DATA PROVIDER. COM

Global web security report 2024

About Dataprovider

Dataprovider.com indexes a wide range of security metrics for over 750 million hostnames on a monthly basis. This structured web data is accessible using Dataprovider.com's search engine. With 4 years of historic web data, it is possible to spot global web security trends.

- We help organizations such as the United Nations with thorough insights into the digital economy.
  We provide data intelligence to corporations like GoDaddy, PayPal, and Google to better understand different markets, customers, and competitors.
- We provide structured data to governments, intergovernmental organizations, National Statistics Offices and chambers of commerce to support their data-driven research and policy making.
- We supply key data for investment funds to help them with their investment choices.

Interested to see what our data can do for you? Reach out at info@dataprovider.com or sign up for a free demo.

About our data

Our data and processes comply with the European General Data Protection Regulation (GDPR) as well as with the California Consumer Privacy Act (CCPA).
We do not crawl websites if they disallow crawling, thereby complying with the international standard of the Robots Exclusion protocol. You can trust the integrity of our data, as we can always trace it to its source: we don't use any third-party data (except for our Traffic Index). Our Privacy by Design technology ensures that, by default, we minimize the personally identifiable information (PII) to what is needed to accomplish your goal.

- Fully compliant with GDPR and CCPA regulations
- 750 million hostnames, with more added each month
- Information on software versions, SSL certificates, DNS records and much more
- 50 million company websites
- 4 years of monthly, historical data

National businesses at risk: understanding website security vulnerabilities

In their 2024 Global Risks Report, the World Economic Forum ranks cyber insecurity as the 4th biggest short-term threat and predicts that it remains a major risk throughout the next ten years. We used our structured web data to get a more in-depth understanding of the current state of information security. For this report, we compared the security status of websites from thirteen countries around the globe. And despite growing attention to cybersecurity, many businesses are woefully unprepared against cyber threats, endangering sensitive information and undermining consumer trust and business continuity.

Number of websites per country

Country	Flag	E-commerce websites	Business websites	Total websites
Australia		18,181	1,140,038	1,158,219
Brazil		109,254	1,226,937	1,336,191
Chile		21,920	188,224	210,144
Czech Republic		44,810	513,610	558,420
Estonia		6,035	53,893	59,928
France		136,237	1,907,474	2,043,711
Indonesia		11,092	519,553	530,645
Mexico		30,982	356,406	387,388
Norway		14,790	179,197	193,987
Philippines		2,692	45,524	48,216
South Africa		13,338	283,774	297,112
Spain		42,817	1,246,405	1,289,222
Turkey		56,510	669,235	725,745

Source: Dataprovider.com, Jan 2024

Small business websites an easy target

Cyber insecurity bears huge economic risks, demanding policies and guidelines to safeguard against this increasing threat. Business websites are an easy target, especially those of small and medium-sized companies that may not have the necessary sources and knowledge to keep on top of security measures. However, the security of a business website is a vital element of a company's credibility and survival.

Poor security can lead to inequity, giving bigger companies an advantage over small ones, according to Forbes. For this report, we looked at a diverse group of countries and checked the security measures in place on national business and e-commerce websites.

Learning from past breaches

Ransomware is one of the most common cyber threats to organizations and can cause significant financial damage. Next to that, it negatively influences a company's reputation, consumer trust, and investor relationships. According to IBM, the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

Website security plays a crucial role in reducing risks for both consumers and businesses. The 2017 Equifax data breach, one of the most significant and far-reaching cybersecurity incidents to date, was caused by a vulnerability in a web application framework. This breach exposed sensitive data of about 147 million consumers and had far-reaching repercussions, including lawsuits, a decline in stock price, and the resignation of its CEO.

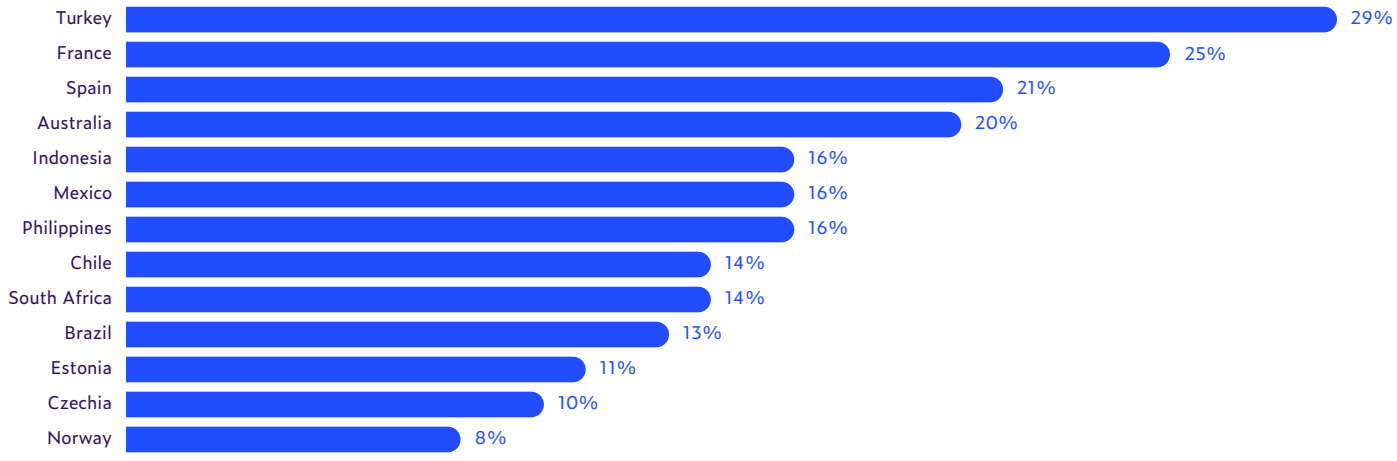
In light of heightened political tension around the world, countries and international organizations have implemented policies or national strategies to improve cybersecurity. These strategies are often part of broader efforts to protect national infrastructure, businesses, and citizens from cyber threats.

But just how effective are these strategies, and how well are businesses implementing basic and more advanced security measures? First, we'll focus on the basic aspects of website security for business and e-commerce websites in the thirteen selected countries.

