Soforthilfe

Sicherheit für Unternehmenswebsiten

HACKER FINDEN.DE Powered by Audat

Disclaimer

Haftungsausschluss
Die dargestellten Inhalte werden mit größtmöglicher Sorgfalt zusammengestellt. Dennoch müssen wir die Haftung für die Vollständigkeit, Richtigkeit und Aktualität der eigenen Informationen, die auf der Website zur Nutzung bereitgehalten werden, ausschließen, es sei denn, wir handeln vorsätzlich oder grobfahrlässig. Der Haftungsausschluss gilt auch für Linksammlungen, die zurzeit Bestehen oder in Zukunft bestehen werden.

Rechtlicher Hinweis
Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen. Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen.

Die Inhalte unserer Website sind urheberrechtlich geschützt. Soweit Sie die Inhalte für Ihre eigenen beruflichen oder persönlichen Zwecke benötigen, räumen wir Ihnen das Recht ein, die bereitgestellten Texte ganz oder teilweise zu speichern und zu drucken.

Die Speicherung und Vervielfältigung von Bildmaterial oder Grafiken aus unserer Website ist nicht gestattet.

Wenn Sie weitere Fragen oder Anmerkungen haben, kontaktieren Sie uns per Mail: hilfe@hacker-finden.de

Einführung

Die rasante Entwicklung der Technologie wird von immer mehr Bedrohungen der Cybersicherheit begleitet. Jeden Tag fallen 30.000 Websites Hackern zum Opfer, und es gibt keine Garantie, dass Ihre nicht die nächste sein wird. Wenn Ihre Website kompromittiert wurde, sollten Sie das Problem so schnell wie möglich beheben. Auf diese Weise können Sie Schäden minimieren, die in Form von Reputationsverlusten, Umsatzeinbußen, Gerichtsverfahren und fehlenden Suchergebnissen entstehen könnten. Dieses Manual befasst sich mit den Symptomen einer gehackten Website und deren Behebung. Außerdem erfahren Sie, wie Sie Ihre Website vor zukünftigen Angriffen schützen und Ihre Besucher am besten über Sicherheitslücken informieren.

So überprüfen Sie, ob Ihre Website gehackt wurde

Bevor Sie irgendwelche Schritte unternehmen, um Ihre Website zu bereinigen, müssen Sie zuerst feststellen, ob Sicherheitslücken vorhanden sind. Je nach Art des Angriffs sind die Anzeichen dafür, dass eine Website gehackt wurde, unterschiedlich und möglicherweise nicht einmal sichtbar.
Hier ist eine Liste der häufigsten Anzeichen dafür, dass eine Website kompromittiert wurde:

- Benachrichtigungen über Hacking-Angriffe von Browsern und Suchmaschinen.
- Links leiten auf problematische Seiten weiter.
- Verunstaltete oder beschädigte Websites.
- Ladezeiten sind langsamer als üblich.
- Warnung auf der Google-Blacklist.
- Versendete E-Mails landen als Spam.
- Die Website wurde vom Hosting-Provider heruntergefahren.
- Unerwünschte Werbung

Zufällige Codefragmente in der Kopf- oder Fußzeile.

Zahlreiche Website-Checker wie Sucuri SiteCheck, DeHashed und Have I Been Pwned? sind verfügbar, um Ihren Verdacht zu bestätigen.

Wir empfehlen, Ihre Website mit mehr als einem Tool zu überprüfen, um genauere Ergebnisse zu erhalten.

10 Schritte zur Behebung einer gehackten Website

Sobald Sie feststellen, dass Ihre Website gehackt wurde, sollten Sie Maßnahmen ergreifen, um das Problem zu beheben.

Die folgenden Schritte führen Sie durch den Prozess der Wiederherstellung und Reparatur einer gehackten Website.

1 Bleiben Sie ruhig und geraten Sie nicht in Panik

Kein Grund zur Panik - gehackte Seiten können oft wiederhergestellt werden. Emotional zu reagieren, ohne die Situation ruhig einzuschätzen, kann mehr schaden als nützen. Bleiben Sie also ruhig und machen Sie mit dem nächsten Schritt weiter.

2 Ändern Sie Ihre Kennwörter und überprüfen Sie den Zugang

Brute-Force-Angriffe gehören zu den häufigsten Bedrohungen der Cybersicherheit. Hacker versuchen, das Kennwort des Administratorkontos zu erraten, indem sie verschiedene Kombinationen aus Buchstaben und Zahlen verwenden.
Wenn Sie alle Ihre Passwörter ändern, können Hacker nicht mehr auf Ihre Website zugreifen und verhindern, dass sie andere Konten kompromittieren und weiteren Schaden anrichten.

Im Folgenden finden Sie eine Checkliste der Konten, deren Passwörter Sie so schnell wie möglich zurücksetzen müssen:

- **Hosting-Konto.**
- **FTP-Konten** (primär und sekundär).
- **Administratorkonto** des Inhaltsverwaltungssystems.
- **Datenbanken** (tun Sie dies über die Datenbankverbindungsdatei).
- **E-Mail-Konten**, die mit der gehackten Website verbunden sind.

Wenn Sie andere Konten mit denselben Anmeldedaten wie Ihre gehackte Website haben, ändern Sie diese sofort. Dies gilt für Konten in sozialen Medien, private E-Mail-Konten und andere persönliche Konten. Denken Sie daran, dass Sie Passwörter gar nicht erst wiederverwenden sollten.

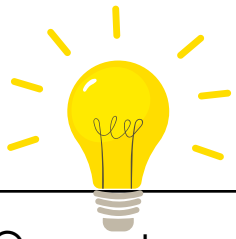
Neben der Änderung aller Passwörter empfehlen wir auch, die Zugriffsrechte der Website-Benutzer zu überprüfen. Wenn es den Hackern gelingt, über ein Administratorkonto auf die Website zu gelangen, haben sie vollen Zugriff auf alle Verwaltungsfunktionen.
Wenn die gehackte Website auf WordPress gehostet wird, überprüfen Sie die vorhandenen Benutzerrollen und -berechtigungen, indem Sie über das Admin-Dashboard auf Benutzer zugreifen.

Überprüfen Sie die -Konten mit Superadmin- und Admin-Rollen, die die höchste Zugriffsebene haben.

Führen Sie dasselbe Verfahren bei Plattformen durch, die mehreren Benutzern Zugang gewähren, wie z.B. Ihr Hosting-Kontrollpanel und Ihr FTP-Konto.

Legen Sie über den Dateimanager des Webhosters die entsprechenden Berechtigungen für Ihre Website-Dateien fest, insbesondere für die Dateien im Stammverzeichnis wie den Ordner wp-admin und die Datei wp-config.php.

Auf diese Weise hindern Sie unbefugte Benutzer daran, vorhandene Dateien zu ändern und auszuführen.



Nutzen Sie einen Passwort-Generator, um Ihre Passwörter zu verwalten und Sicherungskopien der Passwörter zu speichern.

3 Erstellen Sie ein Backup Ihrer Website

Ihre Website könnte gehackt worden sein, aber sie ist immer noch funktionsfähig und enthält alle wichtigen Daten. Wenn Sie eine Sicherungskopie der Website herunterladen, können Sie diese Version der Website erneut hochladen und den Bereinigungsprozess wiederholen, falls er beim ersten Mal fehlschlägt.

Bewahren Sie die Sicherungsdatei nach dem Hack getrennt von den älteren Versionen auf. Die nicht beschädigten Sicherungsdateien dienen als Plan B, falls der Wiederherstellungsprozess fehlschlägt

4 Verfolgen Sie Ihre Handlungen zurück

Die meisten Hackversuche finden statt, nachdem eine Website geändert wurde und neue Schwachstellen entstanden sind, die ausgenutzt werden können. Indem Sie Ihre Aktionen zurückverfolgen, sollten Sie die Quelle der Sicherheitsprobleme viel schneller identifizieren können.

