How to verify website authenticity?

Posted on November 14, 2019

The Internet is an ever-growing ocean of knowledge, opportunities, and conveniences. At the same time, immense swaths of that ocean are filled with fake websites, scams, and increasingly efficient and sophisticated ways to steal the 21st century's greatest treasure - personal information.

In this guide, we will show you 10 tricks that can help you verify website authenticity. Admittedly, the simple tricks cannot ensure 100% safe browsing experience. This is why this article also included sophisticated verification measures used by the most reputable cybersecurity tools designed for in-depth, sophisticated analysis of fraudulent websites.

Simple Tricks to Verify Website Authenticity

Whether you are doing your regular online shopping, looking for software or gathering information, there are a few ways to check whether you are dealing with a fake website right off the bat.

1. Check the connection type

You don't have to be a pro to understand the website's connection type. All you have to do is click on the URL and check whether the site in question has an "HTTP" or "HTTPS" tag. The "https" tag is more secure compared to "HTTP".

HTTP is an abbreviation for "hypertext transfer protocol," which enables your web browser and server to communicate by exchanging data. HTTP enables the connection on demand, and doesn't spend time securing the way information is exchanged. This makes the basic protocol vulnerable to interception and alteration.

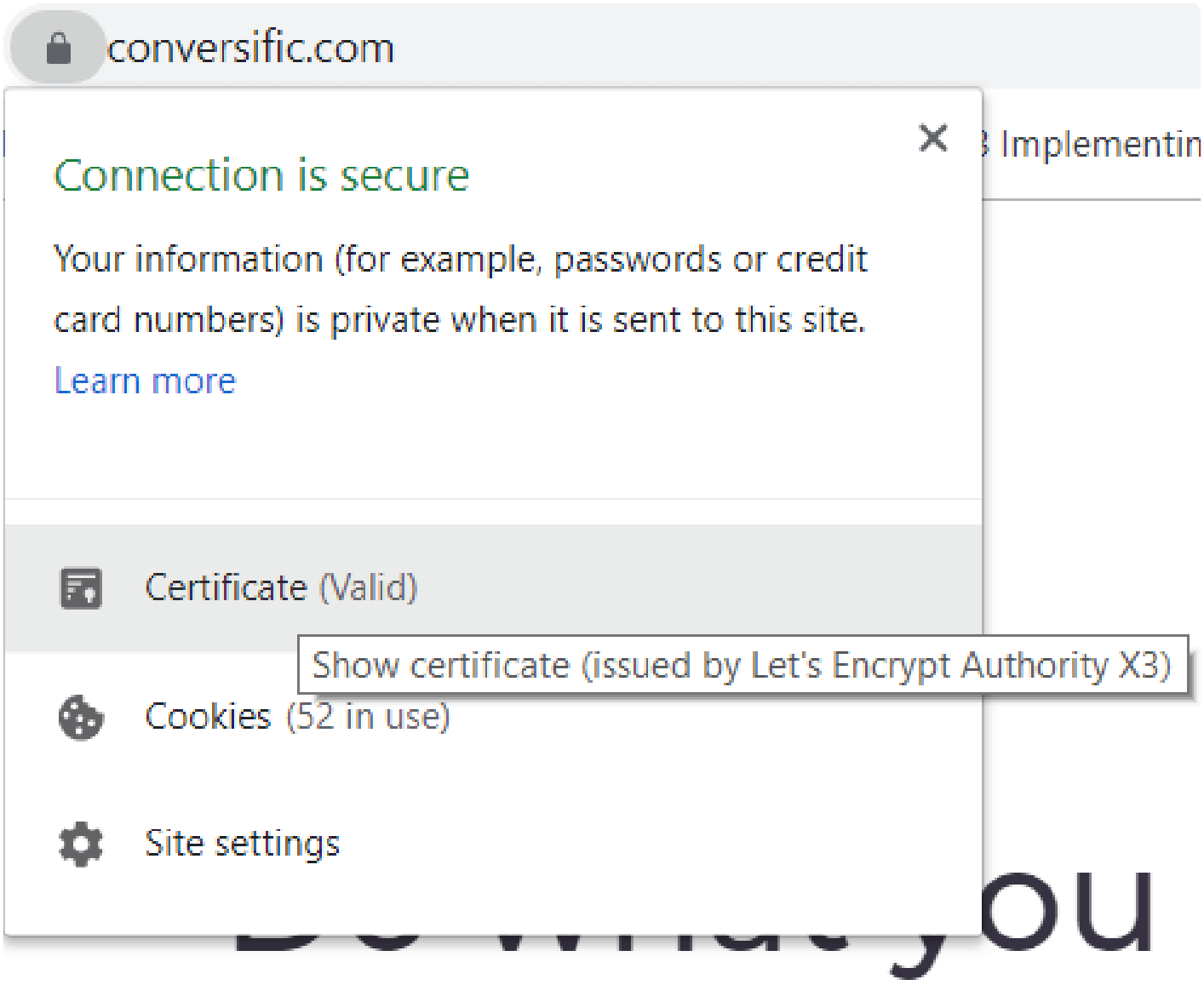
HTTPS, on the other hand, uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) that creates an encrypted connection between a server and a browser. Encryption connection is based on an algorithm that scrambles or encrypts data and then uses a key for the receiving party

