TRUST DOM
CYBERSECURITY RATINGS

Domain
Cybersecurity Ratings

DOMAINNAME

Last Scan Date: 09-07-2021

Report Generated: 09-07-2021

Table of Contents

"By 2022, security ratings will become as important as credit ratings when assessing the risk of existing and new business relationships"

Innovation Insight for Security Rating Services, Gartner, July 2019

Report
Introduction

This is an executive report which provides an insight into an organisation's commitment to cyber privacy, accountability and trustworthiness. This report offers a comprehensive analysis of a domain's cyber security posture, a domain's attack surface and an overview of domain data and communication security.

In addition to results, this report also provides additional information, which allow the reader to understand the nature of rating calculation within the broader risk zones and at the scanning level.

Simple remediation strategies are provided at the end of each report, allowing users to take steps to mitigate their identified cyber risks. These can be passed on to in-house teams or external vendors who can help an organisation improve their risk ratings over time.

TRUST DOM
CYBERSECURITY RATINGS

Gain insight into an organisation's commitment to cyber privacy, accountability and trust worthiness.

Overview
Of Cybersecurity Ratings

Cybersecurity Ratings provide a quick and cost-effective way to review a company's cyber security posture. We do this by pointing cyber probes at domain security entry points and open source data to collect real-time information on an organisation's online presence and associated security risks.

Cybersecurity Ratings guide the user in making risk-related decisions based on the security of a domain's data and communication posture. By providing the user with critical cyber security information, a user can ascertain the level of risk associated with the domain. (For example, has it been compromised? How well is the website secured? What are its vulnerabilities?)

Using Trust Dom Scanners, users can passively probe any internet domain for a non-intrusive cybersecurity profile assessment. By dispatching a collection of finely tuned probes, we can retrieve and dissect important data signals to reveal a domain's trustworthiness.

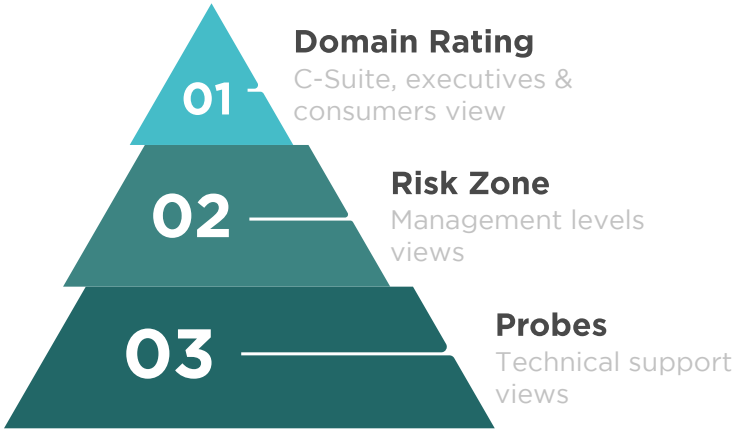
Trust Dom
Cyber Ratings

Trust Dom Cyber Ratings are categorised into three broad cyber rating areas; Domain Rating, Risk Zone Rating and Probe Rating. Each area has been designed to target the needs of a specific audience. For example, the C-Suite executives are more likely to be interested in the domains overall rating, whilst the IT department maybe more likely to focus on the lower level probes and remediation reports.

Domain Rating indicates the average result of the Risk Zone and Probes

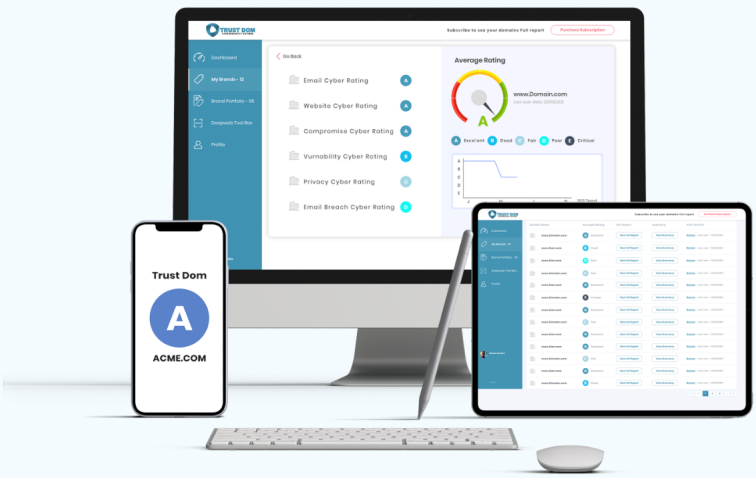
Risk Zones review probe results and package them by risk areas