Outdated and unsupported software

PHP (Hypertext Preprocessor) is an open-source scripting language for web development. PHP plays a pivotal role in website management and maintenance due to its scalability, ease of use, and compatibility with numerous web servers and operating systems. New PHP releases are fully supported for two years. After the two years, support is continued only for critical security issues for an additional 12 months. Then, that version no longer is supported. Once a PHP version is no longer supported, they can pose significant risks. They are vulnerable to exploitation by cyberattackers, leading to potential data breaches and compromised websites.

Fig 1: Share of business websites that run on unsupported PHP version



In our analysis, the share of business websites with unsupported PHP versions ranges from 8% to 29%. Nearly a third of Turkish, a quarter of French and a fifth of Spanish business websites are operating on PHP versions that no longer receive security updates. Norway is the country with the lowest share (8%) of vulnerable business websites.

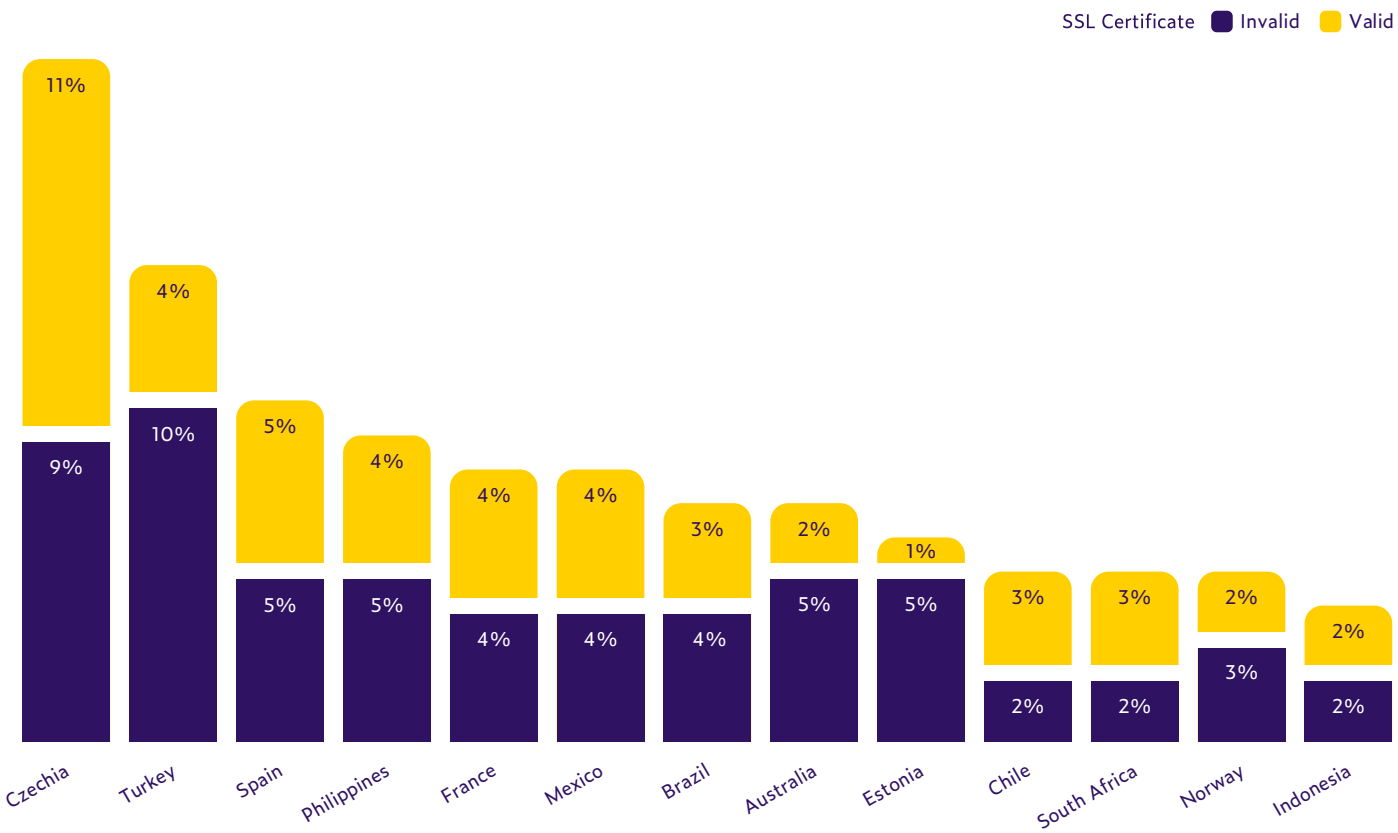
We looked at unsupported PHP branches 4 to 7.4, but 8.0 is also no longer supported as of 26 November 2023, meaning that the true share per country is likely to be even higher. For website administrators, it is crucial to regularly check for new releases and ensure software is kept up-to-date. Hosting providers also have a role to play, alerting clients when older versions no longer receive security patches and assisting with migration to new releases.

SSL certificates at the basis of security

An SSL certificate provides fundamental protection for a website by ensuring that all communication with an external browser is encrypted. Obtaining one is fairly straightforward and is free for the most basic version. Therefore, there is no rationale for not having an SSL certificate.

In our sample, the Czech Republic (11%) has the highest share of business websites with no SSL certificate, followed by Spain (5%). These two also have the highest share of invalid certificates, 9% and 5% respectively. Only Turkey has a larger share; here, 10% of all business websites have an invalid certificate. The overall winner for SSL protection is Indonesia, with only a 4% share of websites with either an invalid or no certificate.

