#1. Bảo mật tên người dùng và mật khẩu quản trị

Đặt mật khẩu phức tạp – phương thức bảo mật đơn giản nhất và hiệu quả nhất. Một mật khẩu mạnh bao gồm chữ in hoa, chữ thường, số, kí tự đặc biệt.

Mật khẩu đủ mạnh, đủ khó sẽ bảo vệ bạn, tránh bị hacker dò mật khẩu.

#2. Chủ động cập nhật và sử dụng phiên bản mới nhất của WordPress và Plugins

WordPress là một mã nguồn mở. Nó sẽ cập nhật liên tục những bản vá lỗi. Và WordPress thông báo update chủ yếu bao gồm có bản vá bảo mật cùng với các tính năng bổ sung cần thiết để chạy các plugin mới nhất.

Chỉ cần dùng phiên bản mới nhất, được chỉnh lỗi nhiều nhất, bạn sẽ bảo vệ được website WordPress của mình rất nhiều.

#3. Chú ý sao lưu dữ liệu

Có rất nhiều WordPress backup plugin miễn phí và trả phí. TinoHost khuyên bạn lưu trữ dữ liệu MỖI NGÀY trên một dịch vụ đám mây như: Amazon, Dropbox, hay một đám mây cá nhân như Stash.

#4. Thực hiện quy trình quét thường xuyên

Nhằm phát hiện các lỗ hổng bảo mật trong hệ thống, bạn cần cài đặt tiện ích WP Security Scan và tiến hành quét thường xuyên. Song song đó, việc thay đổi wp\_ thành bất tiền tố tùy chỉnh sẽ giúp bạn tránh khỏi sự nhòm ngó của hacker.

#5. Mã hóa thông tin đăng nhập



Khi truy cập ở nơi công cộng, bạn đã vô tình tạo cơ hội dành cho hacker. Tuy nhiên, bằng plugin Chap Secure Login sẽ giúp bạn giảm thiểu điều này. Plugin Chap Secure Login có chức năng chính là gán thêm những đoạn mã hash ngẫu nhiên vào chuỗi ký tự mật khẩu, sau đó tiến hành xác nhận tính hợp pháp của tài khoản với giao thức CHAP.

Cài đặt Plugin: bạn chỉ cần vào add plugin và gõ vào trình search: Chap Secure Login.

#6. Tự động log-out user khi không hoạt động

Rất nhiều các trang web ngân hàng và tài chính đều tự động đăng xuất với người dùng không hoạt động. Bạn có thể thực hiện chức năng tương tự trên trang WordPress của bạn. Thao tác rất đơn giản:

Bước 1: Cài đặt và kích hoạt Idle User Logout plugin.

Bước 2: Chọn Settings » Idle User Logout để tùy chỉnh plugin.

Bước 3: Chọn thời gian chờ và bỏ tích ở tùy chọn “Disable in WP Admin” cho tính bảo mật tốt hơn.

Bước 4: Lưu.

#7. Xóa phiên bản WordPress

Việc tìm ra phiên bản WordPress mà bạn đang sử dụng sẽ giúp hacker lần ra dấu vết lỗ hổng dễ dàng. Nếu xoá phiên bản WordPress, hacker sẽ mất nhiều thời gian nghiên cứu hơn để công phá.