Probes record technical details and remediation plans



Domain Rating

A Domain Rating indicates an overarching cybersecurity profile for the domain's website and email services. All Domain Ratings are available in real-time, providing the user with an immediate grade at their fingertips. Domain ratings provide the user with confidence that an 'A' grade domain exhibits an excellent level of cyber security and trustworthiness and is therefore safe to use.



Risk zone
Cyber Ratings

Risk Zones are assessed across four sub zones i.e. Email, Website, Compromised, Vulnerability. Each Risk Zone consists of several probes that are designed to assess the level of cybersecurity exposure and vulnerability. These four Risk Zones comprise a composite of over 50 probes which when scanned and scored, produce each Risk Zone Rating. A Grade is then assigned to the website for its compliance with Data Privacy regulations e.g. GDPR and Local Privacy Laws.

As example, an 'E' grade for the Email Zone reflects very poor communication security. This may potentially lead to emails being susceptible to malware, ransomware and spam.

EMAIL ZONE EVALUATION

Can we trust that the email communications has protected our privacy? Is it susceptible to email fraud and malware ? Does it protect, encrypt, and secure communications?

WEBSITE ZONE EVALUATION

Can we trust the website to protect our privacy, data and access? Does the website protect us from malware and attempted data breaches?

COMPROMISED ZONE EVALUATION

Can we trust that the domain has not been compromised by hackers? Is it safe to join the website or communicate with this domain?

VULNERABILITY ZONE EVALUATION

Can we trust that the domain is not vulnerable to a cyber attack? Has the domain been regularly patched and fixed with the latest security service advisories?

DATA PRIVACY COMPLIANCE RATING

Can we trust that the website follows global privacy standards? Is the website secure in protecting personal information?

Probe
Cyber Ratings

There are over 50 Probes dispatched across four sub Risk Zones. Each probe has been carefully designed to passively interrogate a domain's cybersecurity posture and return the results back to the user.

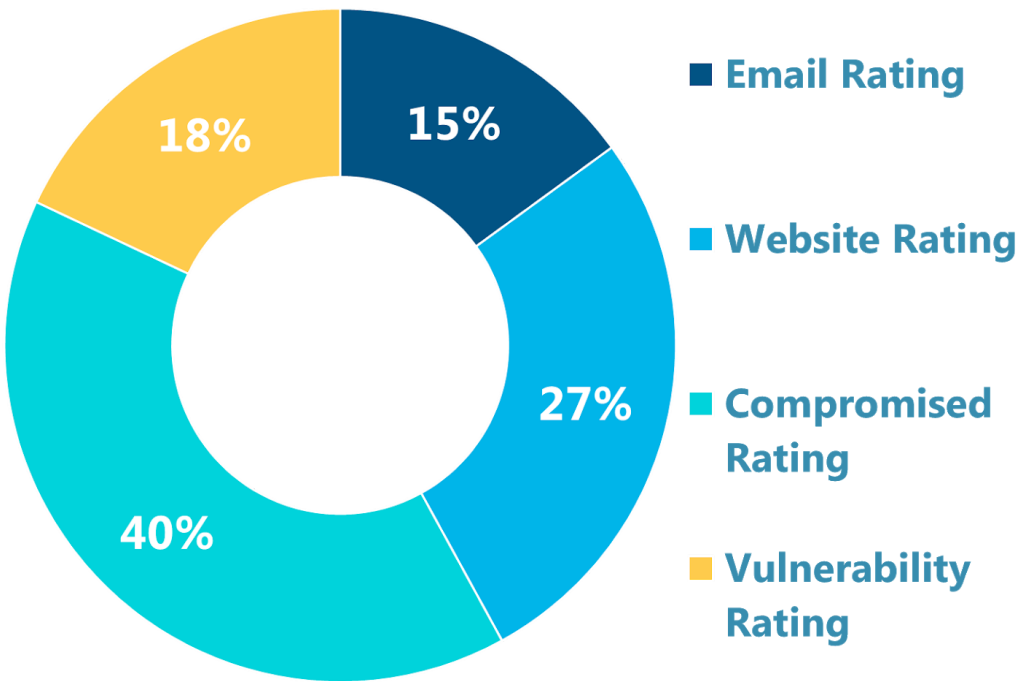
Each probe is assigned an impact and severity value; which in total, calculates the results for the Domain Rating and its associated sub Risk Zones.

