

CHECKLIST BẢO MẬT WEBSITE TOÀN DIỆN

Biên soạn bởi: HỒNG MINH (MINH HM)

CEO LIGHT | Chuyên gia Marketing Online, lập trình với 12+ năm kinh nghiệm

QUẢN LÝ TÀI KHOẢN & MẬT KHẨU

- ☐ Sử dụng mật khẩu mạnh (tối thiểu 12 ký tự, kết hợp chữ hoa, chữ thường, số, ký tự đặc biệt)
- ☐ Thay đổi tên đăng nhập mặc định (admin, administrator)
- ☐ Sử dụng username khác với tên miền website
- ☐ Đặt mật khẩu riêng cho mỗi tài khoản quản trị
- ☐ Thay đổi mật khẩu định kỳ (ít nhất 3 tháng/lần)
- ☐ Sử dụng trình quản lý mật khẩu (LastPass, 1Password, Bitwarden...)
- ☐ Tắt lưu mật khẩu trên trình duyệt công cộng
- ☐ Xóa tài khoản không sử dụng
- ☐ Kích hoạt thông báo đăng nhập bất thường
- ☐ Thiết lập khóa tài khoản sau nhiều lần đăng nhập thất bại

XÁC THỰC & PHÂN QUYỀN

- ☐ Bật xác thực hai yếu tố (2FA) cho tất cả tài khoản quản trị
- ☐ Sử dụng app xác thực thay vì SMS (Google Authenticator, Authy...)
- ☐ Giới hạn số lần đăng nhập thất bại
- ☐ Thiết lập CAPTCHA cho form đăng nhập/đăng ký
- ☐ Phân quyền chi tiết cho từng vai trò người dùng
- ☐ Áp dụng nguyên tắc "quyền tối thiểu" cho tài khoản
- ☐ Giới hạn quyền truy cập theo IP (nếu có IP tĩnh)
- ☐ Giới hạn thời gian phiên đăng nhập (session timeout)
- ☐ Tạo tài khoản riêng cho từng admin/developer
- ☐ Ghi nhật ký tất cả hoạt động của người dùng

CẬP NHẬT & BẢO TRÌ

- ☐ Cập nhật hệ điều hành server thường xuyên
- ☐ Cập nhật CMS (WordPress, Joomla, Drupal...) lên phiên bản mới nhất
- ☐ Cập nhật theme/template
- ☐ Cập nhật tất cả plugins/extensions
- ☐ Gỡ bỏ plugins/themes không sử dụng

- ☐ Sao lưu website trước khi cập nhật
- ☐ Thiết lập cập nhật tự động (nếu phù hợp)
- ☐ Kiểm tra tương thích sau mỗi lần cập nhật
- ☐ Quét mã độc định kỳ
- ☐ Xóa các file tạm, cache không cần thiết

BẢO MẬT MÃ NGUỒN & DATABASE

- ☐ Sử dụng prepared statements cho truy vấn SQL
- ☐ Mã hóa dữ liệu nhạy cảm trong database
- ☐ Lọc và xác thực tất cả dữ liệu đầu vào
- ☐ Ngăn chặn SQL Injection
- ☐ Ngăn chặn Cross-Site Scripting (XSS)
- ☐ Ngăn chặn Cross-Site Request Forgery (CSRF)
- ☐ Đổi prefix database mặc định
- ☐ Sử dụng tham số bảo mật trong wp-config.php (WordPress)
- ☐ Hạn chế hiển thị thông báo lỗi chi tiết
- ☐ Kiểm tra code thủ công hoặc bằng công cụ tự động

BẢO MẬT SERVER & HOSTING

- ☐ Cài đặt tường lửa (Firewall)
- ☐ Cấu hình Web Application Firewall (WAF)
- ☐ Giới hạn quyền chmod cho thư mục (755) và file (644)
- ☐ Chặn truy cập vào thư mục quan trọng (.git, wp-admin...)
- ☐ Tắt directory listing
- ☐ Vô hiệu hóa các hàm nguy hiểm (exec, shell_exec...)
- ☐ Giới hạn truy cập REST API
- ☐ Giới hạn XML-RPC (WordPress)
- ☐ Cấu hình ModSecurity
- ☐ Theo dõi log server thường xuyên

SSL & HTTPS

- ☐ Cài đặt chứng chỉ SSL
- ☐ Chuyển hướng HTTP sang HTTPS
- ☐ Cập nhật tất cả nội dung mixed content
- ☐ Cấu hình HTTP Strict Transport Security (HSTS)
- ☐ Thiết lập cảnh báo hết hạn chứng chỉ SSL
- ☐ Sử dụng SSL version mới nhất

