WordPress: 10 Tipps zur Sicherung Ihrer Website

Halten Sie Hacker aus dem weltweit beliebtesten Content-Management-System heraus

Willem L. Middelkoop
Mar. 31, 2019

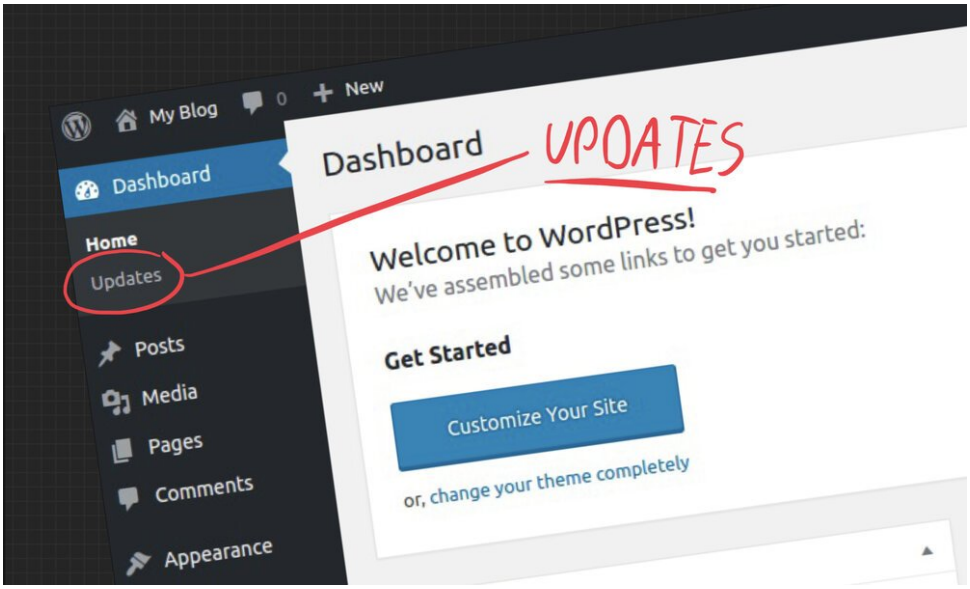
Viele Leute verwenden WordPress, um ihre Website zu verwalten, daher ist es nicht verwunderlich, dass ich gebeten werde, mir die Sicherheit ihrer Website anzusehen. Als Ethical Hacker begegne ich WordPress in verschiedenen Formen, Größen und Zuständen. Einige von ihnen sind wirklich schlecht gegen Hacks geschützt. Verhindern Sie, dass Ihre Website gehackt wird, indem Sie diese 10 praktischen Tipps befolgen.

1) WordPress aktualisieren (und Plugins + Themes)

Die Mehrheit der WordPress-Hacks ist das Ergebnis einer mangelhaften Aktualisierungspolitik. Hacker verwenden automatisierte Bots, um veraltete Softwareversionen zu finden, die

bekannte Sicherheitsprobleme enthalten. Sobald sie Ihre Website als anfällig eingestuft haben, ist das Hacken oft ein Kinderspiel.

Heutzutage kann die Aktualisierung von WordPress automatisch erfolgen, sodass Sie es nicht selbst tun müssen. Lesen Sie die instructions on how to update WordPress.

