If there’s any reason why you as a website owner don’t consider steps to boost your website security, it’s because either you believe your website will never be attacked or it’s of no value for attackers. This mindset is completely wrong and that’s why hackers successfully target such websites. Particularly, if you are in a business that deals with customer data, you can put yourself and your customers at serious risk of fraud and identity theft.

To help ensure that it doesn’t happen, let’s consider six easy and important ways you can ensure your website security.

**Protect it Against SQL Injections**

An SQL injection attack happens when an attacker gains access to your website by using a URL parameter for manipulating your database. If you are using a standard TransactSQL, it’s easy for attackers to type a rogue code into the query and access your information. In order to stop this, it’s important to use a parametrized query. It’s simple to use and most of the web languages have it.

**Install Secure Sockets Layer (SSL)**

To add SSL to your website, the best way is to use HTTPS, a protocol that ensures website security by allowing secure communication over your network. It ensures that when a user browses your website, enters login details or submits financial information, their data remains safe.

**Protect Against XSS Attacks**

Cross-site scripting or XSS attacks directly attack the users instead of the server or application. An attacker injects a malicious JavaScript code into a web application’s output such as comment section, cookies, forums or search fields. From there they can get access to critical data login information, session IDs and credit card numbers.

To protect against XSS attacks, the best way is to use an advanced Security Development Lifecycle or SDL. SDL helps to limit coding errors in your web application. Another way is to make a user re-enter their password before accessing a website page.

**Use Secure Email Transmission Ports**

Another prime target of attackers is not your website itself but your email.

Have you ever thought about whether your email transmissions are secure or not? To find it out, go to your email settings and see which ports you are using form communication. If you are communication through POP3 Port 110, IMAP Port 143 or SMTP Port 25, your email transmission is not secured. Conversely, if you are communicating through POP3 Port 995, IMAP Port 993 or SMTP Port 465, your emails transmission is secure and encrypted.

**Invest in Website Vulnerability Assessment**

Finally, invest in a good website vulnerability scanning service that can identify weaknesses in your website beyond common vulnerabilities.

All these methods do not guarantee website security for you, but for the least part they can make your website less appealing to cyber criminals and hence, more secure.