to unscramble or decrypt the information.

Long story short, whatever you share via an encrypted connection, remains between you and the receiving party. HTTPS is an absolute must on any page where you share your personal information, contact information, credit card numbers, etc.

2. Check the site's security

Another way to check the site’s security status is to click on the padlock icon in the address bar. This will display information about the site’s connection security, the validity of its SSL certificate and the identity of its issuer.



Security certificate issuers require website owners to provide evidence that the web domain is their legal property. On top of that, businesses also have to present legal documents such as permits, tax forms or charters.

Are these two steps a 100% guarantee that you are dealing with a legitimate website? Unfortunately, they are not.

Online scams can actually take place on websites with valid SSL certificates. With a little help from technologies such as Cloudflare, SSL certificates can be obtained and implemented for free. So what are some other ways to verify website authenticity?

3. Check the URL

While you're still inspecting the address bar, don't just look for the padlock and the "https" sign. Look at the name of the domain. Does it contain any unusual symbols, too many dashes, or suspicious attempts at mimicking big brands' or other businesses' names and products?

For example, this website looks like your reputable online shopping haven Amazon. It even has an HTTPS connection! Until...you take a closer look into its domain name and realize that it has one extra "x" at the end of "amazon".

Image source: Digileads

It's a minor detail, which is not always easy to notice, but things like this are a dead giveaway that you are dealing with a scam.

Another thing you should look at in the URL is top-level domain extensions, the ones that are at the end of the website address. Not all of them are easy to obtain. For example, the following domain extensions have been identified as common extensions for spam websites:

- .biz
- .info
- .science
- .stream
- .men
- .party
- .top
-

On the other hand, here are some of the more reliable domain extensions based on their rankings by Google.

- .edu
- .gov
- .com
- .org
- .net
- .io

The first two are the most difficult to obtain since they are used by educational and governmental institutions. The rest have also been proven to have a decent track record.

Sub-domain, the famous “www” is somewhat trickier to notice because browsers no longer automatically display them in the address bar. This is where more sophisticated scammers jump in

with subdomain hijacking - like this one:

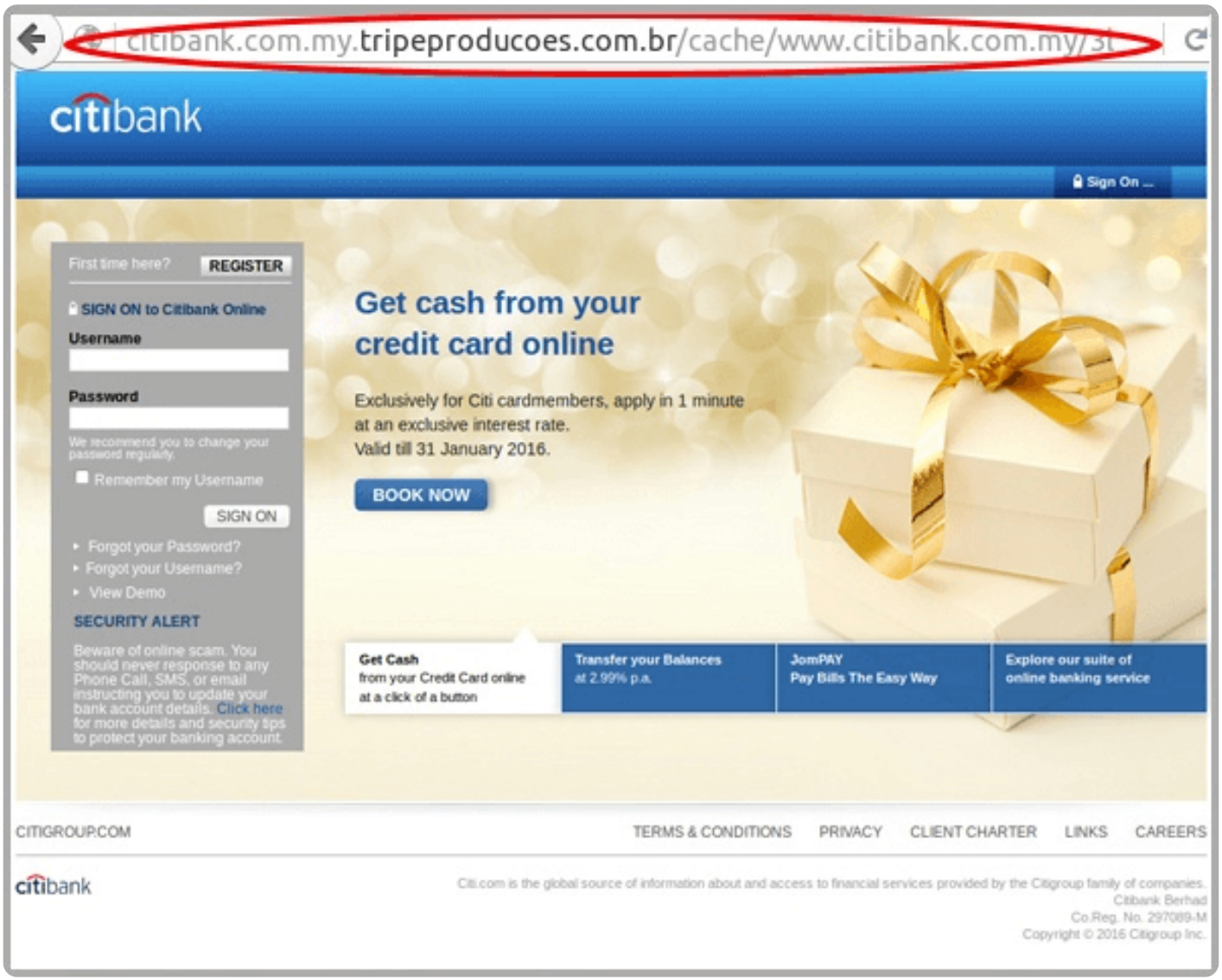


Image source: MailGuard

If you expand the URL in the address bar, you will notice that the subdomain in this URL is “citibank.com.my” while the actual domain name and sub-domain are “tripeproducoes.com” and “br” respectively. Yes, that is a full-on phishing website.

4. Check website content

Perusing an entire website takes time, but it can be a fairly reliable way to verify website authenticity.

For a shopping site, some of the green lights would be clear product descriptions, high-quality product photos, and transparent pricing. Reputable businesses also have clearly stated refund policy, shipping info, and privacy policy. If you are looking at some other type of business or organization, a good way to check their credibility is to look for their partners or trust seals.

