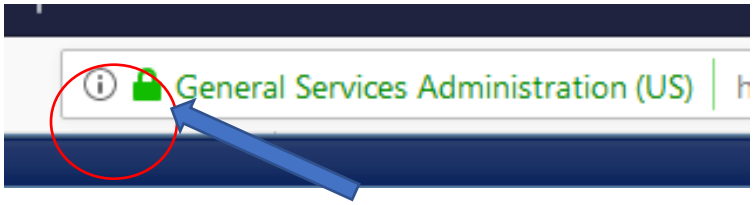
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

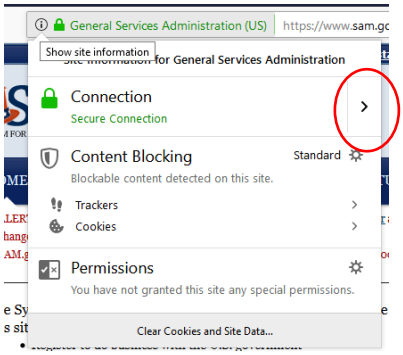
In this edition of the WPI InfoSec bulletin:

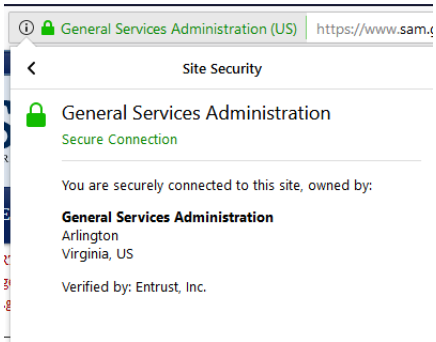
1. **How to determine if the .gov site you are visiting is legitimate**
2. **Understanding Website Certificates**
3. **Why should .gov domains be trusted?**
4. **What is so important about the "s" in https?**

This web site looks like the SAM registration site but is it?

Can I or should I trust the padlock – see How to Check a Certificate in the NCIS Security tip.







Who is Entrust Inc and should they be trusted? See How to Check a Certificate in the following Security tip.

Understanding Website Certificates

Anyone who surfs the web and is interested in computer security can benefit from understanding a little more about the URL that they enter or the link that they select.

The following security tip from NCIS provides a brief overview of the following three items.

1. What are website certificates
2. Can you trust a certificate?
3. How do you check a certificate?

The following is a link to this Security tip: https://www.us-cert.gov/ncas/tips/ST05-010

InfoSec – April 2019

.Gov Domains – to trust or not to trust?

Bona fide government services should be easy to identify on the internet, so GSA's Office of Information Integrity and Access oversees the .gov top-level domain (TLD).

We ensure that .gov domains are easy to obtain and resolve globally, and work to make the .gov zone a trusted, safe space. We support, develop, and implement strategic and operational actions to strengthen .gov. We also monitor and report on policy compliance and best practices for Federal websites and digital services.

Copied from: https://www.gsa.gov/policy-regulations/policy/information-integrity-and-access/gov-domain-services

DotGov – As stated on the website https://home.dotgov.gov "It should be easy to identify governments on the internet. .gov is the top level domain for US-based government organizations.

Why is the "s" in https://www.sam.gov important?

HTTPS (Hypertext Transfer Protocol Secure) is a protocol that gives users a level of security and privacy when connecting to websites and web services.

The internet's fundamental design means that both visitors and website owners have very little control over where communications will travel, or whose devices will carry that communication. To ensure secure communication across the internet, traffic must be encrypted all the way from visitors' devices to the website owners' devices – and that's exactly what HTTPS does. Without HTTPS, hostile networks can inject malware or tracking beacons, or otherwise monitor or change visitor interactions online.

Without HTTPS, website visitors have no guarantees about what happens as they browse the web. Without HTTPS, a visitor's communication with a website can be modified or monitored by anyone or anything "between" them and the website they're visiting. The attacker could be someone using that coffee shop WiFi (or the coffee shop itself), or it could be someone who's hacked an old, out-of-date load balancer which website traffic is flowing through on its way around the internet.

Copied from: https://home.dotgov.gov/management/preloading/

WPI InfoSec Bulletin

Information security has always been a critical element to businesses involved in government contracting. The importance of information security cannot be overstated. Businesses not only need to manage paper, prints and information accessed and used by employees, members of the supply chain and customers, they must also manage their digital information and develop sounds and compliant cyber programs. These programs and policies will continued to be a priority for contractors.

The purpose of this bulletin is to be an information resource for individual involved with developing, managing or integrating requirements of programs such a CUI, ITAR, EAR and JCP. It is also our hope that our readers will share information, their thoughts and experiences/suggestions. We realize the power and value of a network and would like to tap into the knowledge and resources of our readers. Our goal is simple - to benefit all. ***We encourage questions and have established the following email address for this purpose - infosec@wispro.org or call Marc Violante at 920-456-9990.***