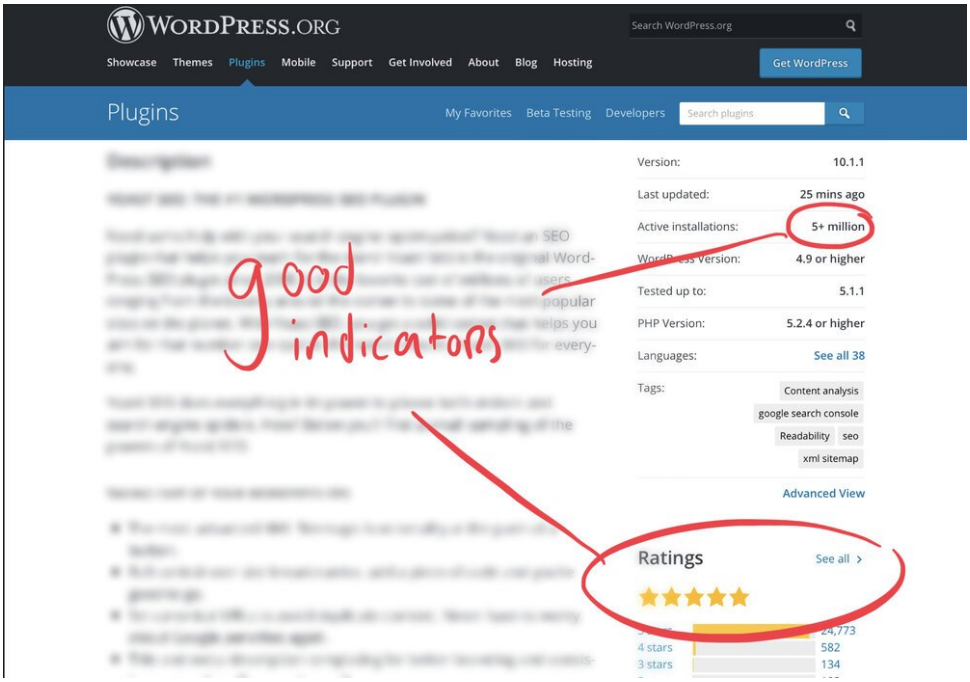


WordPress über das wp-admin Dashboard aktualisieren

2) Plugins und Themes

Der schlechte Sicherheitsruf, den WordPress sich erworben hat, ist hauptsächlich auf die erweiterbaren Teile der Plattform zurückzuführen, insbesondere auf Plugins und Themes. Dies sind die primären Angriffsvektoren, die von Cyberkriminellen ausgenutzt werden, um Ihre WordPress-Website zu hacken und zu missbrauchen. Ihre Sicherheitslücken sind in der Regel das Ergebnis von Fehlern und Versäumnissen während der Entwicklung.

Seien Sie sehr zurückhaltend und vorsichtig bei der Installation von Plugins auf Ihrer WordPress-Website. Sie sollten überprüfen, wer der Entwickler des Plugins oder Themes ist, und feststellen, ob er einen guten Ruf hat, wenn es um das Schreiben von sicherem Code geht. Plugins und Themes mit vielen Downloads werden oft aktiv gepflegt, ein guter Indikator für Sicherheit. Aktualisieren Sie alle Plugins und Themes und behalten Sie die Sicherheitsbilanz im Auge, indem Sie eine Website wie wpvulndb.com verwenden.

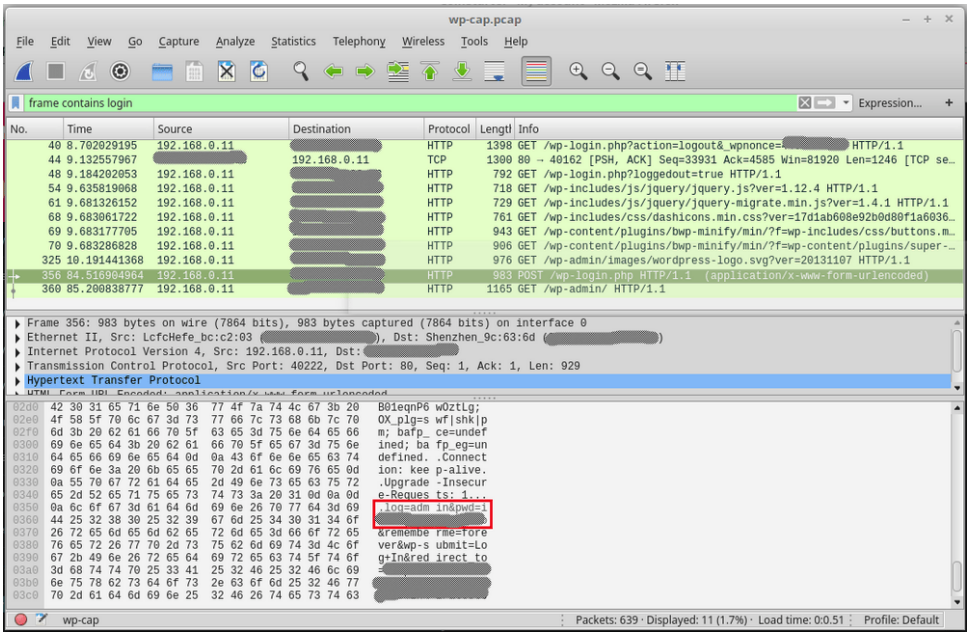


Den Ruf eines WordPress-Plugins anhand der Anzahl der Downloads und seiner Bewertung überprüfen