Trust seals are often used by software companies as both a way to boost their credibility and market the product. Trust seals are logos of clients who endorse business or organization in question. They look like this:

Finally, check the contact information. Legitimate websites, businesses, and organizations have no reason to hide. Their contact page thus will include their full name, representatives, physical address, or an email address for customer support and inquiries.

Pay attention to the email address domain - inspect it in the same way you did with the URL. For example, john.doe@quhgruls.com is surely not the address that will provide you with an answer or refund – not ever. You can also use online tools that can help you with email verification, but we will get into more details about them in one of the following sections.

Other fake website red flags include poor grammar, spelling mistakes, gibberish in website copy or blog content, as well as a multitude of intrusive ads.

5. Check the website's social proof

Bad news travels fast in the digital world, so checking the users' feedback can also help you verify website authenticity. Google the organization! While some businesses have plenty of reviews automatically displayed by Google, some require a bit of deeper digging.

In that case, you can google the organization with an added keyword such as "reviews," "scam," etc. It could help you run into social media feedback or blog posts and comments about the website.

Finally, it is no secret that reviews can be bought. Even on reputable and real Amazon, up to 70% of the reviews are fake - so imagine how it can be elsewhere.

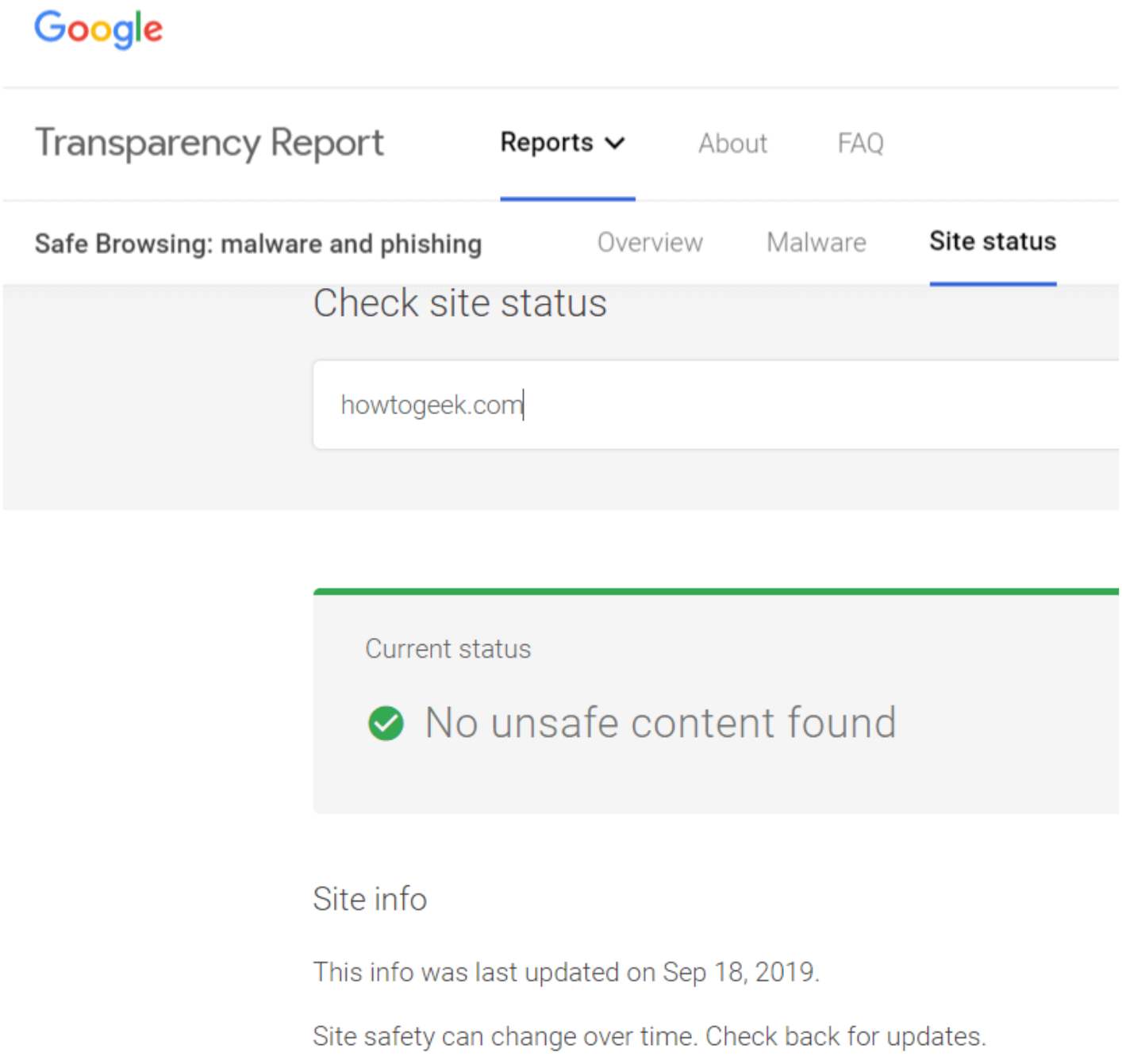
So, we're still in a deadlock. Algorithms and users are getting smarter and more cautious, but scammers are catching up. With a little bit of tech-savvy, they can run a website that looks completely credible and reliable. What happens then?