Fig 2: Share of business websites with an invalid or no SSL certificate



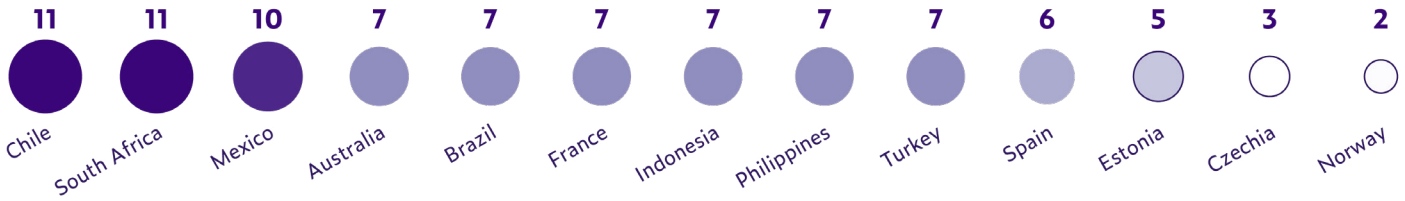
Too many open ports lead to vulnerabilities

The term 'open port' refers to a network port that is configured to accept data packets. A website needs certain open ports to receive traffic. However, open ports can be a significant vulnerability if not properly managed. The more open ports there are, the higher the risk of someone sneaking in where they shouldn't.

The image shows the median number of open ports for business websites for each country, meaning that exactly 50% of all websites fall below and 50% above that number. Norway ranks safest with a median of only two open ports. On the other end of the scale, South Africa and Chile have a median of 11 open ports, signalling a greater vulnerability among businesses in these countries.

Similar to safeguarding physical doors against unauthorized access, it is imperative to protect open ports against cyber criminals. This involves implementing firewalls, keeping software up to date, and only opening up ports when necessary. Open ports without proper security measures invite attackers to gain access to sensitive data, execute malicious code, or disrupt services. That is why regular monitoring and management of open ports are essential components of effective network security.

Fig 3: Median number of open ports for all business websites



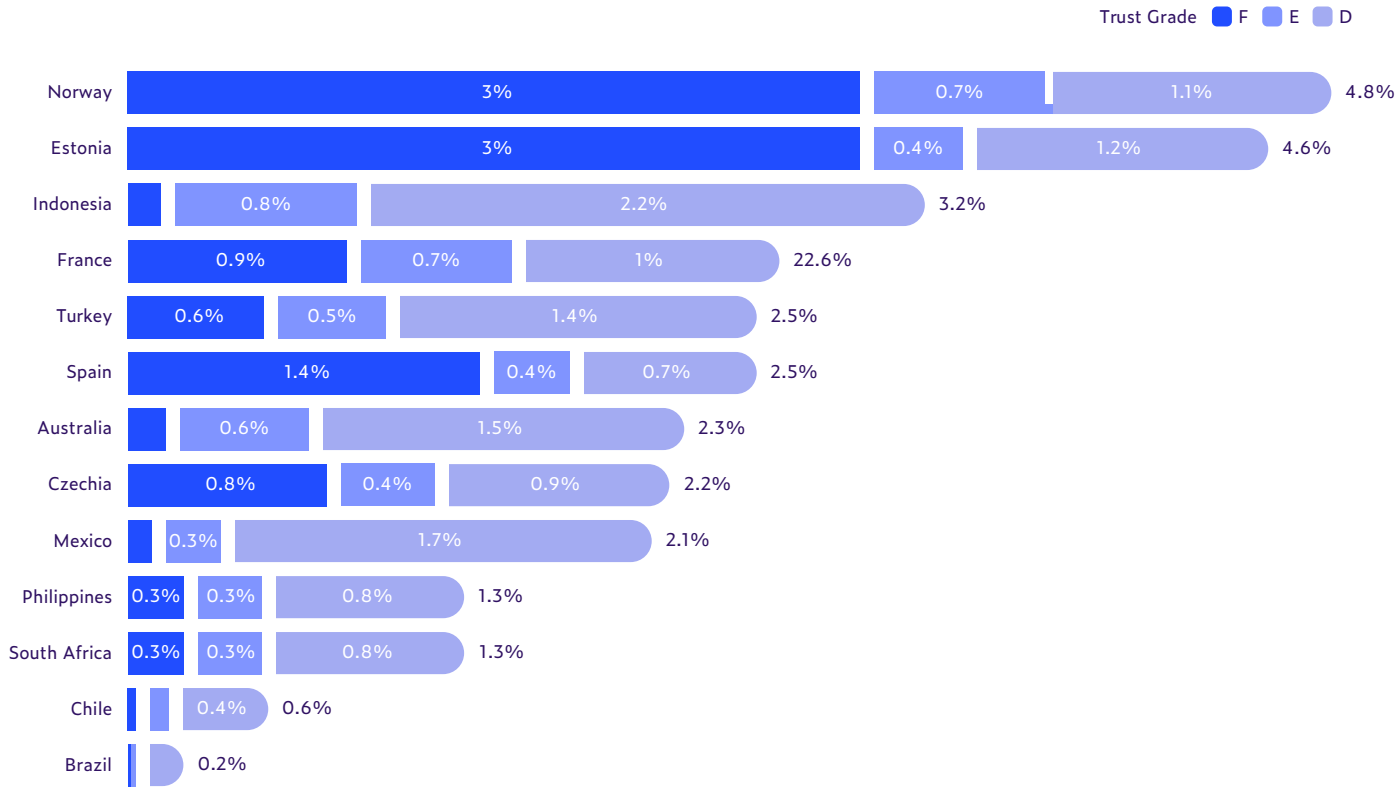
Fraudulent online stores based on Dataprovider.com's Trust Grade

Scrutinizing security measures can offer insights into the trustworthiness of a website. A great example of this are fake webshops. These online stores typically sell counterfeit merchandise or offer products at incredibly low prices, luring consumers to spend without ever providing the product. But fake online stores often lack decent security.

Our proprietary Trust Grade provides an indication of the level of credibility an online store possesses. The scale ranges from A to F, wherein A signifies a high level of trustworthiness. A D, E, or F rating indicates less trustworthiness, with scores of E and F almost certainly indicating a fraudulent online shopping portal. The image shows the highest percentage of dubious online stores are found in Norway (4.8%), followed by Estonia (4.6%) and Indonesia (3.2%). The countries with the lowest share among e-commerce sites are South Africa (1.3%), Chile (0.6%) and Brazil (0.2%). Interestingly, while Norway scored relatively high on other security measures, their strong economy perhaps attracts a more significant number of fraudulent web stores.

Tracking suspicious online stores and taking them down as quickly as possible to minimize damage to consumers and brand reputation is perhaps a task for national law enforcement. Similar to scams in the physical world, consumers need protection to make the web safer for all.