- ☐ Kiểm tra độ mạnh của mã hóa SSL
- ☐ Cấu hình Security Headers
- ☐ Vô hiệu hóa TLS phiên bản cũ
- ☐ Thiết lập Content Security Policy (CSP)

FORMS & USER INPUT

- ☐ Xác thực dữ liệu ở cả client-side và server-side
- ☐ Lọc tất cả dữ liệu người dùng nhập vào
- ☐ Giới hạn kích thước file upload
- ☐ Quét virus cho file upload
- ☐ Hạn chế định dạng file được phép upload
- ☐ Đổi tên file upload
- ☐ Lưu file upload ở thư mục an toàn
- ☐ Giới hạn số lần submit form trong thời gian ngắn
- ☐ Thêm Google reCAPTCHA cho các form
- ☐ Kiểm tra valid email khi đăng ký

SAO LƯU & PHỤC HỒI

- ☐ Thiết lập sao lưu tự động
- ☐ Sao lưu website ít nhất 1 tuần/lần
- ☐ Sao lưu database riêng biệt
- ☐ Lưu bản sao lưu ở nhiều vị trí khác nhau
- ☐ Mã hóa file backup
- ☐ Kiểm tra khả năng phục hồi từ bản sao lưu
- ☐ Xác định thời gian phục hồi tối đa cho phép (RTO)
- ☐ Thiết lập quy trình khôi phục sau sự cố
- ☐ Lưu trữ backup ở dịch vụ cloud an toàn
- ☐ Lưu giữ backup trong thời gian đủ dài (ít nhất 30 ngày)

GIÁM SÁT & ỨNG PHÓ

- ☐ Cài đặt công cụ giám sát bảo mật 24/7
- ☐ Thiết lập cảnh báo xâm nhập
- ☐ Theo dõi traffic bất thường
- ☐ Quét malware/virus định kỳ
- ☐ Giám sát thay đổi file (File Integrity Monitoring)
- ☐ Lập và duy trì kế hoạch ứng phó sự cố
- ☐ Ghi nhật ký các sự kiện bảo mật quan trọng

- ☐ Phân tích log định kỳ
- ☐ Kiểm tra uptime
- ☐ Thiết lập phương án liên lạc khi có sự cố

SAI LẦM BẢO MẬT THƯỜNG GẶP CẦN TRÁNH

- ☐ Sử dụng các theme/plugin nulled, crack
- ☐ Không giới hạn số lần đăng nhập thất bại
- ☐ Sử dụng các phiên bản CMS, plugins quá cũ
- ☐ Thiếu quy trình sao lưu thường xuyên
- ☐ Sử dụng hosting giá rẻ không có bảo mật
- ☐ Không kiểm soát quyền truy cập FTP/SFTP
- ☐ Mở quá nhiều cổng không cần thiết trên server
- ☐ Chưa cấu hình headers bảo mật
- ☐ Cho phép tải lên file thực thi (.php, .exe...)
- ☐ Không kiểm tra định kỳ các lỗ hổng bảo mật mới

BẢO MẬT NÂNG CAO

- ☐ Thiết lập Intrusion Detection System (IDS)
- ☐ Cấu hình Content Security Policy (CSP)
- ☐ Sử dụng HTTP Security Headers
- ☐ Thiết lập SubResource Integrity (SRI)
- ☐ Cấu hình Rate Limiting
- ☐ Chia nhỏ server (segmentation)
- ☐ Sử dụng VPN cho kết nối quản trị từ xa
- ☐ Sử dụng CDN có tính năng bảo mật
- ☐ Thiết lập sandbox cho các tính năng rủi ro
- ☐ Thuê dịch vụ pentest chuyên nghiệp định kỳ

VỀ CHUYÊN GIA HỒNG MINH

CHUYÊN GIA HỒNG MINH

CEO LIGHT

Hơn 12 năm kinh nghiệm trong ngành Marketing Online, lập trình, SEO, thiết kế đồ họa, chạy quảng cáo, vv...

- Training chuyên sâu về SEO, Google Ads, Quảng Cáo cho hơn 3000+ doanh nghiệp

- 20+ Khóa tư vấn đào tạo cho doanh nghiệp về Marketing Online
 - Facebook: <https://www.facebook.com/hm.phm>
 - Chi tiết: <https://light.com.vn/minh-hm>
 - Youtube: <https://www.youtube.com/@minhbmchannel2340>
-

Light - Nhanh - Chuẩn - Đẹp