Grenzen Sie das Zeitfenster ein, indem Sie Ihre Webprotokolle auf einen plötzlichen Anstieg des Datenverkehrs überprüfen. Untersuchen Sie dann Ihre Zugriffs- und Fehlerprotokolle über Ihr Hosting-Kontrollpanel, um verdächtige Aktivitäten oder Fehler zu identifizieren, die innerhalb des vermuteten Zeitraums aufgetreten sind.

Nachdem Sie den Zeitpunkt des Hacks herausgefunden haben, untersuchen Sie alle Änderungen, die Sie davor vorgenommen haben. Bei WordPress gelangt bösartiger Code in der Regel über neue Dateien, die durch Plugins, Themes und WordPress-Kerninstallationen eingeführt werden, auf die Website.

Hostinger-Benutzer finden die Zugriffsprotokolle unter dem Abschnitt Website im hPanel. Um auf die Fehlerprotokolle zuzugreifen, navigieren Sie zu PHP Configuration im Verzeichnis Advanced

5 Untersuchen Sie aktuelle Sicherheitsverletzungen online

Neuigkeiten im Bereich der Cybersicherheit auf dem Laufenden halten, können Sie die Schwachstellen viel leichter finden und fehlerhafte Software entfernen, bevor sie auf Ihrer Website Schaden anrichten kann.

Hier sind einige der besten Websites zum Thema Cybersicherheit, die unsere Sicherheitsexperten empfehlen:

- **Hacker News** - bietet Hacking-Nachrichten.
- **WP Hacked Help Blog** - bietet WordPress-Sicherheitstipps zur Reparatur gehackter Websites.
- **Daniel Miessler** - veröffentlicht Artikel und Tutorials über Website-Sicherheit und Technologie im Allgemeinen.
- **IT Security Guru** - konzentriert sich auf Cybersicherheit, Internetkriminalität und Ransomware.
- **Security Weekly Blog** - bietet wöchentliche Updates zur Cybersicherheit in Form von Live-Streams.

> Eine der besten Möglichkeiten, sich über Sicherheitsverletzungen im Internet auf dem Laufenden zu halten, besteht darin, individuelle Warnmeldungen einzurichten.

Je nach Art der Nachrichten, die Sie suchen, können Sie IFTTT konfigurieren oder Skripte entwerfen, um Benachrichtigungen zu erhalten, wenn ein neues Thema in der Cybersicherheits-Community populär wird.

Außerdem sollten Sie alle führenden Sicherheitsexperten und Warnmeldungen von Websites wie "SANS Internet Storm Center" und "Have I Been Pwned" verfolgen.

6 Sprechen Sie mit Ihrem Hosting-Anbieter

Wenn Ihre gehackte Website auf einem gemeinsam genutzten Hosting-System läuft, könnte die Quelle der Sicherheitsprobleme von einer anderen Website auf demselben gemeinsam genutzten Server stammen. In diesem Fall könnten die Cyberangriffe auch auf Ihr Hosting-Konto abzielen.

Wenden Sie sich an Ihr Hosting-Unternehmen, um zu prüfen, ob die anderen Websites auf demselben Server ebenfalls angegriffen wurden.

Die meisten Webhoster bieten ihren Nutzern auch Zugang zu den Webprotokollen, so dass Sie die Besuche auf der Website überwachen können. Wenn die Protokollierung des Serverzugriffs standardmäßig deaktiviert ist, setzen Sie sich mit Ihrem Hosting-Anbieter in Verbindung oder aktivieren Sie sie manuell.

Zur Erinnerung: Entscheiden Sie sich für ein sicheres Webhosting, um Ihre Website vor Hackerangriffen zu schützen.

7 Untersuchen Sie mit der Google-Blockliste und der Spam-Blockliste

Wenn Google verdächtige oder gefährliche Aktivitäten auf einer Website feststellt, wird die Suchmaschine diese wahrscheinlich blockieren. Wenn eine Website auf die Blockliste gesetzt wird, erscheint sie nicht in den Suchergebnissen, um Besucher vor potenzieller Malware zu schützen.

Überprüfen Sie mithilfe der Google Search Console, ob Ihre Website auf der Google-Blockierliste landet.
Die Warnung wird unter Sicherheitsprobleme im Abschnitt Sicherheit und manuelle Maßnahmen angezeigt.

Google Safe Browsing ist ein weiteres Tool, mit dem Sie den Status Ihrer Website überprüfen können. Es teilt Ihnen mit, ob der Besuch der Website sicher ist.

Wenn Sie keinen Zugriff auf den DNS-Zonen-Editor haben, können Sie den Datenverkehr Ihrer Website mit **Google Analytics** überprüfen. Ein plötzlicher Rückgang des Traffics ist eine solide Bestätigung dafür, dass Google Ihre Website auf die Blockliste gesetzt hat.

Neben der Google-Blockliste könnte Ihre Website auch in der Anti-Spam-Datenbank erscheinen. Internetdienstanbieter, Mailbox-Anbieter und Anti-Spam-Plattformen verwenden Spam-Blocklisten, um zu verhindern, dass Spam-E-Mails in ihr System gelangen. E-Mails von IP-Adressen, die auf dieser Blockliste aufgeführt sind, werden blockiert oder landen im Spam-Ordner.

7 Untersuchen Sie mit der Google-Blockliste und der Spam-Blockliste

Klären Sie mit Domain Health Checkern wie **MxToolBox** und **Domain DNS Health Checker**, ob Ihre Domain auf der Spam-Blockliste steht. Diese Tools geben nicht nur Aufschluss über den Status der Domain, sondern können auch Probleme im Zusammenhang mit Ihrem Webserver, Mailserver und DNS aufdecken.

8 Setzen Sie Ihre .htaccess-Datei zurück

.htaccess ist eine Datei, die hochrangige Konfigurationseinstellungen für eine auf dem Apache-Webserver gehostete Website enthält.
Aus diesem Grund ist .htaccess ein beliebtes Ziel von Cyberangriffen.

Zu den häufigsten Angriffen auf .htaccess-Dateien gehören:

- Umleitung von Suchmaschinen zu Malware.
- Umleitung von Fehlerseiten zu Malware.
- Malware-Anhang an PHP-Dateien.
- Offenlegung von Informationen.
- Browser-Fingerprinting.
- Watering Hole-Angriffe.

Das Deaktivieren und Wiederherstellen der ursprünglichen Version Ihrer .htaccess-Datei kann helfen, das Sicherheitsproblem zu beheben. Ändern Sie außerdem die Dateiberechtigungen so, dass nur bestimmte Benutzer darauf zugreifen können.

Benutzer können die .htaccess-Datei über den Dateimanager des hPanel finden und ändern.

9 Untersuchen Sie Ihre Website und beheben Sie die Schwachstelle

Sicherheitsschwachstellen sind für Administratoren nicht immer sichtbar. Wir empfehlen die Verwendung von Website-Scan-Tools, um Ihre gesamte Website auf Schwachstellen zu überprüfen und diese zu beheben.

Verwenden Sie ein Scanning Plugin oder Tool
WordPress-Benutzer haben Zugang zu verschiedenen kostenlosen und Premium-Sicherheits-Plugins, von denen die meisten Ihre Website auf gefährdete Dateien scannen und jeglichen bösartigen Code erkennen können.

Hier sind einige der beliebtesten Freemium-WordPress-Sicherheitsplugins, die Sie in Betracht ziehen sollten:

- **Sucuri Security** - bietet serverseitiges und Remote-Scanning, Sicherheitsmaßnahmen nach einem Hack und Überwachung der Dateiintegrität.
- **Wordfence** - ist mit Echtzeit-Firewall-Regeln und Malware-Signatur-Updates ausgestattet.
- **Jetpack** - bietet Malware-Scans, Echtzeit-Backups und Spam-Filterung.
- **BulletProof Security** - bietet einen Setup-Assistenten, Malware-Scanner, Login-Überwachung und Tools zur Erzwingung sicherer Passwörter.
- **WPScan** - unterstützt geplante Sicherheitsscans für bekannte Schwachstellen im WordPress-Kern, in Plugins und Themes.