Fig 4: Share of suspicious online stores by Trust Grade



Adding cryptography to DNS with DNSSEC

Domain Name System Security Extensions (DNSSEC) helps protect the system that translates domain names into IP addresses, a crucial step in cybersecurity. DNSSEC adds cryptographic signatures to existing DNS records. These signatures are used to verify that the source of the DNS data is authentic, i.e., the data is coming from where it claims to be coming from and that the data has not been tampered with during transmission.

The objective of DNSSEC is to safeguard against certain types of attacks, such as man-in-the-middle attacks, wherein a user's attempt to access a legitimate website is hijacked and redirected to a fraudulent website.

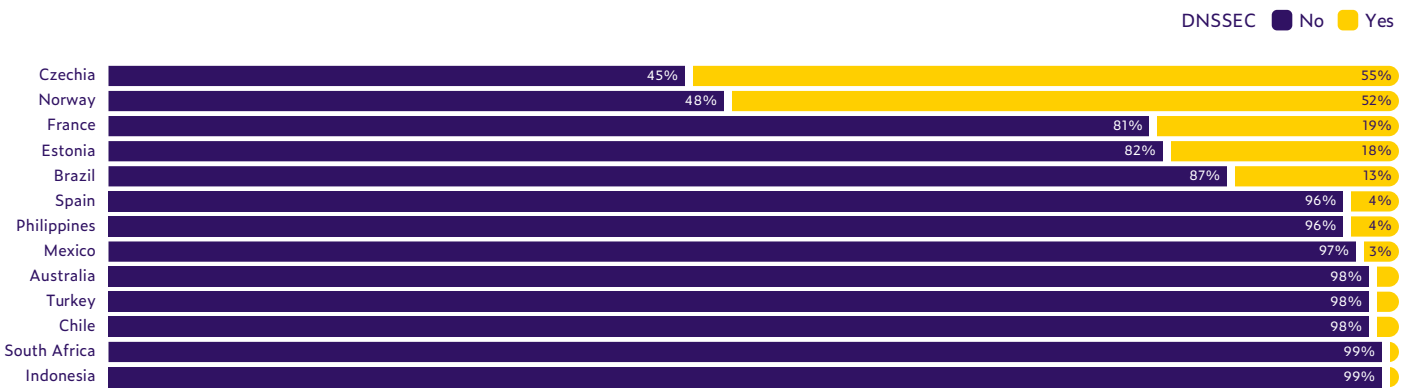
We identified just two countries where a mere half of business websites had DNSSEC enabled, namely the Czech Republic (55%) and Norway (52%). France, Estonia, and Brazil, with respective percentages of 19%, 18%, and 13%, are ranked as the third, fourth, and fifth most secure countries, with between 10% and 29% of their business websites being protected by DNSSEC. The vast majority of websites in the remaining nations are not protected.

Enabling DNSSEC typically requires coordination between domain registrars and DNS hosting providers, indicating that many could do more to protect clients. The .no country code top-level domain (ccTLD) is known to be one of the TLDs with the highest protection through DNSSEC, and our results support this. Several countries have issued directives regarding the implementation of DNSSEC to enhance their national cybersecurity infrastructure.

In Brazil, for example, the implementation of DNSSEC has been pushed to improve internet security within the country. Various initiatives within the EU, including ENISA (European Union Agency for Cybersecurity), have advocated for the implementation of DNSSEC.

However, due to the absence of an EU-wide directive, there are significant disparities among EU nations when it comes to the implementation of DNSSEC.

Fig 5: Share of business websites with and without DNSSEC



Prevent phishing and spam with three key DNS records

Phishing and email spam are the most common ways for hackers to enter a network. It takes just one employee clicking on a malicious link or email attachment to compromise an entire enterprise with ransomware. To prevent a domain from being abused for phishing, just three key DNS records need to be set properly. Those records are SPF, DKIM, and DMARC. The three can help ensure the legitimacy of emails, making it more challenging for attackers to impersonate trusted senders.

The Sender Policy Framework (SPF) enables domain owners to specify which mail servers are authorized to send emails on behalf of their domain.

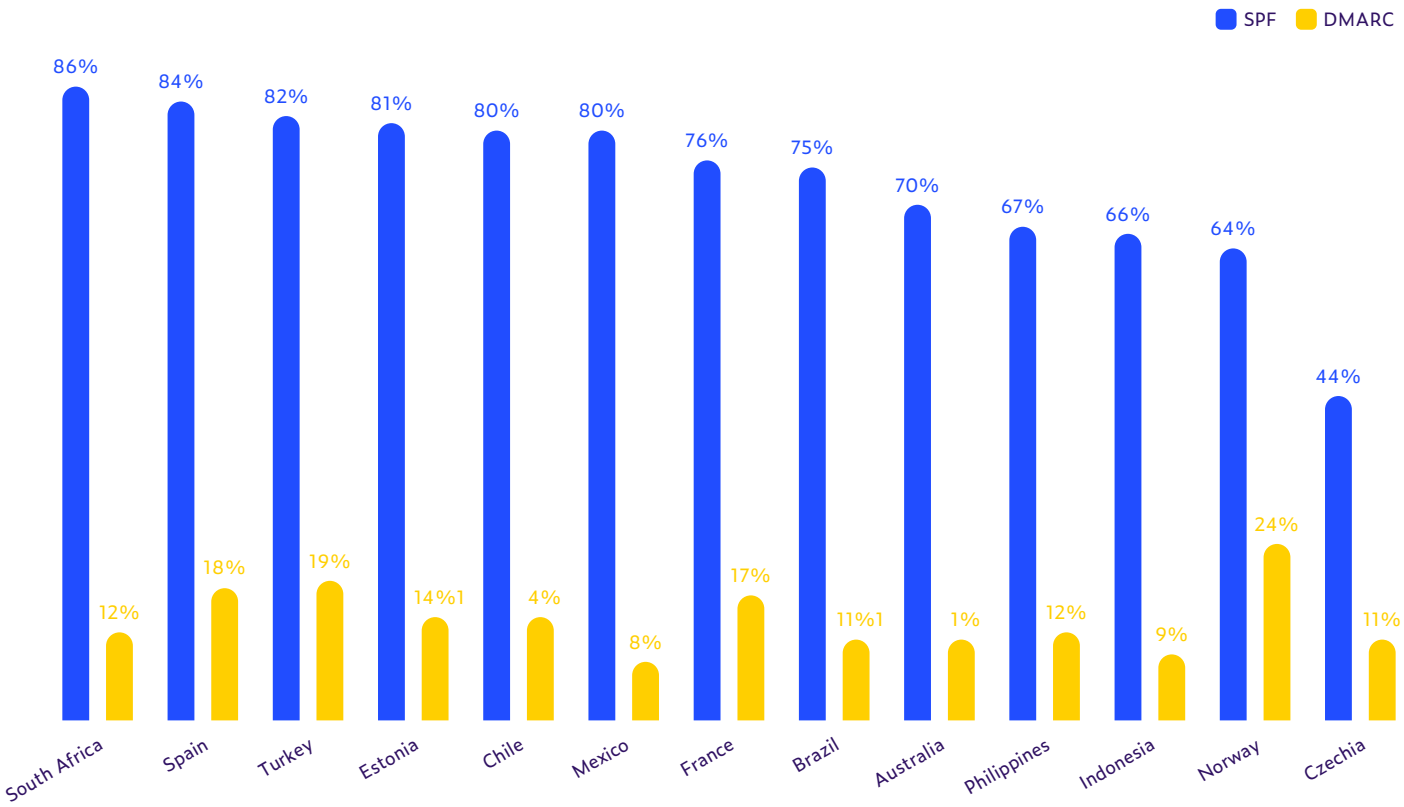
Domain Keys Identified Mail (DKIM) provides a way for an email to be signed with a digital signature, which is then verified by the recipient using the sender's public key published in the DNS. This ensures the email's content has not been tampered with during transit and that the email genuinely originates from the specified domain, making it harder for phishers to forge emails.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) allows domain owners to specify how receiving mail servers should handle emails that fail SPF or DKIM checks. It also specifies an address to send reports on pass/fail statistics, providing visibility into attempts to spoof or forge emails. DMARC helps prevent phishing by ensuring that only authenticated emails are delivered to users and by informing domain owners of potential abuse.

Most business websites in the countries we researched specify SPF, ranging from 64% in Norway to 86% in South Africa. The Czech Republic is the online nation with less than 50% of business websites protected with SPF. DMARC coverage ranges from 8% in Mexico to 24% in Norway, indicating that a lot more could be done to improve the coverage of the DMARC framework.

DKIM is not shown in the image due to its very limited coverage. In no country did the coverage exceed 0.5%. Although it appears that the majority of business websites have taken at least one measure to prevent phishing attacks, a significant proportion of domains have yet to utilize all available security measures to prevent the misuse of email fraud.

Fig 6: Share of business websites with SPF and DMARC in DNS text



HTTP headers play a vital role in website security

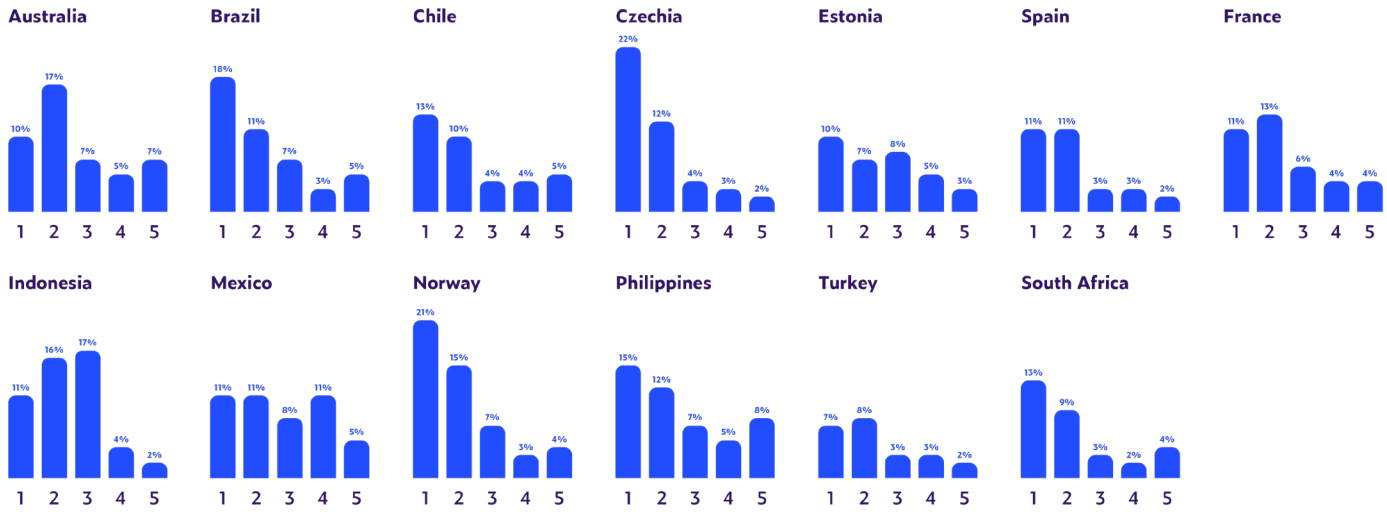
Hypertext Transfer Protocol (HTTP) headers play an important role in the secure and efficient operation of web communications by enabling browsers and servers to exchange information beyond the content of the web page itself. They are used for various purposes, one of which is to specify security policies.

For this research, we examined five security-related HTTP headers (X-XXS-protection, X-Frame-Options, Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options). Without going into technical details, each of these headers can add another layer of security to a website. The image shows the percentage of business websites per country that specify between one and five headers.

In general, the data indicates that well over two-thirds of business websites could significantly enhance their security by defining one or more security-related HTTP headers. In many countries, between 10% and 20% of business websites include at least one or two security-related HTTP headers, but, less than 5% specify four or five of these. Overall, Norway, Indonesia, and the Philippines possess the highest coverage, whereas South Africa, Spain, and Turkey are the lowest ranked. The large share of business websites in all countries that do not utilize these extra layers of protection suggests more could be done to educate domain owners about the utility of specifying HTTP headers. This would provide them with the necessary knowledge to implement them.

