How do you make sure the system is secure and data safe?

It must be ensured that the data on the system is kept safe and not exposed to cyber-attacks. If the data is compromised due to some reasons, it can discourage visitors from coming back and also damage our reputation. That’s why, security is a critical component and must be taken very seriously.

What data is sensitive?

* Login credentials of a user.
* Any personal data of the user like Full Name, Home Address, City, Postcode, Telephone, Age, Date of Birth, Gender or race, Web cookie, etc.
* Data on the Hosting server
* Online payment related data, for example credit card information.

How will you protect it?

* Login credentials, especially passwords can be protected:
* By prompting the user to create a strong password by using lowercase and uppercase letters, numbers and special characters combination.
* Passwords should always be stored as encrypted values, preferably using a one way hashing algorithm such as SHA.
* Any personal data of the user must me collected only after user’s consent. The data collected should be kept confidential and used as per the agreement with the user.
* Hosting providers usually protect the server our website is on. We must ensure that a trusted hosting provider must be chosen so that we can rely that our data on the server remains in safe hands.
* Any online transaction should be processed through secure payment gateway.The most well-known hosted gateways are PayPal, Amazon Payments, Stripe, SagePay, etc. which are highly secure and support transaction types like authorisation, capture, sale, refund, and void.

What specific technologies will you use for protection?

* **An SSL certificate**: SSL certificates protect the data collected by your website, like emails and credit card numbers, as it is transferred from your site to a server. This is a basic website security measure, but it’s so important that popular browsers and search engines are now labelling sites without SSL as “insecure,” which could make visitors suspicious of a site.

Getting an SSL certificate for our site, would add **HTTPS** label to the website.

* **A web application firewall (WAF):** A WAF protects from automated attacks that commonly target small or lesser-known websites. These attacks are carried out by malicious bots that automatically look for vulnerabilities they can exploit, or cause DDoS attacks that slow or crash our website.
* **A website scanner:** A website scanner looks for malware, vulnerabilities and other security issues so that we can mitigate them appropriately. SiteLock’s scanners not only remove known malware, they also look for threats on a daily basis and let you know the moment anything is found, reducing the amount of damage it can do to your site.
* **Software updates:** Websites hosted on a content management system (CMS) are at a higher risk of compromise due to vulnerabilities and security issues often found in third-party plugins and applications. These can be prevented by installing updates to plugins and core software in a timely manner, as these updates often contain security patches – you can even use an automatic patching solution to make it easier.