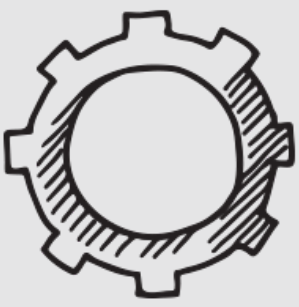
bis BUSINESS INFORMATION SOLUTIONS Getting IT done.

6 CRITICAL STEPS TO SECURING YOUR WEBSITE



1 UPDATE YOUR WEBSITE

A website is like any other application in that it needs to be updated to remain secure. These 3 things need to be updated frequently:

#1: OS Server - where your website is hosted

#2: Content Management System (CMS) - where you edit your website such as DNN or WordPress

#3: 3rd Party Apps

2 PERFORM PERIODIC PENETRATION TESTING

Go through the steps hackers take when trying to access your site. Basically, you are trying to hack your own website to determine what areas are weak and need to be secured.

3 MONITOR SUDDEN SURGES OF TRAFFIC

Review your website analytics weekly to look for unusual amounts of traffic. it could be a distributed denial-of-service (DDOS) attack where cyber criminals attack your website from multiple compromised systems and networks to overwhelm the site and make it unavailable.

4 BACKUP YOUR SITE

Websites need to be backed up just like company data. If your website were to be compromised, you would need a backup copy of your site so you could quickly restore it.

5 SET USER PERMISSIONS

Employees are the #1 threat to businesses! Make sure to set permissions when adding users to the website. Only allow certain employees to make updates . As soon as an employee leaves the organization, immediately delete the users access to the website.

6 USE HTTPS

Use a secured connection (HTTPS) so hackers cannot intercept communication. This is extremely important if you allow visitors to input confidential information including credit card numbers, birth dates, social security numbers or anything else that could be used for identity theft.