9 Untersuchen Sie Ihre Website und beheben Sie die Schwachstelle

In der Zwischenzeit sind die folgenden Scan-Tools mit anderen CMS als WordPress kompatibel:

- **HostedScan Security** – führt Schwachstellen-Scans für Netzwerke, Server und Websites durch.
- **Intruder** – ein Cloud-basierter Scanner, der internes, externes und Cloud-Schwachstellen-Scanning unterstützt.
- **Detectify** – bietet automatisierte Asset-Überwachung und Tests, die von einer ethischen Hacker-Community unterstützt werden.
- **ImmuniWeb** – bietet verschiedene Website-Sicherheitstests unter Einhaltung der GDPR- und PCI DSS-Standards.
- **SiteGuarding** – unterstützt die Überwachung von Suchmaschinen-Blockierlisten, tägliches Scannen von Dateien, Überwachung von Dateiänderungen sowie die Erkennung und Beseitigung von Malware.

Stellen Sie sicher, dass Sie die besten WordPress-Sicherheitspraktiken befolgen, um Ihre Website zu schützen.

Vergewissern Sie sich, dass der Scanner alle Webanwendungen erkennt, die Teil Ihrer Website sind. Wenn der Crawler nicht in der Lage ist, alle vorhandenen Webanwendungen zu crawlen, bleibt Raum für Sicherheitslücken.

Eine weitere wichtige Funktion, auf die Sie achten sollten, ist die einfache Integration mit externen Tools. Dies ist notwendig, wenn Sie einen Großteil des Prozesses automatisieren möchten.

Manuelles Scannen Ihrer Dateien und Datenbanktabellen

Eine weitere Möglichkeit, Malware auf Ihrer Website aufzuspüren und zu entfernen, ist das manuelle Scannen der Website-Dateien. Dies können Sie mit PC-Antivirensoftware wie McAfee und ESET oder dem in Ihrem Betriebssystem integrierten Antivirenprogramm tun - Microsoft Defender für Windows-Benutzer und XProtect für Mac-Benutzer.

Gehen Sie folgendermaßen vor, um Website-Dateien manuell zu scannen:

- Laden Sie alle Dateien über Ihr Hosting Control Panel herunter. Hostinger-Benutzer können Website-Dateien über das Menü Backups im hPanel herunterladen.
- Führen Sie einen vollständigen Scan der Dateien mit der von Ihnen gewählten Antivirus-Software durch.
- Beseitigen Sie alle erkannten Probleme.
- Laden Sie die bereinigten Website-Dateien auf den Server hoch.

Bereinigen Sie als nächstes Ihre Datenbanktabellen mit **phpMyAdmin**. Entfernen Sie alle Datensätze, die verdächtigen Code enthalten, sowie alle neuen Datensätze, die Sie nicht erstellen. Am einfachsten ist es, mit den Tabellen zu beginnen, die bestehende Seiten und Beiträge verwalten (wp-posts und wp-options Tabellen in WordPress).

Website-Besitzer, die keine technischen Kenntnisse haben, finden die oben genannten Methoden möglicherweise schwierig. In diesem Fall ist es am besten, die gehackte Website einem Experten für Cybersicherheit anzuvertrauen. Diese Methode ist zwar kostspieliger als die beiden anderen, garantiert aber eine erfolgreiche Bereinigung und Wiederherstellung Ihrer Website.

Glücklicherweise bieten **zahlreiche Cybersicherheitsagenturen** und **-Spezialisten Bereinigungsdienste für globale Kunden an**. Einige der besten Cybersicherheitsunternehmen sind Sapphire, Palo Alto Networks und Bugcrowd.

Alternativ können Sie auf Job-Such-Websites wie LinkedIn einen Cybersicherheitsexperten finden und ihn als unabhängigen Auftragnehmer einstellen.