Fig 7: Share of business websites that specify security-related HTTP headers

Percentage of websites with 1,2,3,4 or 5 headers.



Security.txt offers direct contact methods for reporting

The security.txt may not be the most high-tech cybersecurity measure, but this standardized file does offer websites to define and publicly share security policies. It's typically placed in the website's root directory, providing contact information for reporting security vulnerabilities. The objective of security.txt is to facilitate the responsible disclosure of potential security issues.

Surprisingly, only one country out of the thirteen under investigation had a mentionable percentage of sites with a security.txt available. 6.5% of Czech business websites have such a file. For all other countries, the share was less than 0.6%. Having a security.txt is certainly not a strong tool against major cyber threats, but being alerted to vulnerabilities can't hurt and may in the best cases mitigate actual breaches before any actual damage is done.

No country boasts a high level of secure websites

Having examined fundamental and less well-known security measures to reduce website vulnerabilities, it's possible to draw a couple of conclusions. First, no country is exceptionally well-secured. Although business websites have some security measures set in place, they are often limited to just a single factor. For instance, instead of specifying SPF, DKIM, and DMARC, just one of them is covered.

Furthermore, not a single nation performs well on all security indicators. Norway may have performed well in several areas, but is among the worst when it comes to fraudulent online stores. Equally, the Czech Republic seems quite secure in most measures, but SSL coverage is lower than in other countries, as is phishing protection. All researched countries would benefit from significant security improvements.

With SSL certificates being a notable exception, there is still a lot of room for corporate websites across the globe to enhance their security measures. An approach that takes multiple measures into account, from improving DNS records to HTML headers and SSL, can create a safer internet for all.

Website security is a responsibility for website owners and governments

The responsibility of securing a website, however, should not solely rest with business owners. Both governments and organizations have a responsibility to fulfill, as do registrars and hosting providers. The state of business website security is a delicate issue that demands immediate and collective action.

Web data is a potent ally in this battle, but it requires the support and active participation of governments and organizations to translate insights from web data into tangible action.

Methodology

This report was prepared based on data collected in January 2024. Countries were selected to showcase broad global coverage and to represent various economies. Data for other countries can be made available upon request. We determine the country a website is affiliated with based on a combination of parameters.These include the location of the website's hosting server, the top-level domain, the language(s) used on the website, as well as any ZIP codes or telephone numbers listed on the contact page.

For the purpose of this research, we focused exclusively on business and e-commerce websites. We classify a website as Business based on information such as a company name, address details, available page types and other content from the website. Websites are classified as e-commerce depending on presence or absence of a shopping cart system, payment methods, products etc.

Dataprovider.com scans the entire web and will follow links, which means any website will be included as long as another website links to it. Websites that have no incoming links are less likely to be found unless they are included in publicly available zone files such as, for example, the .com zone file. All the domains listed there will be included in the crawl. As such, Dataprovider.com does not cover 100% of the web, but it is estimated to represent around 95% of all websites of supported countries. The data represents website data but not individual social media profiles, so businesses that exclusively trade via social media or marketplaces and without a separate domain are not identified.

If you are interested in more information on other countries, feel free to reach out at **info@dataprovider.com**.

DATA PROVIDER. COM

Web Security Australia

Total Business Websites:

1,158,188

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Australia in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.20%

Open ports

Median: 7

Mean: 7.4

DNSSEC

✕ 98%

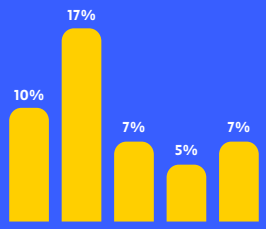
✓ 2%

SSL certificates

Share of websites with a valid, invalid, and no SSL certificate

HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

20%

Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

403

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.

DATA PROVIDER. COM

Web Security Brazil

Total Business Websites:

1,336,175

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Brazil in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.05%

Open ports

Median: 7

Mean: 8.7

DNSSEC

✗ 87%

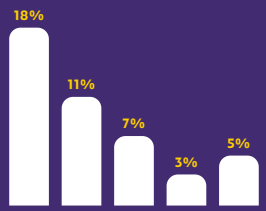
✓ 13%

SSL certificates

Share of websites with a valid, invalid, and no SSL certificate

HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

13%

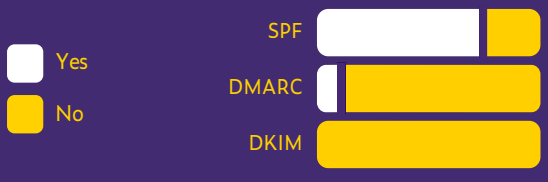
Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

403

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.



DATA PROVIDER. COM

Web Security Chile

Total Business Websites:

210,127

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Chile in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.20%

Open ports

Median: 11

Mean: 10

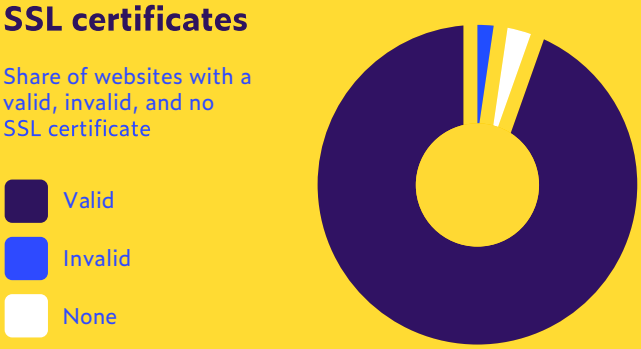
DNSSEC

✗ 98%

✓ 2%

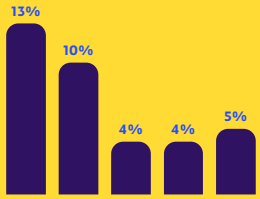
SSL certificates

Share of websites with a valid, invalid, and no SSL certificate



HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

14%

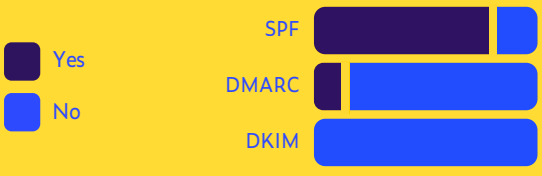
Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

125

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.