Probe Ratings are demarcated as either a pass or fail grade. For example, a 'Failed' Botnet probe would indicate the domain is hosting malware and other hacker services.

Risk Weighting & Algorithm

The risk weighting is managed by an algorithm that calculates each Risk Zone against a probe's impact value and severity before assigning a Rating. For example, the Email Zone is weighted 15% of the overall Domain Rating.

Note: The algorithm may change from time to time as our experts adjust it to reflect new cyber risks. Please also note that we do not share details of our Probes values or our algorithms.



How accurate are **Trust Dom ratings?**

We have taken every effort to ensure that our ratings are accurate and transparent. We have focused on assessing data points that are tangible and clearly quantifiable.

Our ratings explicitly indicate whether an organisation has sufficiently implemented security standards that allow us to trust their public security and trust profile and our email and web-based interactions with them.

Whilst these ratings can correlate to the internal security profile of an organisation, we should NOT assume that an “A” rating definitively means that an organisation is fully secure.

Trust Dom Global Cyber Security Standards

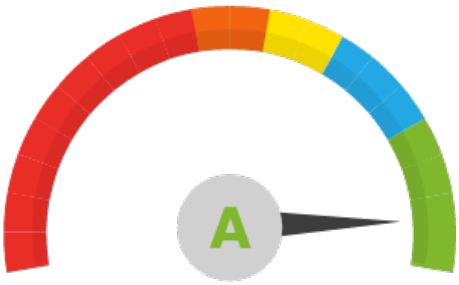
Trust Dom is aligned to the following industry standards:

01. National Institute of Standards and Technology (NIST)

02. ISO27001, PCI, IETF, CVE, NIST CVSS

03. UK Cyber Essentials

Executive **Summary**



A DOMAINNAME

Excellent

The Domain has PASSED more than 80% of Trust Dom's Cybersecurity Controls

RISK ZONE RATINGS

E-mail Cyber Rating	B	Good- The Domain's Email System PASSED 65-79% of Trust Dom's Email Cybersecurity Controls
Website Cyber Rating	C	Fair- The Domain's Website PASSED 55-64% of Trust Dom's Website Cybersecurity Controls
Compromised Cyber Rating	A	Excellent- The Domain PASSED more than 80% of Trust Dom's Compromised Cybersecurity Controls
Vulnerability Cyber Rating	A	Excellent- The Domain PASSED more than 80% of Trust Dom's Vulnerability Cybersecurity Controls
Data-Privacy Cyber Rating	C	Fair- The Domain's Website PASSED 55-64% of Trust Dom's Data Privacy Cybersecurity Controls

A Excellent B Good C Fair D Poor E Critical

Risk Zones
& Probes

A DOMAINNAME

Excellent

E-mail Cyber Rating

Probes	Results	Failed/Pass Message	Remediation
Email Spoof Protection	Pass	Testing The brand's email services are appropriately configured to protect the user from email spoofing, business email compromise and CEO fraud phishing attacks. 90% of all cyber attacks are initiated via email phishing.	N/A
Email Spoof Handling	Pass	The brand's email services are appropriately configured to reject emails from an unknown domain source. Emails are placed in quarantine or labelled as 'suspicious' to protect the user.	N/A
Email Adv Spoof management	Pass	The brand's email services are appropriately configured to protect users from email spoofing, business email compromise and CEO fraud phishing attacks. 90% of all cyber attacks are initiated via email phishing.	N/A
Email Adv Spoof Treatment	Pass	The brand's email services are appropriately configured to reject emails from an unknown domain source. Emails are placed in quarantine to protect the user.	N/A

Email Banner Declaration	Pass	The brand's email server banner is correctly labelled with the organisation's brand name. This configuration method helps to identify the authenticity of the source.	N/A
Email Relay Protection	Fail	The brand's email services are NOT correctly configured to protect it from cyber criminals hijacking the relay services to send out spam and phishing emails.	Technical Failure: You did not configure your email server for spam & phishing relay protection, therefore you need to make the following changes to multiple server configurations. Pls contact your email admin to check email settings: Messages from local IP addresses to local mailboxes Messages from local IP addresses to non-local mailboxes Messages from non-local IP addresses to local mailboxes Messages from client's that are authenticated and authorized Refer to site for more details: https://en.wikipedia.org/wiki/Open_mail_relay
Email Encryption By Default	Fail	The brand's email communication default is to NOT encrypt emails with other email services to protect the confidentiality of the email.	Technical Failure: You did not configure your email server for email encryption by default, therefore you need to make changes to the email service settings. You will need to access the email admin console to include STARTTLS and to ensure you have a valid x509v3 cert or (SSL cert) to encrypt emails. Refer to site for more details: https://tools.ietf.org/html/rfc3207,
Email Encryption Standard	Pass	The brand's email communication services are protected by the latest industry encryption standards (TLS 1.3, 1.2) to protect the confidentiality of emails.	N/A

Website Cyber Rating

Probes	Results	Failed/Pass Message	Remediation
Website Encrypted	Pass	Data communication between the website's service and the client's browser is encrypted and therefore protects the confidentiality of user's data.	N/A
Website Valid Encryption	Pass	The websites encryption certificate is kept up-to-date and is therefore a valid/certified record to protect the confidentiality of user's data.	N/A
Website Encryption Key Strength	Fail	The websites 'encryption key' is WEAK and is therefore lowering the protection of communications from brute force password attacks.	Technical Failure: You did not configure your web server to use a strong data encryption key, therefore you need to install a stronger TLS modern certificates v1.2 and 1.3 cipher suite. Contact your website admin team to acquire a stronger TLS cipher suite cert from a CA certified authority to generate a CSR and private key for your domain. Refer to site for more details: https://tools.ietf.org/html/rfc5246 , https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
Website Browser Trust	Pass	The website is trusted by global browsers such as Mozilla, Chrome, IE or Safari.	N/A
Website Encryption Standards	Pass	The website's data communication is protected by the industry's latest acceptable modern encryption standards, TLS 1.3, TLS 1.2	N/A
Website Encryption Vulnerability	Pass	The website is protected from known exploitable encryption vulnerabilities e.g. Heartbleed, Poodle.	N/A
Redirect Protection	Pass	The website is configured to force the user's browser to always use HTTPS or the website's encrypted pages. This also protects users being diverted to a fake website.	N/A
Clickjack Protection	Pass	The website protects the user's browser from being compromised by the clickjack exploit. The website blocks hackers from injecting hidden malicious code into the website pages or iframes.	N/A

