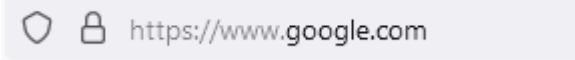
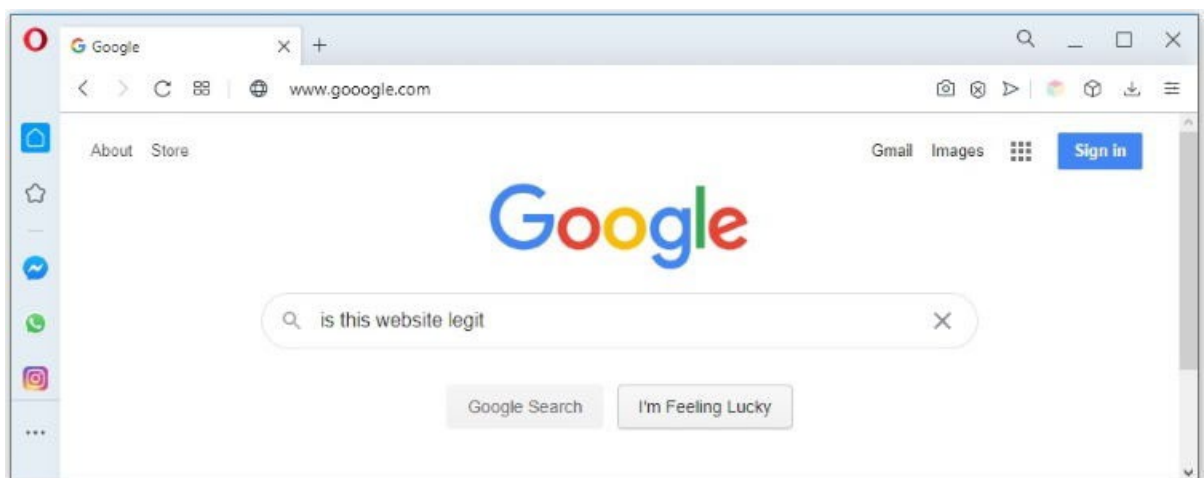


In this journal we are asked if we can spot three fake websites and compare the three fake websites to three real websites, plus showcase what makes the fake websites fake. The first and perhaps easiest way to tell that a website is not legitimate is when the domain name doesn't match the official company domain. A common tactic is to use a URL that is like the legitimate web address or to include part of the legitimate URL as part of the fake domain name. For example: <https://www.paypal.com> is the official site while paypal.com.security.alert.confirmation-manager-security.com uses first and second-level sub-domains to mimic a valid TLD.

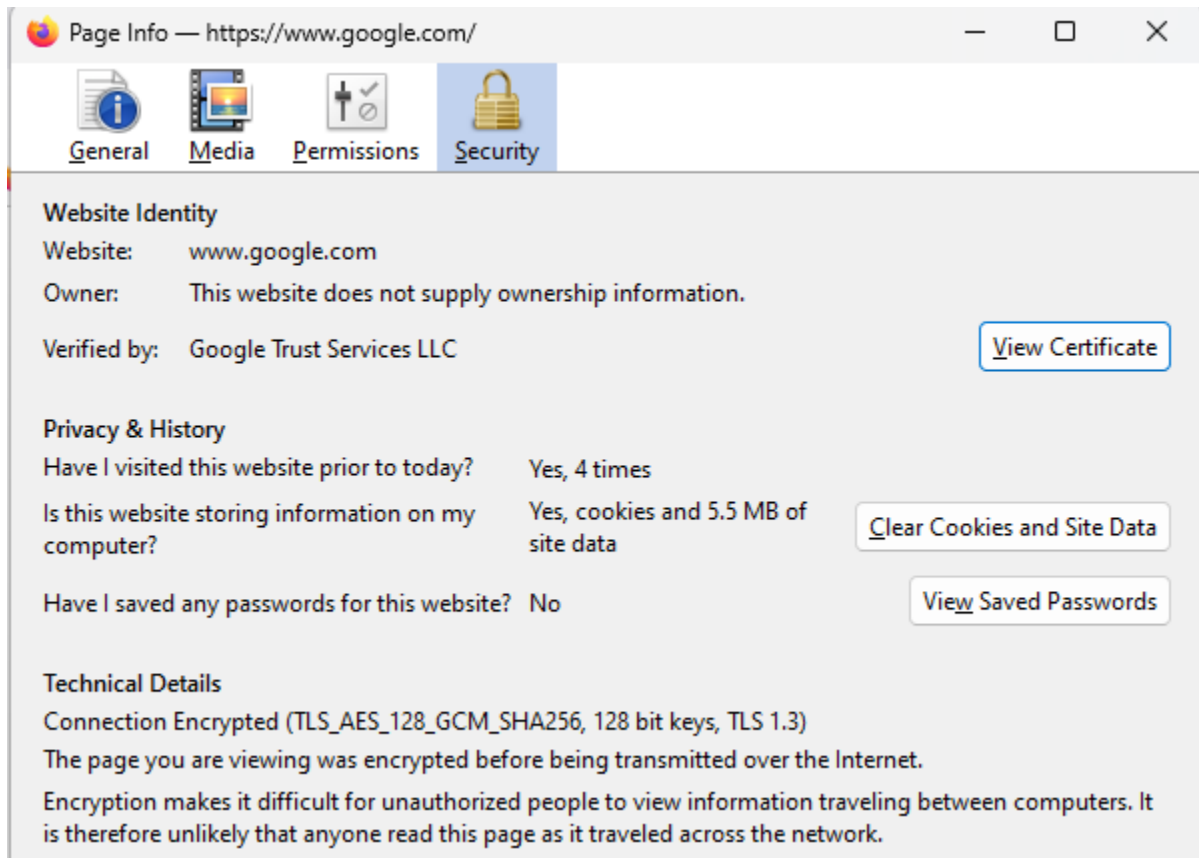
Second, check the URL to ensure that the website has an SSL certificate, indicated by a padlock icon in the address bar. All web browsers (Safari, Firefox, Google Chrome) allow you to check if a site has a valid security certificate by looking for a padlock symbol next to the URL in