3) Verschlüsselung verwenden (TLS/SSL)

WordPress-Websites ohne TLS/SSL-Verschlüsselung stellen ein Sicherheitsrisiko dar, da Ihr Passwort immer dann im Klartext gesendet wird, wenn Sie sich anmelden, um die Website zu verwalten. Das bedeutet, dass jeder, der Ihren Netzwerkverkehr abhört, Ihr Passwort leicht erhalten kann. Mit einem gültigen Passwort können sich Hacker einfach anmelden, Sie wollen es ihnen nicht so that easy machen, oder?

Verwenden Sie TLS/SSL, um die gesamte Kommunikation zwischen dem Webserver und Ihrem Browser zu verschlüsseln. Das bedeutet, dass niemand entschlüsseln kann, was Sie in das Passwortfeld eingeben, indem er den Netzwerkverkehr betrachtet. TLS/SSL-Zertifikate, die Sie benötigen, um die HTTPS-Verschlüsselung zu aktivieren, sind heutzutage sehr günstig. Bitten Sie Ihren Hosting-Provider, eines für Ihre Website zu besorgen.

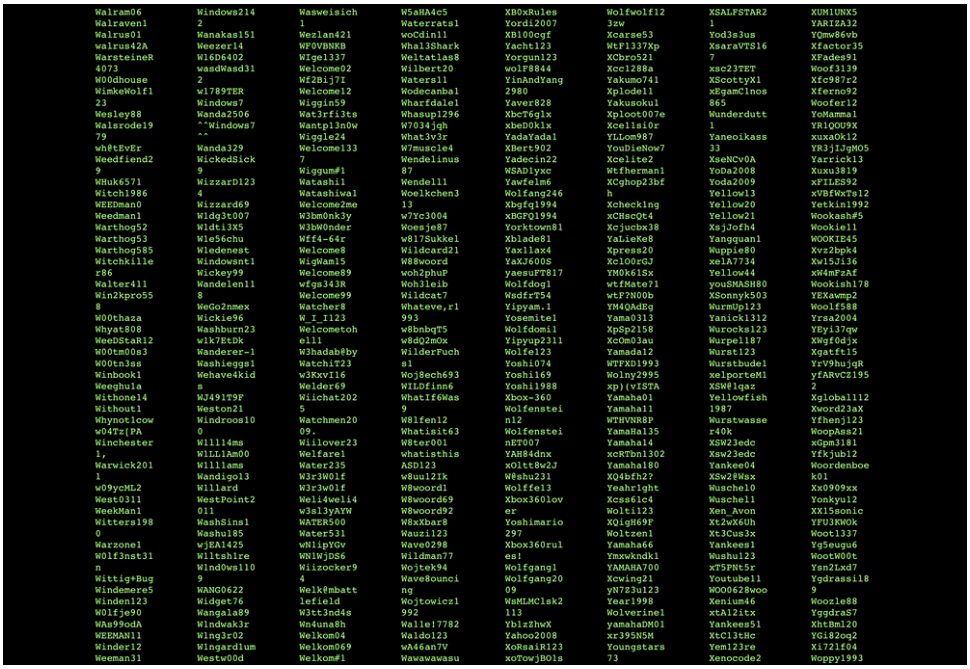


WordPress-Passwort mit WireShark-Paketerfassung ausspionieren (via blog.wpscans.com)

4) Starke Passwörter verwenden

Egal, ob Sie alle anderen Tipps zum Schutz Ihrer Website befolgen, schwache Passwörter sind eine weitere häufige Ursache für Sicherheitsverletzungen bei WordPress. Da die meisten WordPress-Installationen einen ”admin”-Benutzer haben, können Hacker password dictionaries verwenden, um Ihr Passwort automatisch zu erraten.

Stellen Sie sich ein starkes Passwort als etwas vor, das noch niemand zuvor verwendet hat. Das bedeutet in der Regel länger, mit mehr verschiedenen Zeichen, ohne bekannte Wörter oder Phrasen. Sie können einen Passwortgenerator verwenden, um etwas wirklich schwer zu erratendes (und leicht zu vergessendes...) zu erhalten. Vermeiden Sie die Verwendung desselben Passworts auf mehreren Websites und erwägen Sie die Aktivierung der enabling two step authentication for maximum access control.