DATA PROVIDER. COM

Web Security Czechia

Total Business Websites:

558,417

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Czechia in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

6.54%

Open ports

Median: 3

Mean: 3.9

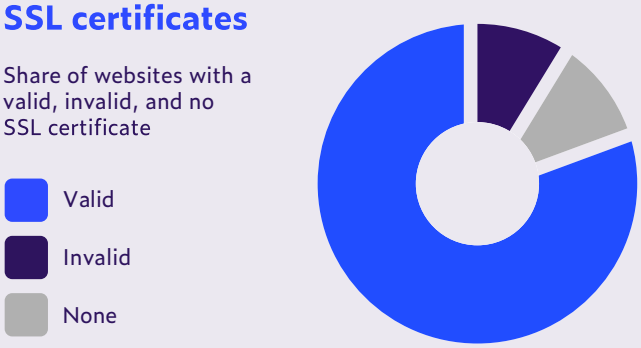
DNSSEC

✗ 45%

✓ 55%

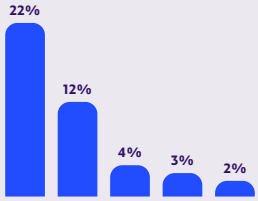
SSL certificates

Share of websites with a valid, invalid, and no SSL certificate



HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

10%

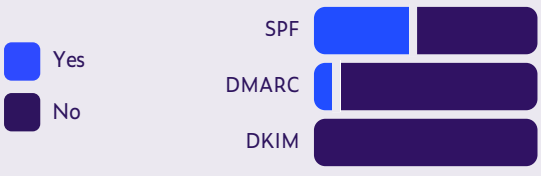
Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

967

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.



DATA PROVIDER. COM

Web Security Estonia

Total Business Websites:

59,925

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Estonia in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.19%

Open ports

Median: 5

Mean: 5.6

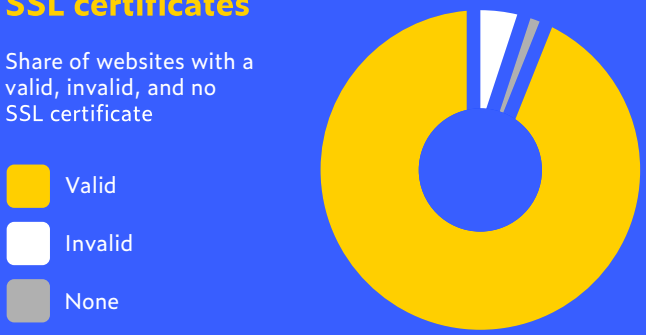
DNSSEC

✕ 82%

✓ 18%

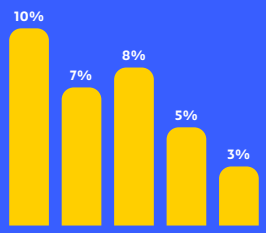
SSL certificates

Share of websites with a valid, invalid, and no SSL certificate



HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

11%

Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

275

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.

DATA PROVIDER. COM

Web Security France

Total Business Websites:

2,043,677

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for France in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.59%

Open ports

Median: 7

Mean: 32.7

DNSSEC

✗ 81%

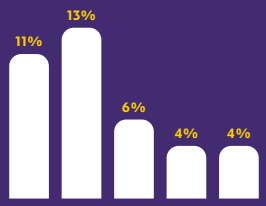
✓ 19%

SSL certificates

Share of websites with a valid, invalid, and no SSL certificate

HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

25%

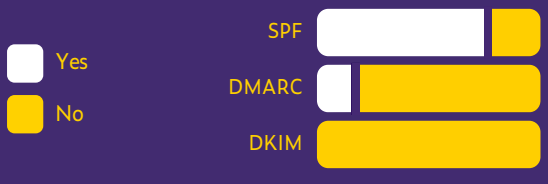
Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

3,529

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.



DATA PROVIDER. COM

Web Security Indonesia

Total Business Websites:

530,642

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Indonesia in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.05%

Open ports

Median: 7

Mean: 8.9

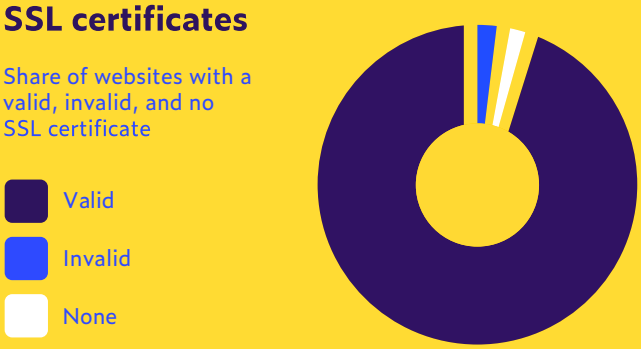
DNSSEC

✗ 99%

✓ 1%

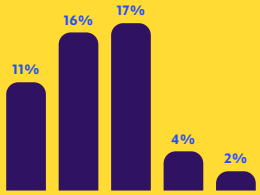
SSL certificates

Share of websites with a valid, invalid, and no SSL certificate



HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

16%

Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

353

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.

DATA PROVIDER. COM

Web Security Mexico

Total Business Websites:

387,384

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Mexico in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.25%

Open ports

Median: 10

Mean: 9.9

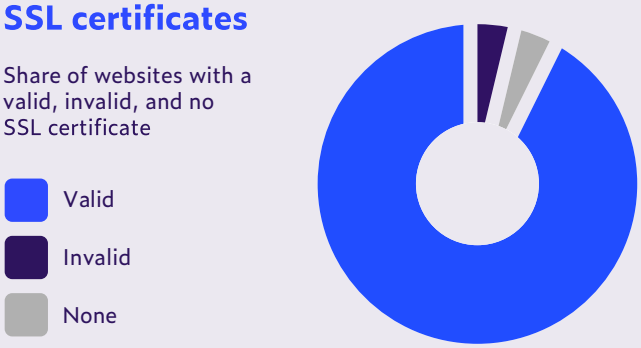
DNSSEC

✗ 97%

✓ 3%

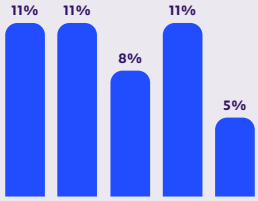
SSL certificates

Share of websites with a valid, invalid, and no SSL certificate



HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

16%

Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

650

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.