the address bar.  the URL will start with <https://>

(hypertext transfer protocol secure) vice http which is not secure. Fake websites will often use http in the URL as the example below shows.





Unfortunately, cybercriminals can mimic valid SSL's so in some instance it would be wise to right click on the padlock icon to check the details of the SSL certificate and see if it was issued from a trusted source.




Finally, you can also use <https://whois.domaintools.com/> to check how long a website has been active, who the registrar is, list of name servers, the hosting Ip address and Ip location. The example below is the Whois record for <http://www.amazon.com>. With an original registration date of 11-01-1994, hosted within the United States. The next example below this one is for a domain: amazon-activity.com. This fake website was created on 11-26-2023 and is 87 days old, the Ip address and hosting location are in Frankfurt, Germany.

Domain Profile

Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.208.685.1750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	10,704 days old Created on 1994-11-01 Expires on 2024-10-30 Updated on 2023-05-16
Name Servers	NS1.AMZNDNS.CO.UK (has 4,734 domains) NS1.AMZNDNS.COM (has 3 domains) NS1.AMZNDNS.NET (has 1 domains) NS1.AMZNDNS.ORG (has 15 domains) NS2.AMZNDNS.CO.UK (has 4,734 domains) NS2.AMZNDNS.COM (has 3 domains) NS2.AMZNDNS.NET (has 1 domains) NS2.AMZNDNS.ORG (has 15 domains)
IP Address	3.163.18.236 - 11 other sites hosted on this server
IP Location	 Oregon - Portland - Amazon.com Inc.
ASN	 AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And No Website
IP History	688 changes on 688 unique IP addresses over 20 years
Registrar History	2 registrars with 2 drops
Hosting History	5 changes on 5 unique name servers over 20 years

Whois Record (last updated on 2024-02-21)

Domain Profile

Registrar	Streamline Domains, LLC IANA ID: 2273 URL: http://www.networksolutions.com Whois Server: whois.web.com domain.operations@web.com (p) +1.877.381.2449
Registrar Status	ok
Dates	87 days old Created on 2023-11-26 Expires on 2024-11-26 Updated on 2024-02-01
Name Servers	7513FAF1.VERIFY.HN (has 482,574 domains) NS1.DAN.COM (has 2,579,663 domains) NS2.DAN.COM (has 2,579,663 domains)
IP Address	3.64.163.50 - 3,181,717 other sites hosted on this server
IP Location	 Hessen - Frankfurt Am Main - A100 Row Gmbh
ASN	 AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And No Website
IP History	10 changes on 10 unique IP addresses over 9 years
Registrar History	4 registrars with 3 drops
Hosting History	17 changes on 11 unique name servers over 16 years

Whois Record (last updated on 2024-02-21)