Achten Sie bei der Auswahl eines Cybersicherheitsunternehmens oder -experten darauf, dass Sie mit ihm zusammenarbeiten:

- Prüfen Sie den Ruf und das Portfolio des Unternehmens oder Experten.
- Planen Sie ein realistisches Budget ein, damit Sie sich hochwertige Dienstleistungen leisten können.
- Prüfen Sie die Bewertungen des Unternehmens oder des Experten.
- Überlegen Sie, ob Sie leichten Zugang zu einem zuverlässigen Support-Team haben.

Profi-Tipp

Fallen Sie nicht auf niedrige Preise herein, denn das deutet in der Regel auf minderwertige Arbeit hin, die weitere Probleme auf Ihrer Website verursachen kann.

Wiederherstellung eines Backups

Wenn Ihnen die vorangegangenen Methoden zu zeit- oder kostenaufwändig erscheinen, können Sie stattdessen die Sicherungsdatei der Website wiederherstellen. Bei dieser Methode werden alle Daten und Änderungen, die seit der Erstellung des Backups vorgenommen wurden, entfernt, weshalb wir diese Methode nur empfehlen, wenn Sie sich den Datenverlust leisten können.

Aus diesem Grund eignet sich diese Methode am besten für die Reparatur von Websites, die nicht häufig geändert werden oder die zu Testzwecken erstellt wurden.

Profi-Tipp

Löschen Sie nach der Wiederherstellung des Website-Backups den Browser-Cache und leeren Sie den lokalen DNS-Cache, um die Änderungen zu sehen.

10 Scannen Sie Ihren PC mit einer Antivirus-Software

Der letzte Schritt besteht darin, Ihren Computer auf Malware zu scannen, um sicherzustellen, dass der Schädling, der Ihre Website infiziert hat, nicht auch Ihren Rechner gefährdet.

Wir haben bereits McAfee und ESET als Premium-Software empfohlen. Nachfolgend finden Sie einige der besten kostenlosen Antivirenlösungen, aus denen Sie wählen können:

- **AVG Free Antivirus**
- **Avast**
- **Avira Kostenlos**
- **Kaspersky Sicherheits-Cloud**
- **Malwarebytes**

Aktualisieren Sie Ihre Antiviren-Software, bevor Sie einen Scan durchführen.

11 Wie Sie verhindern können, dass Ihre Website in Zukunft gehackt wird

Herzlichen Glückwunsch, Sie sollten die gehackte Website inzwischen wiederhergestellt haben.
Leider gibt es keine Garantie dafür, dass sie in Zukunft nicht wieder angegriffen wird. Es gibt jedoch Möglichkeiten, das Risiko von Cyberangriffen zu minimieren.

Hier sind einige grundlegende Tipps zum Schutz Ihrer Website vor verschiedenen Arten von Malware:

- Nutzen Sie günstige Webhosting-Anbieter mit Bedacht.
- Entfernen Sie veraltete Software, die Sie nicht mehr benötigen.
- Verwenden Sie sichere Passwörter.
- Scannen Sie Ihre Website regelmäßig mit seriöser Sicherheitssoftware.
- Führen Sie regelmäßig Backups Ihrer Website durch.
- Installieren Sie ein SSL-Zertifikat.
- Begrenzen Sie die Anmeldeversuche.
- Aktivieren Sie die Zwei-Faktoren-Authentifizierung.

Wie kommunizieren Sie einen Sicherheitsvorfall an Ihre Besucher?

Ihre Besucher verlassen sich nicht nur auf die Produkte und Dienstleistungen, die Sie ihnen anbieten, sondern erwarten auch, dass Ihre Marke in der Lage ist, ihre Daten zu schützen. Wenn Ihre Website gehackt wird, riskieren Sie, das Vertrauen zu verlieren und die Glaubwürdigkeit Ihrer Marke zu beschädigen.
Dennoch ist es wesentlich besser, Sicherheitsvorfälle transparent zu machen, als sie vor Ihrer Zielgruppe zu verbergen. Dies könnte einen Aufschrei verursachen und Ihrer Marke schaden, aber Sie warnen sie vor der Bedrohung und minimieren den Schaden auf ihrer Seite.