6. Google Safe Browsing Transparency Report

Online scams and cyber-attacks are not in Google's best interests, which is why their algorithms for spotting fraudulent websites are getting better every day. In fact, they are examining hundreds of thousands of URLs as you're reading this, accumulating billions of addresses in its database.

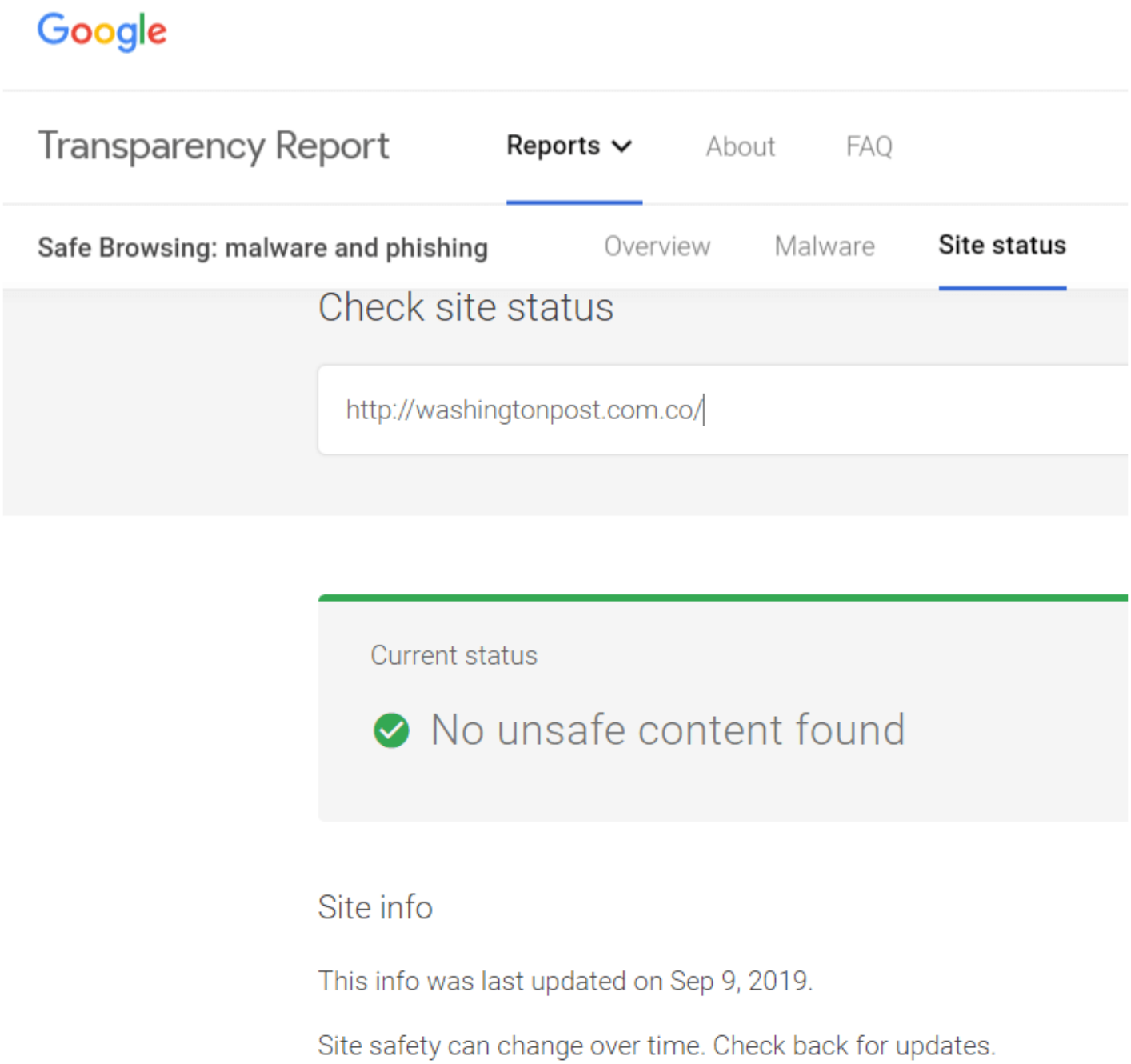
Google Safe Browsing Transparency Report enables you to check the website's credentials by simply pasting the URL into the search bar. Google compiles the report by scanning sections of their web index to identify potentially compromised websites. They test them by using a virtual

