mijndomein

Dé checklist om je website gemakkelijk en snel te beveiligen

Maak jij het hackers te makkelijk?

Cybercrime blijft dagelijks groeien en hackers worden steeds beter in wat ze doen. Het aantal cyberaanvallen dit jaar ten opzichte van 2021 is met maar liefst 32% (!) gestegen binnen verschillende organisaties. Voorkom dat criminele hackers je website misbruiken. Worst case scenario: je raakt je website kwijt. De hoogste tijd dus om kritisch naar je website beveiliging te kijken en onze checklist na te lopen. Hoeveel kan jij er al afvinken?

- ☐ **Maak (lokale) back-ups van je website**. Misschien wel de belangrijkste tip van deze checklist. Op deze manier kun je je website altijd nog op een oudere versie terugzetten, mocht er ingebroken worden.

- ☐ **Goede hosting**. Waar draait jouw website? Heb je webhosting, dan is het belangrijk dat de partij bij wie je dat afneemt betrouwbaar en veilig is. Verzorgen wij jouw webhosting, weet dan dat veiligheid en betrouwbaarheid bij ons hoog in het vaandel staan. We kunnen niet specifiek ingaan op hoe we onze servers precies beschermen, omdat hackers het dan vaak als een uitdaging zien om daar langs te komen.

- ☐ **Kies een veilig CMS (Content Management Systeem)**. Er zijn tegenwoordig talloze CMS systemen waar je uit kunt kiezen, zoals Wordpress of Joomla. De vuistregel is wanneer ze open source zijn, er een grote community aan werkt en er regelmatig updates uitgebracht worden, de kans op kwetsbaarheden relatief hoog zijn, maar doe altijd goed onderzoek.

- ☐ **Kies een sterk wachtwoord.** Geboortedatums, ‘Wachtwoord1234’ en de naam van je huisdier kunnen echt niet meer. Er zijn tegenwoordig handige website extensies en apps (b.v. Google Password) om je wachtwoorden op een veilige plek op te slaan. Ook geven ze wachtwoord suggesties voor een sterke beveiliging.

- ☐ **Update je website.** De techniek verandert en hackers worden steeds slimmer. Die bedenken nieuwe manieren om je website te infiltreren en CMS-aanbieders spelen daar op in. Ze brengen regelmatig updates uit om jouw website zo veilig mogelijk te houden. Update je niet, dan is jouw website kwetsbaar voor aanvallen. Wij raden aan om minimaal één keer per maand te controleren op updates.

- [ ] **Werk altijd met een veilige internetverbinding.** Of je nu thuis werkt, op een openbare locatie of op je werk; het is belangrijk om altijd te werken op een beveiligd netwerk. Zorg er dus altijd voor dat je wifi goed beveiligd is en er geen virussen op je computer staan. Installeer hiervoor virusscanners en check regelmatig op virussen.

- [ ] **Houd je website schoon en overzichtelijk.** Werk je met een CMS dat werkt met extensies en plugins? Check regelmatig of deze nog up-to-date zijn én of je ze daadwerkelijk gebruikt. Hoe meer plugins, hoe groter de kans op inbreuken van buitenstaanders. Ook wel fijn; je website wordt sneller door het verwijderen van overbodige plugins.

- [ ] **Gebruik reCAPTCHA**. De laatste op het lijstje, maar onmisbaar. Misschien heb je er nog nooit van gehoord, geen zorgen! reCAPTCHA is een beveiligingsvorm van Google die checkt of een echt mens een formulier invult of een spambot. Aanklikken hoeveel palmbomen of zebrapaden je ziet? Dat is dus reCAPTCHA! Nog meer redenen waarom je reCAPTCHA moet gebruiken, lees je **hier**.

Dat waren onze 8 tips om jouw website zo veilig mogelijk te maken! Mocht je alle bovenstaande problemen nou voor willen zijn of vind je de beveiliging van je website in eigen beheer toch wat te spannend vinden? Kies dan voor onze veilige **Webhosting** pakketten.