DATA PROVIDER. COM

Web Security Norway

Total Business Websites:

193,983

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Norway in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.53%

Open ports

Median: 2

Mean: 4.5

DNSSEC

✗ 48%

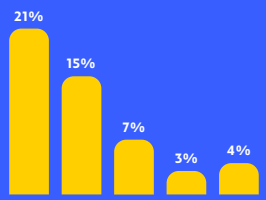
✓ 52%

SSL certificates

Share of websites with a valid, invalid, and no SSL certificate

HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

8%

Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

710

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.

DATA PROVIDER. COM

Web Security Philippines

Total Business Websites:

48,216

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for the Philippines in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.16%

Open ports

Median: 7

Mean: 8.9

DNSSEC

✗ 96%

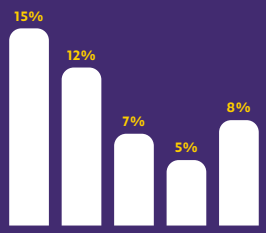
✓ 4%

SSL certificates

Share of websites with a valid, invalid, and no SSL certificate

HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

16%

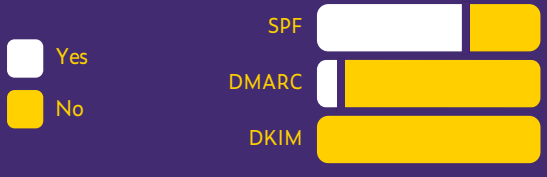
Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

36

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.



DATA PROVIDER. COM

Web Security South Africa

Total Business Websites:

297,099

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for South Africa in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.07%

Open ports

Median: 11

Mean: 9.9

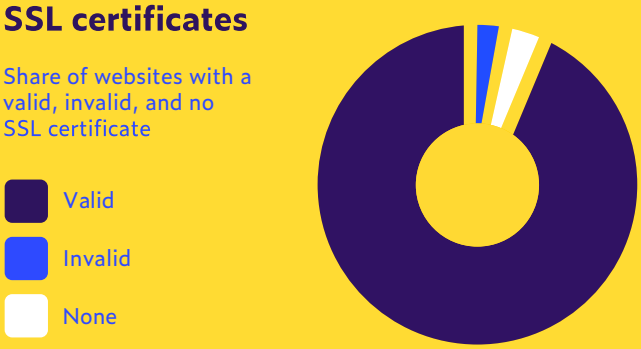
DNSSEC

✗ 99%

✓ 1%

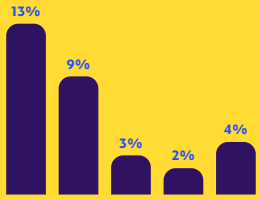
SSL certificates

Share of websites with a valid, invalid, and no SSL certificate



HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

14%

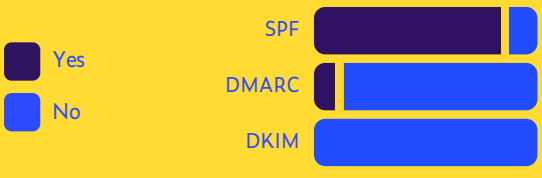
Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

178

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.



DATA PROVIDER. COM

Web Security Spain

Total Business Websites:

1,289,198

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Spain in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.22%

Open ports

Median: 6

Mean: 9.5

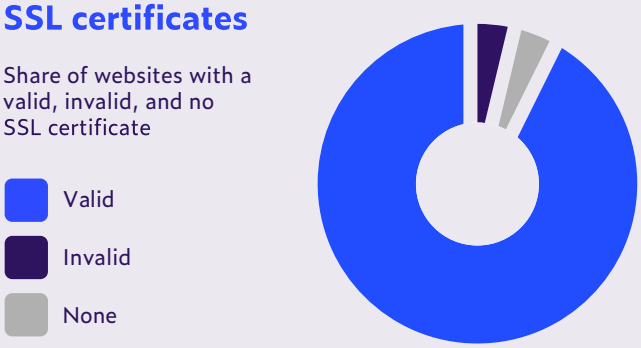
DNSSEC

✗ 96%

✓ 4%

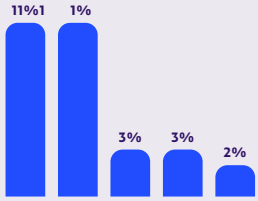
SSL certificates

Share of websites with a valid, invalid, and no SSL certificate



HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

21%

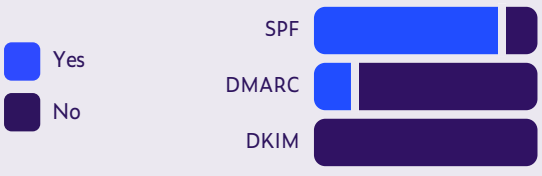
Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

275

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.



DATA PROVIDER. COM

Web Security Turkey

Total Business Websites:

725,735

For this research, we examined eight web security statistics for a varied selection of countries. Below you will find a score for Turkey in each of the researched categories. All data from this research was gathered in January 2024.

Security.txt

Share of websites that provide a security.txt file

0.04%

Open ports

Median: 7

Mean: 8.8

DNSSEC

✕ 98%

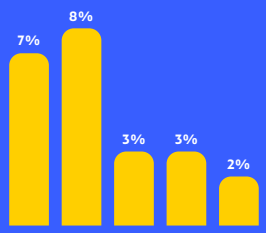
✓ 2%

SSL certificates

Share of websites with a valid, invalid, and no SSL certificate

HTTP headers

Share of websites that specify between 1 and 5 security related HTTP headers (CSP, XSS, HSTS, X-Content-Type-Options, X-Frame-Options, CORS)



Outdated PHP versions

Share of websites with outdated PHP versions

29%

Suspicious e-commerce websites

Number of online stores with a low Trust Grade.

1,420

Spam and phishing

Share of websites with and without SPF, DMARC, DKIM protection.