Malicious Code Injection	Fail	The webpages are NOT protected from malicious code injections between the server and the user's browser.	"Technical Failure: You did not configure your web server for security headers XSS protection, therefore you need to make changes to the <webserver HTTPd file>. for example Apache server /etc/apache2/httpd.conf file add the ""header set 'X-XSS-Protection: 1; mode=block' "" https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection"
Filetype Protection	Fail	The website has NO standard MIME file format policy to prevent users from uploading malicious executable programmes within a different file type. This does NOT prevent browsers from wrongfully labelling malicious file types, also known as MIME Sniffing.	"Technical Failure: You did not configure your web server for security headers content type ptorection, therefore you need to make changes to the <webserver HTTPd file>. for example Apache server /etc/apache2/httpd.conf file add the ""X-Content-Type-Options: nosniff"" Refer to site for more details: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options"
Content Protection Policy	Fail	The website does NOT restrict its content delivery to user's browser via registered services thus NOT protecting the user from receiving content from unknown malicious websites.	"Technical Failure: You did not configure your <web server> for <content security policy> therefore you need to make changes to the <webserver HTTPd file>. for example Apache server /etc/apache2/httpd.conf file add the ""Header set Content-Security-Policy ""default-src 'self';"" Refer to site for more details: https://content-security-policy.com/"
Link data protection	Fail	The website does NOT use a referrer policy to protect the user's identity and data when being transferred to another website or domain.	"Technical Failure: You did not configure your <web server> for <content security policy> therefore you need to make changes to the <webserver HTTPd file>. for example Apache server /etc/apache2/httpd.conf file add the ""Header set Content-Security-Policy ""default-src 'self';"" Refer to site for more details: https://content-security-policy.com/"
Data Store Protection	Pass	The website uses data management policies to remove temporary data stores accessible via exploitable cyber attacks.	N/A
Site Content Protection	Fail	The website does NOT use approved whitelists to control content from other domains and web services.	"Technical Failure: You did not configure your <web server> for <x permission cross domain policy> therefore you need to make changes to the <webserver HTTPd file>. for example Apache server /etc/apache2/httpd.conf file add the ""Header set 'X-Permitted-Cross-Domain-Policies' ""none"" - blocks other sites from loading content to browser. Refer to site for more details: https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies"

Encryption Validation	Fail	The websites encryption certificates have NOT been verified as genuine by a trusted public database.	"Technical Failure: You did not configure your web server for an encryption validation check, therefore you need to make changes to the <webserver HTTPd file>. for example Apache server /etc/apache2/httpd.conf file add the ""Expect-CT: max-age=86400, enforce, report-uri=""https://foo.example/report"" "" Refer to site for more details: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect-CT"
Protect Server Name	Fail	The website service information is NOT appropriately hidden from the public via the internet.	"Technical Failure: You did not configure your web server for server headers information protection, therefore you need to make changes to the <webserver MOD_Security file>. for example Apache server /etc/apache2/mod_security file add / remove any reference to Apache, IIS, or other services Refer to site for more details: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Server"
Protect Server Info	Pass	The website service information is appropriately hidden from the public via the internet.	N/A
Cookie Data Encrypted	Pass	The website's cookie data is encrypted between the server and the user's browser, therefore protecting the identity and confidentiality of the communication.	N/A
Cookie Source Mgmt	Fail	The website's cookie data is NOT secured by the server and the user's browser, therefore protecting the integrity and authenticity of the communication.	"Technical Failure: You did not configure your web server for Samesite Cookie protection, therefore you need to make changes to the <webpage code>. for example within javascript ""Set-Cookie: <cookie code> expires=Tue, 20-Apr-21 05:23:36 GMT; path=/; domain=.www.domain.com; SameSite=LAX OR Strict:"" Refer to site for more details: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies"
Cookie Source Protected	Pass	The website's cookie data is secured by the server and the user's browser, therefore protecting the integrity and authenticity of the communication.	N/A
Domain services vulnerable	Pass	The website's port services are appropriately filtered by a firewall and there are no high risk or vulnerable ports open.	N/A
Cookie Disclaimer	Fail	You don't have a cookie notifier on the site that meets data privacy regulations	your website needs to add a cookie notification explaining to the user how you manage cookies
Privacy Notify	Fail	Your website does not have a privacy notification that meets data privacy regulations	Your website needs to add a privacy notification that explains to users how you manage their data

