Quelles sont les meilleures astuces pour sécuriser son site internet ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Quelles sont les meilleures astuces pour sécuriser son site internet ?				

Vous souhaitez sécuriser votre site internet des attaques ? voici nos conseils pour protéger vos données des cybercriminels.

Quelles sont les meilleures astuces pour sécuriser son site internet ?

Avec Internet, nous avons vu arriver la cybercriminalité. Cette nouvelle forme de criminalité utilisant les réseaux de communication s'est développée au fil des années et fait toujours plus de victimes. Même si votre site est petit et ne génère pas beaucoup de visites, il n'est pas à l'abri d'un piratage.
C'est pourquoi il vous faut appliquer certaines mesures de sécurité. Ces sécurités donneront beaucoup de fil à retordre aux pirates venus mettre à mal votre site. Mais quelles sont les sécurités à mettre en place ? Thibaut, auteur du blog Bonjour Rome, nous livre toutes les astuces à mettre en place pour sécuriser votre site internet.

Sécuriser son site, des protections simples à mettre en place

Il existe des solutions très simples à mettre en place pour sécuriser votre site. Parmi ces solutions nous pouvons retrouver :
• Le choix de votre hébergeur ;
• L'utilisation de plug-in de sécurité ;
• La mise en place de mots de passe complexes ;
• Le choix d'un mot de passe que vous n'utilisez nulle part ailleurs.
Le choix de votre hébergeur est un point important si vous lancez votre site internet. Ne vous lancez pas tête baissée chez le premier hébergeur web que vous trouverez. Choisir un hébergeur de site web pour son prix est souvent une mauvaise idée. Vérifiez quelles fonctionnalités de sécurité il met à votre disposition. Un serveur SSL sécurisé est le minimum à attendre d'un hébergeur.
Thibaut pour son blog sur Rome a choisi WP Engine, qui est relativement cher mais hyper professionnel. Il optimise la sécurité de votre site et le service client est hyper réactif en cas de problème ou de bug ou d'attaque informatique lié à votre site.
Utiliser un plug-in de sécurité vous aidera aussi à vous protéger des cyberattaques. Ces plug-ins vous sont disponibles si vous utilisez WordPress. Nous pouvons notamment retrouver les plug-ins Jetpack, Secupress ou encore Wordfence Security qui font partit des meilleurs plug-ins de sécurité du moment. De plus, l'installation de ce genre de plug-in ne vous demandera pas de compétences informatiques particulières, WordPress étant l'outil le plus simple pour mettre son site web en ligne.
Enfin, **la mise en place de mots de passe complexe ajoutera grandement à la sécurité de votre site**. Pour créer un mot de passe complexe, vous devrez mélanger les minuscules, les majuscules et ajouter des caractères spéciaux et des chiffres. N'utilisez pas le prénom de vos enfants ou de votre animal de compagnie, les pirates ont généralement accès à ce genre d'informations personnelles.

Améliorer la sécurité de son site, les protections plus complexes

Si vous voulez renforcer la sécurité de votre site web, il va falloir passer par des mesures plus complexes. Vous pourrez :
• Installer un format HTTPS
• Vous protéger des attaques SQL
• Vous protéger des attaques XSS

Le HTTPS, ou protocole de transfert hypertexte sécurisé, rend votre site beaucoup plus sécurisé. Ce protocole est fortement conseillé si vous possédez un site d'e-commerce. Il permettra de sécuriser vos données et celles de vos clients.
Les attaques SQL sont très dangereuses pour votre site. Les pirates qui utilisent l'injection de SQL sont ensuite capables de voler toutes vos informations personnelles présentes sur votre site. Pour s'en protéger, il vous faudra utiliser des requêtes paramétrées. La requête paramétrée vous demandera de mettre certaines informations entre crochets pour pouvoir la sécuriser.
Si vous utilisez WordPress, ce qui est aujourd'hui le cas pour la majorité des blogueurs, vous pouvez utiliser le plugin gratuit que Thibaut utilise pour son blog Bonjour Rome : https://fr.wordpress.org/plugins/really-simple-ssl/
Il faut avoir le certificat SSL (fourni par la majorité des hébergeurs comme OVH), mais le reste est automatique. Une fois installé, un petit verrou apparaît à gauche de votre URL dans la barre de recherche.
Enfin, il vous faudra aussi **vous protéger des attaques XSS**. Ces dernières sont similaires aux attaques SQL mais sont beaucoup plus violentes. Pour les éviter, il faudra vous assurer que les visiteurs de votre site n'ont pas la possibilité d'insérer des tags JavaScript sur votre site.
En mettant en place tous ces conseils, votre site web aura plus de chances de résister aux attaques des cybercriminels. Vos données et celles des utilisateurs de votre site seront protégées et vous pourrez développer votre site en toute quiétude.

Auteur : *Thibaut, auteur du blog Bonjour Rome*

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous