Kindly follow these guidelines to safeguard your site from malware.

1): Keep your site updated. (its the most common issue - that is why mostly sites get hacked)  
==> Always do check for any latest update either wordpress, or plugins. All need to be update to almost on regular basis

2): Secure Your Login Page  
==> Protect the default login page url with something else.  
==> Choosing a strong username and password (instead of admin)  
==> Can add security question in login page.  
==> We can use - "[Limit Login Attempts Reloaded](https://wordpress.org/plugins/limit-login-attempts-reloaded/)" plugin to stop users from being able to make endless attempts to break into your account.  
==> Can Add Two Factor Authentication

3): Create Regular Backups of Your Site  
==> Need a proper backup on regular intervals to rollback if any malfunctions happens.

4): Install a Security Plugin  
==> Sucuri - Its scans site from malware and keep uptodate.  
==> Wordfence Security - Its good for strong firewall. and its also include malware scanner too and can monitor traffic and hacking attempts in real time

5): File Permissions:  
==> Need to harden the wp-config.php file and other core files which are very much important.  
==> A good rule of thumb is to set files to 644 and folders to 7556): SSL Secure  
==> Move Your WordPress Site to SSL/HTTPS

7): Disable File Editing  
==> Disable file editing from the wp-admin backend,  
define( 'DISALLOW\_FILE\_EDIT', true );

8): Disable PHP File Execution in Certain WordPress Directories  
==> Disabling PHP file execution in directories where it’s not needed such as /wp-content/uploads/  
==> Need to save the file .htaccess -  
<Files \*.php>  
deny from all  
</Files>

9): Change WordPress Database Prefix  
==> By default, WordPress uses wp\_ as the prefix for all tables in your database. Change the prefix.

10): Disable Directory Indexing and Browsing  
==> Turn off directory indexing and browsing by adding code in .htaccess file at the very end in the root directory.  
Options –Indexes

11): Disable XML-RPC in WordPress (if not using mobile app or remote connections  
==> If you’re using the web-application firewall mentioned earlier, then this can be taken care of by the firewall.  
==> Add the below code in .htaccess  
# Block WordPress xmlrpc.php requests  
<**Files** xmlrpc.php>  
order deny,allow  
deny from all  
allow from 123.123.123.123  
</**Files**>

12): Automatically log out Idle Users in WordPress  
==> Automatically logout inactive users the same way banking and financial sites does.