Außerdem sind Sie, wenn Sie dem DSGVO-Gesetz unterliegen, gesetzlich verpflichtet, alle Datenschutzverletzungen, die die Datensicherheit Ihrer Kunden gefährden könnten, zu veröffentlichen.

Wenn Ihre Website kompromittiert wurde, informieren Sie Ihr Publikum in einer offiziellen Mitteilung über die Datenschutzverletzung. Wenn Sie eine E-Mail-Liste haben, senden Sie eine formelle E-Mail mit denselben Informationen an Ihre Abonnenten. Achten Sie darauf, dass sie klar und deutlich formuliert ist, damit auch Kunden mit begrenzten technischen Kenntnissen sie verstehen können.

Der Inhalt der Mitteilung sollte das gesamte Ausmaß der Sicherheitsverletzung erklären, insbesondere die Art der Daten, die durchgesickert sind. Als Nächstes sollten Sie die zur Schadensbegrenzung ergriffenen Abhilfemaßnahmen aufschlüsseln. Ziel ist es, den Zuhörern zu versichern, dass Sie die volle Verantwortung für den Vorfall übernehmen und in ihrem besten Interesse handeln.

12 Fazit

Die rasante Entwicklung von Cyberangriffen stellt eine große Bedrohung für jede Website im Internet dar. Wenn Ihre Website gehackt wurde, ist es am besten, sofort Maßnahmen zu ergreifen und den Schaden zu begrenzen.

Hier eine Zusammenfassung, wie Sie eine gehackte Website reparieren können:

- Ändern Sie Ihre Kennwörter und überprüfen Sie den Benutzerzugang.
- Erstellen Sie eine Sicherungskopie der Website.
- Verfolgen Sie Ihre Aktionen zurück, um die Schwachstellen zu ermitteln.
- Untersuchen Sie die jüngsten Sicherheitsverletzungen im Internet.
- Sprechen Sie mit Ihrem Hosting-Anbieter, um herauszufinden, ob auch andere Nutzer betroffen sind.
- Untersuchen Sie mit Google Blocklist.
- Setzen Sie Ihre .htaccess-Datei zurück.
- Untersuchen Sie die Website und beheben Sie die Sicherheitslücken.
- Scannen Sie Ihren Computer mit Antiviren-Software.

In der digitalen Welt kann es immer zu individuellen Problemen und Lösungen kommen. Wenn Sie schnell, einfach und diskret Handlungsempfehlungen erhalten und gemeinsam mit einem Experten das Problem lösen wollen, erhalten Sie hier eine kostenlose Ersteinschätzung: hilfe@hacker-finden.de.

IT-Hilfe von Experten erhalten

Schnell, einfach & diskret

Wurden Sie gehackt oder erpresst?
Haben Sie den Zugang zu Ihrem Konto verloren?
Müssen Sie sensible Bilder oder Videos entfernen?
Wurde Ihre ID missbraucht?
Wollen Sie eine Beweissicherung für Strafverfolgung?
Möchten Sie Cybermobbing stoppen?
Haben Sie ein Smartphone- oder Computerproblem?
Sind Sie Opfer von Online-Betrug?

Wir helfen Ihr Problem zu lösen

Bei Fragen oder IT-Notfällen einfach ein Online Videogespräch mit einem Experten buchen:
https://www.hacker-finden.de/kontakt/
oder schreiben Sie uns an hilfe@hacker-finden.de

Weitere e-Books: www.hacker-finden.de/ebooks
Weitere Informationen: www.hacker-finden.de

Es gibt Situationen, die sehr fortgeschritten sind und bei denen bestimmte Arten von Online-Schwachstellen oder Hacker-Angriffen die Schadensursache sein können. Wenn die Best-Practice-Schritte nicht zur Behebung führen oder Sie Informationen über den Täter herausfinden wollen, buchen Sie sich eine persönliche kostenlose Ersteinschätzung mit einen Experten:

JETZT STARTEN

HACKER FINDEN.DE Powered by Audat