Passwort-Wörterbuchangriffe verwenden Listen bekannter (durchgesickerter) Passwörter, die man in zwielichtigen Teilen des Internets finden kann

5) Einen vertrauenswürdigen Computer und ein vertrauenswürdiges Netzwerk verwenden

So wie Sie Ihr Bargeld und Ihre Gadgets nicht in zwielichtigen Straßen zur Schau stellen sollten, sollten Sie vorsichtig sein, wo (und wann) Sie sich auf Ihrer Website anmelden. Ein Computer mit Spyware, Malware oder einem Virus kann Tastenanschläge (und Ihr Passwort) aufzeichnen und an Kriminelle senden. Oder auch auf nicht-digitale Weise: Ein Gegner kann Ihnen buchstäblich über die Schulter schauen (im Bus, Zug oder Café), während Sie Ihr Passwort eingeben.

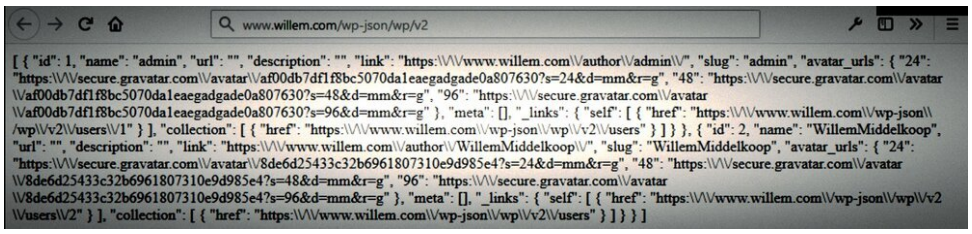
Seien Sie vorsichtig, wo und wann Sie an Ihrer Website arbeiten. Arbeiten Sie nicht an einem gemeinsam genutzten oder öffentlichen Computer, wenn Sie es nicht müssen. Wenn Sie über einen öffentlichen WLAN-Hotspot arbeiten, müssen Sie eine Verschlüsselung verwenden, um zu verhindern, dass jemand mithören kann. Sie können dies mit TLS/SSL oder mit einem VPN (wie buffered.com) tun. Stellen Sie sicher, dass Ihr Computer, Tablet oder Smartphone aktualisiert ist.

Vertrauen Sie dem kostenlosen WLAN, das Sie benutzen? (Image via buffered.com)

6) WordPress REST API deaktivieren

Die WordPress REST API bietet Zugriff auf alle Daten, die auf Ihrer Website verfügbar sind, im maschinenlesbaren JSON-Format. Beiträge, Seiten, Kategorien, Tags, Kommentare, Medien, Benutzer, Einstellungen und mehr können leicht abgerufen werden. Versuchen Sie zum Beispiel, diesen Teil zu Ihrer Website-Adresse hinzuzufügen: **/wp-json/wp/v2/users**, um eine Liste aller gültigen Benutzernamen Ihrer Website zu erhalten. *Wollen* Sie das mit Hackern teilen?

Deaktivieren Sie die REST-API, um Content Scraping (Plagiate) und das Durchsickern von Benutzerdaten zu verhindern. Benutzerdaten sind persönlich und sollten nicht öffentlich weitergegeben werden, wenn Sie Wert auf Datenschutz und Sicherheit legen - denken Sie an die DSGVO. Sie können die REST-API mit Plugins wie Disable REST API oder REST API Toolbox deaktivieren. Lesen Sie den detailed blog post by Jeff Star for more about securing the WP REST API.



Durchsickern lassen persönlicher Benutzerinformationen über die WordPress REST API

7) XML-RPC-Zugriff deaktivieren

XML-RPC ist eine Funktion von WordPress, die die Fernsteuerung Ihrer Website mithilfe von XML ermöglicht (RPC steht für "Remote Procedure Call"). Dieser Mechanismus ermöglicht es Ihnen, Ihre Website zu verwalten, ohne sich im WP-Admin anzumelden, z. B. mithilfe externer Dienste oder Apps. Leider ist die XML-RPC-Funktion eine Sicherheitslücke, da sie im Grunde eine Hintertür ist, die Hacker mit brute force oder special commands zu knacken versuchen können.