machine to see if the machine gets infected.



Now, Google is good at what it does - but the vast digital sphere can let quite a few malicious websites slip. For example, we ran a website “washingtonpost.com.co” through the safe browsing

report. The website was identified as a fake news website which was mimicking the existing website of Washington Post. It no longer exists, but according to Google Report, it is alive, fine and dandy.



What does this mean? It means that at the moment, Google is good at spotting phishing sites, malware or compromised security. However, its transparency check is limited to the technical aspects of website safety, and it does not address all considerations that confirm website authenticity.

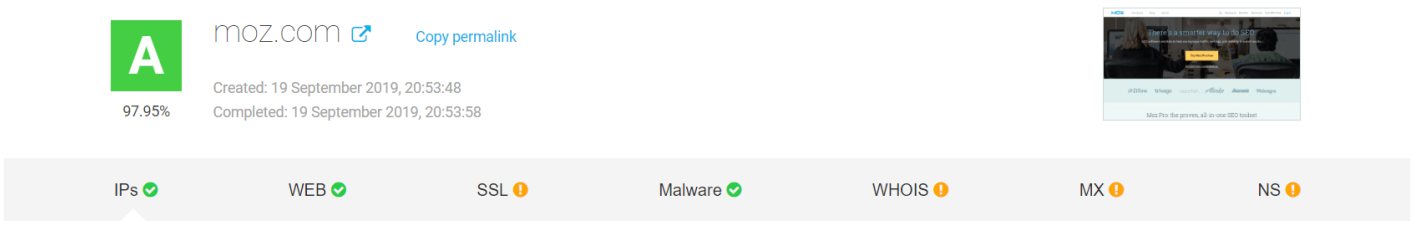
Sophisticated Tricks to Verify Website Authenticity

By this point, you may feel frustrated, thinking: “How am I ever going to be sure I am dealing with a safe website?” The usual checks sometimes simply aren’t enough to verify that the website is safe. In those cases, we recommend taking your time to run an in-depth analysis with a little help from reputable online tools laser-focused on cyber threats and intelligence.

You’ve probably heard about the famous Whois XML API that has been tracking website safety for over a decade. Their database holds more than one billion records and covers a whopping 99.5% IP addresses currently in use. In time, WHOIS developed tools adjusted to various individual and business needs - and here’s how they can help you verify website authenticity.

