How Secure Are You?
Checklist

The following best practices are from the Symantec Internet Security Threat Report (ISTR) Vol 22, our annual report which provides an analysis of the year in global threat activity. Use this checklist and make the necessary changes to strengthen your defenses.

- ☐ **Regularly assess your website for any vulnerabilities.**
  Identify and take actions against the most exploitable weaknesses on your public-facing web pages, web - based applications, and server software.

- ☐ **Scan your website for malware.**
  Make your scans regularly - daily is best, weekly is standard, monthly at a minimum.

- ☐ **Set the secure flag for all session cookies.**
  HTTPS secures the web page data, but doesn't necessarily secure associated cookies, which may temporarily hold your password.

- ☐ **Secure your websites against man-in-the-middle (MITM) attacks.**
  This is where attackers can read, insert, and modify messages between two users or systems.

- ☐ **Display recognized trust marks on your website.**
  A recognized trust mark on your website inspires trust and shows customers your commitment to their security.

- ☐ **Be picky about your plug ins.**
  Not all third-party software are your friends; many come with vulnerabilities or worse, hidden malware.

Symantec