Verhindern Sie Probleme mit xml-rpc.php, indem Sie diese WordPress-Funktion vollständig deaktivieren. Sie können dies mit dem Disable XML-RPC plugin tun oder indem

Sie den Webserver manuell mithilfe using a htaccess file konfigurieren.

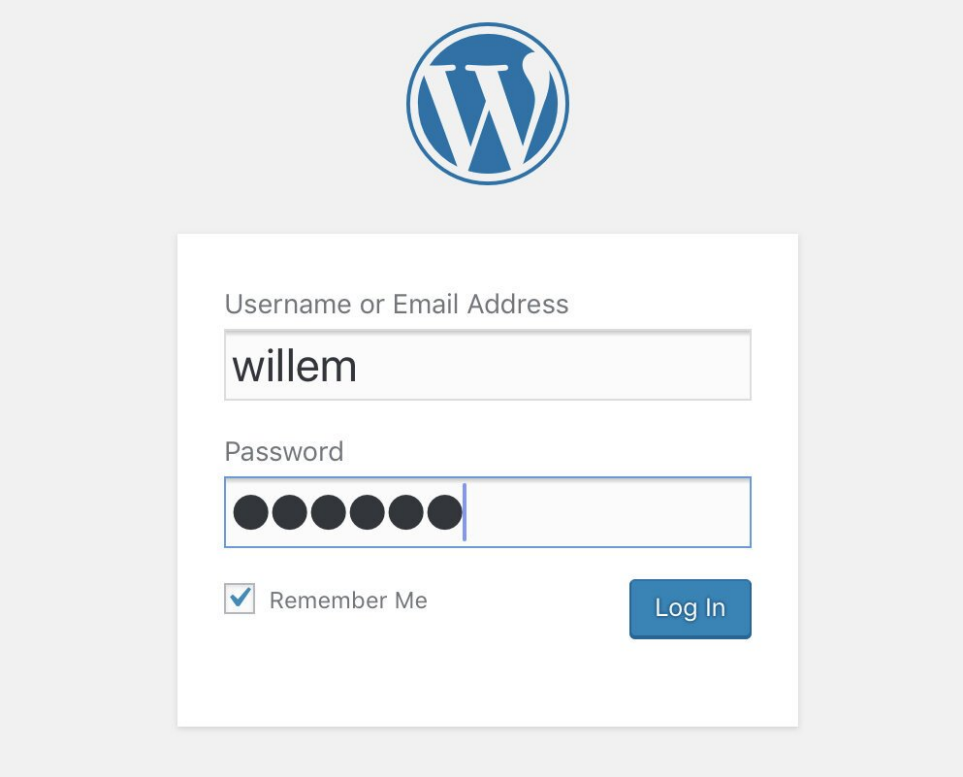
```
# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny,allow
deny from all
allow from [IP]
</Files>
```

Zugriff nach IP-Basis auf XML-RPC mithilfe einer .htaccess-Datei beschränken

8) Die Anmeldeseite ausblenden oder schützen (wp-admin)

Jeder weiß, dass man zum Anmelden bei WordPress einfach '/wp-admin' zur Website-Adresse hinzufügt. Jeder Hacker kann aufgrund dessen leicht mit Brute-Force-Angriffen auf Ihre Website beginnen. Es ist viel schwieriger, ein Schloss zu knacken, wenn man es nicht finden kann.

Erwägen Sie, die wp-admin-Seite auszublenden oder zu ersetzen. Experten nennen dies "security through obscurity", d. h. man verlässt sich auf Geheimhaltung für die Sicherheit. Sie können dafür ein Plugin verwenden oder den Webserver so konfigurieren, dass der Zugriff auf wp-admin durch IP-Adressfilterung eingeschränkt wird. Lesen Sie diesen blog post for ways to hide and protect the wp-admin page. Seien Sie jedoch gewarnt, dass es nicht ausreicht, sich allein auf Geheimhaltung zu verlassen - Sie sollten auch die anderen Tipps umsetzen.



Es ist ziemlich schwierig, meine WP-Admin-Seite zu hacken, weil man sie nicht finden kann (Hinweis: sie ist nicht unter /wp-admin)

9) Zuverlässiges Hosting

Selbst wenn Sie all diese Sicherheitstipps zum Schutz Ihrer WordPress-Website umsetzen, reicht es möglicherweise nicht aus, wenn Ihr Hosting unsicher ist. Hosting ist der Dienst, der es ermöglicht, Ihre Website im Internet verfügbar zu machen. Dies geschieht mithilfe spezieller Computer, die Server genannt werden. Genau wie die Website selbst muss auch der Webserver, der sie veröffentlicht, sicher sein. Stellen Sie sich ein Hosting wie ein Schiff vor, wenn es sinkt, nimmt es alle Passagiere (Websites) mit...