7. Use Threat Intelligence API

Go to Threat Intelligence API and paste target domain or IPv4 address to run a full, in-depth report on website safety. We ran a report for Moz, a popular SEO tool.



While the website scores a solid 97.95% safety score, you can also take a look at some of the site's weak security spots. If you want more details about them, all you need to do is simply click on the issue.

SSL vulnerabilities

Self-signed certificate	OK	CA-signed certificate
Supported protocols	OK	Your server supports protocols:
		SSLv3 - not supported
		TLSv1.0 - not supported
		TLSv1.1 - not supported
		TLSv1.2 - supported
		SSLv2 - not supported
Supported cipher suites	OK	No suboptimal cipher suites found
SSL compression	OK	Disabled
HTTP Public Key Pinning Extension	Warning	Headers not set
Force HTTPS connections	OK	Yes
Heartbeat extension	Warning	Disabled
Heartbleed vulnerability check	OK	OK

In the IP resolution section, you can see the main infrastructure servers, known subdomains, and connected domains.

IPs ✓ WEB ✓ SSL !

Known subdomains

academy.moz.com	104.17.50.95	Build report
analytics.moz.com	104.17.50.95	Build report
apidash.moz.com	104.17.50.95	Build report
apiwiki.moz.com	104.17.50.95	Build report
beta.moz.com	104.17.50.95	Build report
cs.moz.com	104.17.50.95	Build report
devblog.moz.com	104.17.50.95	Build report
freshwebexplorer.moz.com	104.17.50.95	Build report
go.moz.com	104.17.50.95	Build report
guides.moz.com	104.17.50.95	Build report
localapp.moz.com	104.17.50.95	Build report
pro.moz.com	104.17.50.95	Build report
ranktracker.moz.com	104.17.50.95	Build report
sandbox.localapp.moz.com	104.17.50.95	Build report
sandbox.moz.com	104.17.50.95	Build report

A threat Intelligence API report also includes:

- Website analysis
- SSL certificate analysis
- Malware detection
- WHOIS record
- Mail servers analysis
- Name servers analysis

Seems like a piece of cake? It should because it is - at least for an individual user looking to run a quick check on a website they stumbled into. But what happens if you have to verify website authenticity on a larger scale? You turn to API solutions and these tips, depending on the scale of analysis your business requires.

8. Check SSL certificate configuration and chain

We've already explained why clicking on the green padlock is a good quick check but it doesn't guarantee that you're dealing with a safe website. The only way to be completely sure is to analyze SSL configuration and chain.

Using SSL Configuration Analysis API, you can establish and test the SSL connection to the host and analyze how it is configured. This will allow you to understand who issued, verified and signed the certificate, as well as the validity period of SSL certificate, supported protocols, extensions, and vulnerabilities.

```
{
  "hasWarnings": true,
  "testResults": {
    "validFrom": {
      "status": "OK",
      "details": [
        "Valid from 2017-10-17 00:00:00"
      ]
    },
    "validTo": {
      "status": "OK",
      "details": [
        "Valid until 2020-10-16 23:59:59"
      ]
    },
    "crlCheck": {
      "status": "OK",
      "details": [
        "CRL URL: http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl",
        " - Status: ok",
        " - Last update: Dec 14 12:00:41 2017 GMT",
        " - Next update: Dec 18 12:00:41 2017 GMT"
      ]
```


Further focus on SSL certificate chain can also reveal valuable information behind the website, such as the country, province, city, organization, address and business category of the subject using the certificate. You can learn whether the certificate in question is used for its intended purposes, as well as its position in the certificate chain hierarchy (end-user, intermediate or root).

