

One in ten brands fail basic cybersecurity hygiene checks, leaving the door open to cybercriminals, ransomware attacks, and more.

Failing to follow basic cybersecurity hygiene is leaving many global brands, along with their third-party suppliers and customers, open to possible cyberattacks, ransomware, email scams, and worse.

After analyzing nearly 10,000 websites, Cygienic.com found that a staggering 10% of sites owned by top global brands failed basic cybersecurity hygiene checkpoints, such as weak website security or poor email security settings.

As a result, many of these brands, including their customers, could be vulnerable to cyberattacks, ransomware, email scams, and more.

Just like how good personal hygiene helps to promote good health and wellness, good cyber hygiene helps to safeguard the health and security of an organization's sensitive data, reputations, and more.

It can also help to stop would-be hackers and criminal groups in their tracks.

Cygenic.com analyzed nearly 10,000 websites of global brands. It looked at the strength of email and website security, the trustworthiness of IP addresses, and potential website vulnerabilities and data privacy issues. It found that:

10% failed basic cyber hygiene assessments

- 9% scored an overall 'A' or 'A+' Grade
- 40% scored a 'B' or 'B+' Grade
- 30% scored a 'C' or 'C+' Grade

"More than 90% of the corporate brand websites we analyzed didn't obtain our 'A+' cyber rating, as set by industry best practices and standards," said Cygienic.com. "This is a real failure of poor cyber risk management."

With cyberattacks on the increase, cyber risk management is more important than ever. Otherwise, it's like leaving the key under the mat for cybercriminals to steal your data, profit from ransomware, sully your reputation, or worse.

Among the global brand websites examined, Cygienic also found that:

- 9% were already tagged as running botnets, malware, or spam services. This would imply that these website domains were already breached.
- 70% had one or more known website vulnerabilities that could expose that brand or website domain to a cyberattack.
- More than 50% failed to meet basic data privacy checkpoints.

Poor cyber hygiene Impacts a company's cybersecurity rating. Yet, these ratings are essential for:

- Managing and evaluating third-party risk
- Choosing suppliers and investors
- Providing key stakeholders with a measurable ROI

In fact, according to Gartner, strong cybersecurity ratings will become as important as credit ratings in risk assessment for new business relationships. To the point that cybersecurity ratings will become the standard and due diligence level for both buyers and suppliers.

“Good cyber hygiene habits are essential for any business that uses email or has an online presence,” said Cygienic.com. “And it all starts with knowing your cybersecurity rating – before the hackers do.”

To check your cybersecurity rating, click here < <https://cygienic.com/register>>.

ABOUT THE COMPANY

A Singapore-registered private limited company, Cygienic helps businesses to see how exposed they are online, in terms of data breaches, cyberattacks, ransomware, and more. By scanning, checking, and monitoring their cybersecurity ratings, and those of their third-party suppliers and business partners, companies can minimize their cybersecurity risk. In doing so, they help to safeguard their data, finances, and reputations, while promoting their value to potential investors. Click here to check your cybersecurity rating. < <https://cygienic.com/register>>