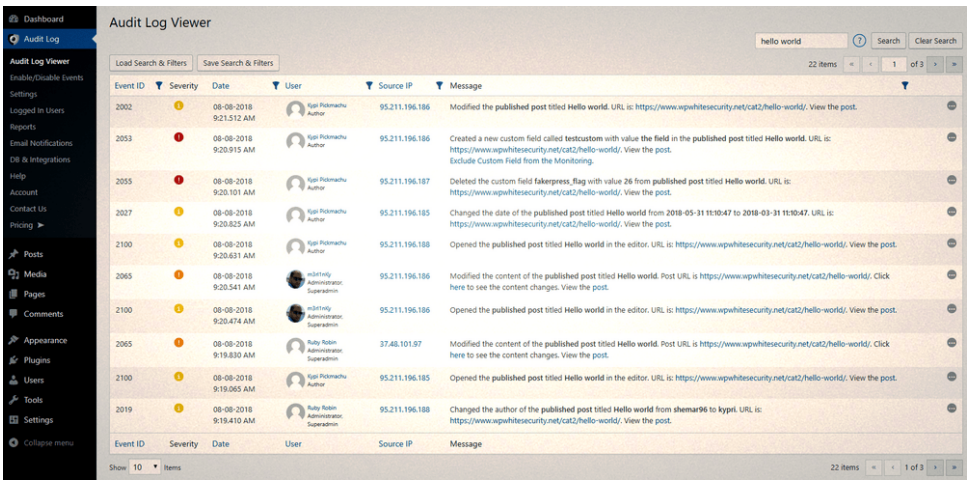
Investieren Sie in zuverlässiges Hosting, indem Sie eine Hosting-Firma mit gutem Ruf wählen. Wählen Sie eine, die gut zu Ihrem Unternehmen passt, und erwägen Sie Hosting mit einem dedizierten (verwalteten) VPS. Seien Sie sich bewusst, dass günstige Hosting-Optionen oft günstig sind, weil sich der Server mit (vielen) anderen (möglicherweise unsicheren) Websites geteilt wird. Lesen Sie weiter, um understand the security concerns in shared hosting zu verstehen.

Irgendwo in einem Rechenzentrum gibt es eine Maschine wie diese, die Ihre Website hostet

10) Backup und Überprüfung

Auch wenn Ihre Website jetzt reibungslos läuft, können sich die Dinge in Zukunft zum Schlechten wenden. Sicherheit ist nie eine absolute Sache, es ist immer möglich, dass Sie in schlechtes Wetter geraten. Bereiten Sie sich auf Probleme vor und lassen Sie Sicherheitsprobleme nicht unbemerkt.

Überprüfen Sie Ihre eigene Website regelmäßig - oder beauftragen Sie jemanden damit. Mit einem Plugin wie WP Security Audit Log können Sie Angriffe und verdächtiges Verhalten frühzeitig erkennen. Erstellen Sie Backups Ihrer Website, damit Sie im Falle einer Cyber-Katastrophe wiederherstellen können. Unfälle passieren den Besten von uns, erstellen Sie ein Backup Ihrer Website, um zu verhindern, dass Ihre Arbeit vollständig verloren geht. Lesen Sie diesen blog post to learn about different ways to backup your WordPress website.



WP Security Audit Log verwenden, um im Auge zu behalten, was mit Ihrer WordPress-Website passiert (wpsecurityauditlog.com)

Schlussfolgerung

Die Sicherheit Ihrer Website ist genau wie die Sicherheit Ihres Büros oder Hauses. Wenn Sie es verlassen, schließen Sie die Fenster und verschließen die Türen, richtig? Vernachlässigen Sie nicht die Sicherheit Ihrer Website, sie ist genauso wichtig wie ihr Design und Inhalt.

Wenn Sie diese Sicherheitstipps umsetzen, wird es für Cyberkriminelle viel schwieriger, Ihre Website zu hacken. Machen Sie es selbst oder bitten Sie jemanden um Hilfe.