9. Check domain infrastructure and reputation

If you want to check which domains are risky and prone to being compromised or mimicked, Domain Infrastructure Analysis API can help you analyze their track record based on the target domain name. It will provide you with a report on its web, mail, and name servers, as well as

subdomains. Each individual host from the list comes with detailed information including IP address, geolocation, and subnetwork information.


```
[
  {
    "domainName": "helsinki.fi",
    "resourceType": "web",
    "ipv4": "128.214.222.24",
    "geolocation": {
      "city": "Helsinki",
      "country": "FI",
      "latitude": "60.1756",
      "longitude": "24.9342",
      "postalCode": "00100",
      "region": "Uusimaa",
      "timezone": "Europe\/Helsinki"
    },
    "subnetwork": {
       "name": "RIPE-ERX-128-214-0-0",
       "ipAddressesRange": "128.214.0.0 - 128.214.255.255",
       "country": "",
       "lastUpdateDate": ""
    }
```

```
{
  "domainName": "adc-vip3.it.helsinki.fi",
  "resourceType": "www.web",
  "ipv4": "128.214.189.90",
  "geo": {
    "city": "Helsinki",
    "country": "FI",
    "latitude": "60.1756",
    "longitude": "24.9342",
    "postalCode": "00100",
    "region": "Uusimaa",
    "timezone": "Europe\/Helsinki"
  },
  "subnetwork": {
    "country": "",
    "inetnum": "128.214.0.0 - 128.214.255.255",
    "netname": "RIPE-ERX-128-214-0-0",
    "lastUpdateDate": ""
  }
```


This data can help you conduct a more detailed domain reputation analysis.

When analyzing a domain name or an IPv4 address, a tool like Domain Reputation API provides you with a score calculated according to a multitude of factors, including:

- Website's content

- Relations to other domains
- Host configuration
- Domain's SSL certificates
- Presence in malware data feeds
- Domain’s WHOIS track record
- Domain’s mail servers
- Domain's IP addresses

This is an example of the quick calculation, but you can also opt for more detailed reports.

Sample output


```
{
    "reputationScore": 97.51,
    "testResults": [
        {
            "test": "Name servers configuration meets best practices",
            "warnings": [
                "Some name servers are located on a single ASN: ns68.domaincontrol.com - AS26496, ns67.
            ]
        },
        {
            "test": "SOA record configuration check",
            "warnings": [
                "The minimum TTL is 600. Recommended range is [3600 .. 86400]"
            ]
        },
        ...
}
```

10. Conduct website categorization

Website categorization is the trick that just may get you as close as possible to 100% certain verification of website authenticity.

Website categorization is enabled by performing real-time analysis of websites using machine learning, artificial intelligence, and human-verification techniques. Sophisticated online tools that categorize websites filter and classify information on three levels:

- Website response - determining whether the website is active during the crawling, a routine process of scraping, storing and organizing website content. This is the first way to check for malicious domains.
- Machine learning and rules - extracting important information and keywords from the website. This information is analyzed based on natural language processing, in a manner that simulates human interaction with web content.
- Human supervision - collected information is authenticated by supervisors to guarantee accuracy in classifying websites into 25 categories. This allows end-users of this tool not only to check websites for malware but also to confirm the activities and purpose behind the website.

Website categorization tools can also be combined with threat intelligence tools we previously mentioned for in-depth analysis and high-level security. On top of that, website categorization is a good choice for businesses that can leverage this tool to boost their targeting efforts, identify profitable opportunities, and prevent potential damage to their brand.

Conclusion

Creating a safe online experience for yourself and others is a never-ending challenge. The six

simple tricks - checking the connection type, site security, URL, content, social proof, and Google report - should become a part of your regular browsing routine.

If you work as a vendor or service provider, guaranteeing online safety for your business and clients takes more than a routine check-up. In that case, verifying website authenticity requires sophisticated online tools that can tackle both technical and human aspects of browsing.

Threat Intelligence API and Website Categorization API is an ideal solution-combo for this challenge, trusted by industry giants such as AT&T, Symantec, Amazon, eBay, Apple, Cisco, and supported by numerous case studies. Want to try it out and check any website's authenticity right now, for free? Click here and find out what we have in store for you!