Compromised Cyber Rating

Probes	Results	Failed/Pass Message	Remediation
Open Proxy site	Pass	The IP addess hosting the domain has NOT been detected as an anonymous web proxy or anonymous HTTP proxy used by hackers	N/A
Darkweb Tor site	Pass	The IP addess hosting the domain is NOT registered as a TOR node or running a TOR-related service for shared or streaming darkweb data.	N/A
Public-Vpn site	Pass	The IP addess hosting the domain does not belong to a public VPN provider. Your internet server has not been compromised and configured as a hacker's VPN service.	N/A
Malware site	Pass	IP addess hosting the domain is NOT registered as a maleware distributiion agent or is running malware.	N/A
Spyware site	Pass	The IP addess hosting the domain is NOT registered as a Spyware distribution agent or running Spyware.	N/A
Dshield Registered site	Pass	The IPaddess hosting the domain has NOT been flagged as an attack source on DShield (dshield.org).	N/A
IP Block Hijacked	Pass	The IP addess hosting the domain is NOT part of a hijacked netblock or a netblock controlled by a criminal organization.	N/A
Hostile Spider site	Pass	The IP addess hosting the domain is NOT running a hostile web spider / web crawler.	N/A
Malicious Bot site	Pass	The IP addess hosting the domain is NOT registered as a malicious botnet or part of a botnet C&C network.	N/A
Spam Host	Pass	The IP addess hosting the domain is NOT registered as a spam bot address sending out spam emails and software.	N/A
Exploit Scanner site	Pass	The IP addess hosting the domain is NOT registered as running exploit-scanning software.	N/A

Vulnerability Cyber Rating

Probes	Results	Failed/Pass Message	Remediation
Vuln Criticals >9.0	Pass	The domain has no known CRITICAL security vulnerabilities. This suggests security patches and vendor upgrades are up-to-date.	N/A
Vuln High>7-8.9	Pass	The domain has no known HIGH security vulnerabilities. This suggests security patches and vendor upgrades are up-to-date.	N/A
Vuln Med>4.0-6.9	Pass	The domain has no known MEDIUM security vulnerabilities. This suggests security patches and vendor upgrades are up-to-date.	N/A

Data-Privacy Cyber Rating

Probes	Results	Failed/Pass Message	Remediation
Cookie Disclaimer	Fail	The website has NO cookie disclaimer page to disclose how user data is managed.	"Technical Failure: You did not configure your web server with a cookie disclaimer, therefore you need to add a cookie statement to the website home page. Include a cookie statement to explain to the user how cookies are being managed on the site. Refer to site for more details: https://www.cookielaw.org/the-cookie-law/"
Privacy Notify	Fail	The website has NO privacy notification page to disclose how user cookies are managed.	"Technical Failure: You did not configure your web server with a Privacy notification, therefore you need to add a privacy statement to the web site home page. Include a Privacy statement page on the site to explain to the user how their data is managed. Refer to site for more details: https://en.wikipedia.org/wiki/Privacy_policy"
Vulnerabable website	Pass	The domain has no known CRITICAL security vulnerabilities. This suggests security patches and vendor upgrades are up-to-date.	N/A
Compromised Website	Pass	The website's cookie data is secured by the server and the user's browser, therefore protecting the integrity and authenticity of the communications.	N/A
Cookie Security	Pass	The website's cookie data is encrypted between the server and the user's browser, therefore protecting the identity and confidentiality of the communications.	N/A
Data Encrypted	Pass	The website's cookie data is secured by the server and the user's browser, therefore protecting the integrity and authenticity of the communications.	N/A

Cyber Stats

Cyber-attacks are on the rise

Let’s work together to stop your company becoming yet another cyber-attack statistic. As the world becomes increasingly connected and more businesses move online, cyber security will become everyones shared responsibility.

More Cyber Security Stats...

01. The global cybercrime economy generates approx USD 1.5 trillion yearly

02. The average cost of a data breach for a company in 2020 was US$3.86m

03. The average cost per stolen record is US$120

"SRM (security and risk management) leaders should leverage security ratings services as an additional data point to provide continuous independent scoring for their overall digital ecosystem- public-facing assets and otherwise"

Top 10 Security Projects for 2019, Gartner, July 2019

THANK **YOU**