امنیت در وبلاگ نویسی

www.HiProgram.ir

فهرست مطالب

سخن گرداورنده

سلام خدمت شما دوستان عزیز این کتاب آموزشی توسط تیم درسنامه نوشته و توسط تیم سلام برنامه و شخص امیر عباس سعدی گرداوری شده است تمامی مباحث آموزش امنیت در وبلاگ نویسی در این کتاب آورده شده است از شما دوستان عزیز خواهشمندیم در صورت انتشار کتاب حتما منبع آن را قید کنید

این کتاب توسط آدرس اینترنتی http://hiprogram.ir انتشار پیدا کرده است.

درس اول–چگونگی انتخاب یک سیستم عامل امن و مناسب

شاید در نگاه اول طرح چنین موضوعی در مبحث امنیت وبلاگ نویسی چندان به جا و مناسب به نظر نرسد. خب، مگر انتخاب سیستم عامل چه ربطی به امنیت وبلاگ دارد؟ چه فرقی می کند که من از ویندوز استفاده می کنم یا لینوکس؟ مگر برای وبلاگ نویسی میان مک و لینوکس تفاوتی وجود دارد؟ چرا باید خودم را به دردسر انداخته و از ویندوز به لینوکس یا مکینتاش مهاجرت کنم؟ ویندوز، ویندوز است دیگر! حالا چه نسخه ای داشته باشیم که دیگر بستگی کامل به سلیقه مان دارد!

در اولین درس این دوره می خواهیم کمی دقیق تر به مساله سیستم عامل بپردازیم، تا ببینیم چرا باید در این خصوص هم نگران و مراقب باشیم. شاید اولین و مهمترین نکته در امنیت یک وبلاگ نویس حرفه ای، انتخاب سیستم عامل باشد.

همان گونه که می دانید، سیستم عامل های مختلف از سطوح امنیتی متفاوتی بهره می برند و در کنار بدافزار و ویروس های متنوع، انواع گوناگونی از برنامه های امنیتی هم برای آنها در بازار وجود دارد. پس یک وبلاگ نویس که اهمیت بالایی برای امنیت خود و وبلاگش قایل است، باید در اولین قدم سیستم عاملی را انتخاب کند که از امنیت مناسبی برخوردار بوده و با کمترین میزان تهدیدات و ایرادها روبرو باشد. در ادامه به بررسی نقاط قوت و ضعف سیستم عامل های مختلف می پردازیم تا ببینیم کدام یک می تواند انتخاب مناسبی باشد.

احتمالا شما قبل از اینکه تصمیم به وبلاگ نویس شدن بگیرید، کامپیوتر یا لپ تاپ شخصی خودتان را داشته اید و کمتر کسی پیدا می شود که به صورت اختصاصی برای وبلاگ نویسی به دنبال خرید یک سیستم جدید باشد. اما سیستم عامل می تواند تاثیر فراوانی در کارآیی، امنیت و حتی خلاقیت یک وبلاگ نویس حرفه ای داشته باشد.

هنگام انتخاب یک سیستم عامل مناسب چندین عامل می توانند تاثیر گذار باشند:

۱ -اینکه شما قرار است چه استفاده هایی از کامپیوتر یا لپ تاپ تان داشته باشید. آیا این دستگاه به طور اختصاصی متعلق به مدیریت وبلاگ و سایت شما است؟ یا اینکه کارهای اداری و شغلی تان را هم باید انجام دهد؟ شاید قرار است ابزار بازی و سرگرمی تان هم باشد؟

۲ -به چه نرم افزارهایی جهت انجام کارهای تان نیاز دارید؟ پاسخ به این سوال، بستگی زیادی به سوال قبل دارد. بسته به اینکه چه نوع کاربردی را از دستگاه تان انتظار دارید، نوع برنامه های مورد استفاده تان هم تعیین می گردد. زیرا در صورت استفاده از برخی برنامه های خاص که تنها برای سیستم عامل ویژه ای تولید شده اند، مجبور به استفاده از همان سیستم عامل هستید.

۳ -میزان تبحر شما در استفاده از هر سیستم عامل و به اصطلاح گیک بودن تان در زمینه کامپیوتر هم گزینه تعیین کننده دیگری است. البته این موضوع که تا چه میزان علاقه مند به یادگیری و کسب مهارت در کار با برنامه ها و سیستم عامل های جدید هم باشید، در این امر دخیل است. گاهی به دلیل ناآشنا بودن یک سیستم عامل ممکن است چشم تان را بر روی همه خوبی های آن ببندید و سراغ یک سیستم عامل راحت و آشنا، ولی مشکل دار بروید. یا اینکه سختی های چند ماهه یادگیری سیستم عامل جدید را به جان خریده و در ازای آن مزایا و امکانات تازه فراوانی به دست آورید.

یکی از مهمترین گزینه ها در انتخاب سیستم عامل، که در اینجا اهمیت دو چندانی پیدا می کند، امنیت آنها است. همه شرکت های سازنده سیستم عامل تلاش می کنند که تا حد ممکن امن ترین سیستم عامل را در اختیار کاربران شان قرار دهند .اما با توجه به مسایلی همچون تعداد کاربران، میزان توجه هکرها و افراد نفوذگر به آن سیستم عامل، باگ ها و ایرادات سیستم عامل و همچنین سوراخ های امنیتی برنامه های جانبی یک سیستم عامل، می توان آنها را دسته بندی نموده و بر حسب امنیت و با توجه به امکانات موجود، دست به انتخاب زد. توصیه ما هم به وبلاگ نویس های حرفه ای آن است که بیشترین توجه را به این مورد داشته باشند.

ویندوز

ویندوز، سیستم عاملی همه گیر است که بیشترین کاربرد را در دنیای کامپیوتر و لپ تاپ دارد و تقریبا همه شما هم اکنون با آن کار می کنید و یا قبلا کار کرده اید. این سیستم عامل سازگاری بسیار خوبی با سخت افزارهای متنوع و متعدد موجود در بازار داشته و نرم افزارهای بسیار زیادی در زمینه های مختلف برای آن نوشته شده است. تقریبا برای انجام هر کاری می توانید برنامه های رایگان و غیررایگان متعددی بیابید که امکان انتخاب خوبی را به شما می دهند.

کار با آن نسبت به دیگر سیستم عامل های مشهور، ساده تر است. در صورت بروز هرگونه مشکل و یا مواجه شدن با ایرادی، افراد بسیار زیادی در اطراف تان هستند که می توانید از آنها کمک بگیرید. نرم افزار، سخت افزار، وسایل جانبی و متخصصان آن را تقریبا در هر جایی می توان یافت و هیچ گاه از این نظر با مشکل روبرو نمی شوید.

به دلیل گستره بسیار وسیع کاربران و همچنین باگ های موجود در برنامه های نوشته شده برای آن، این سیستم عامل بسیار مورد توجه هکرها و افراد خرابکار بوده و تقریبا هدف اصلی آنها در دنیای دیجیتال است. البته به همان نسبت هم تعداد برنامه های امنیتی، فایروال و آنتی ویروس رایگان و غیر رایگان خوب، برای این سیستم عامل وجود دارد. اما در صورتی که اهل راحت طلبی نباشید و بخواهید کمی به خودتان سخت بگیرید، ویندوز انتخاب اول درسنامه برای یک وبلاگ نویس حرفه ای نیست.

البته در صورتی که امکان فنی یا وقت لازم برای کوچ به سیستم عامل دیگری همچون لینوکس یا مک را ندارید، با به کار بستن برخی نکات امنیتی می توانید ویندوز را هم تبدیل به سیستم عامل قابل قبولی برای وبلاگ نویسی امن کنید:

۱ -تا حد امکان از سیستم خود تنها و تنها برای یک کار، و آن هم وبلاگ نویسی استفاده کنید. وقتی قرار باشد چند کار با یک لپ تاپ یا کامپیوتر انجام شود، جابجایی اطلاعات با افراد و گروه های مختلف، از طریق ابزارهای گوناگون می تواند نقطه ضعف امنیتی بزرگی برای سیستم شما باشد. شاید شما در ایمنی ایمیل متعلق به وبلاگ و یا کول دیسک حاوی اطلاعات آن دقت کنید، ولی کم کاری در توجه به امنیت هارد دیسک آرشیو فیلم، یا ایمیل مرتبط با کار شرکت و یا ایمیلی که مطالب سایت های سرگرمی را با آن دریافت می کنید، می تواند به نقطه شروعی جهت حمله به وبلاگ تان تبدیل شود.

۲ -همیشه از آخرین نسخه سیستم عامل ویندوز استفاده کنید. **ویندوز XP یکی از بدترین سیستم عامل های موجود در مقابل حملات امنیتی است** و تقریبا شما را تبدیل به یک سرباز بی سلاح در میان خیل عظیم دشمنان می کند. علی رغم حل بسیاری از مشکلات امنیتی آن در طول زمان، هنوز یکی از ناامن ترین انتخاب های ممکن است. پیشنهاد ما برای وبلاگ نویسی با سیستم عامل ویندوز، حتما و حتما انتخاب ویندوز ۷ است. این سیستم عامل به ابزارهای کنترلی و امنیتی درونی فراوانی مجهز شده است، که کمک زیادی به محافظت از شما در برابر حملات می کنند.

۳ -همیشه آپدیت ها و به روز رسانی های سیستم عامل را نصب کنید. این موضوع در خصوص همه سیستم عامل ها صدق می کند. زیرا شرکت های سازنده، دائما در حال رفع باگ و نقص های امنیتی هستند و مرتبا آنها را در قالب آپدیت و پچ های نرم افزاری عرضه می کنند.

۴ -از برنامه های امنیتی همچون آنتی ویروس، آنتی اسپای ور و فایروال استفاده کنید. این برنامه ها مرتبا سیستم شما را کنترل کرده و تا حد زیادی جلوی نفوذ بدافزارها و برنامه های مخرب به کامپیوتر شما را می گیرند. علاوه بر دقت در انتخاب برنامه مناسب و با کارایی بالا، دقت داشته باشید که همیشه آنها را به روز نگه دارید. زیرا تعداد برنامه های مخرب روز به روز در حال افزایش است و شرکت های سازنده برنامه های امنیتی هم همیشه با تولید ابزارهای شناسایی و حذف

آنها، برنامه های خود را به روز می کنند. از آنجایی که این دوره به صورت تخصصی به امنیت در سیستم عامل ویندوز نمی پردازد توصیه می کنیم حتما در دوره مبانی امنیت در کامپیوتر و اینترنت درسنامه شرکت کنید.

سیستم عامل Mac OS X

این سیستم عامل توسط شرکت اپل به صورت اختصاصی برای نصب بر روی کامپیوتر و لپ تاپ های تولید اپل، ساخته شده است. بنابراین برای استفاده از آن، بهترین گزینه خرید یک لپ تاپ (مک بوک) یا کامپیوتر رومیزی (آی مک) اپل است. البته محصولات این شرکت نسبت به تولیدات دیگران تا حدی گران تر هستند.

مک او اس X بر پایه سیستم عامل یونیکس است و از این لحاظ تقریبا منشا یکسانی با لینوکس دارد. به دلیل گستردگی پایین تر و تعداد کمتر کاربران، میزان توجه هکرها و سازندگان بدافزار هم به این سیستم عامل کمتر از ویندوز است. و البته به همان نسبت هم تعداد توسعه دهندگان برنامه های مربوط به آن کمتر است و نرم افزارهای کمتری نسبت به ویندوز برای آن تولید شده و در دسترس است.

همچنین به دلیل پایین بودن تعداد کاربران معمولا هنگام برخورد با مشکلات، خودتان یک تنه باید با آنها دست و پنجه نرم کنید و در میان اطرافیان تان کسی نمی تواند به یاری تان بیاید، هر چند که به لطف اینترنت و گسترش محتوای فارسی، می توانید منابع کمکی خوبی را در این مورد پیدا کنید.

این سیستم عامل به دلیل مکانیزم حمایت از فایل های سیستمی جدای از حق دسترسی به فایل های کاربر، امنیت نسبتا خوبی را دارد. اپل هم تلاش فراوانی برای تامین حداکثر امنیت ممکن در سیستم عامل خود نموده است و معمولا باگ امنیتی زیادی در نسخه های این سیستم عامل دیده نمی شود. اما باید توجه داشته باشید که افسانه امنیت ۱۰۰ درصد و کامل مکینتاش، تنها جنبه تبلیغاتی و شایعه داشته و به هیچ وجه صحیح نیست. ولی همان طور که گفتیم، در کنار

وسواس اپل بر روی امنیت محصول خود، خرابکاران اینترنتی هم معمولا به دلیل تعداد کم کاربران، چندان انرژی خود را صرف این سیستم عامل نمی کنند. پس تعداد بدافزارها و ویروس های موجود برای مک او اس نسبت به ویندوز کمتر است.

به همین دلیل، در صورتی که قصد خرید یک لپ تاپ یا کامپیوتر جدید دارید و در کنار آن به امنیت بیشتر در وبلاگ نویسی می اندیشید، MacBook و iMac می تواند گزینه های مناسب، زیبا و البته کمی گرانقیمتی برای شما باشند. در صورتی که این سیستم عامل را انتخاب کردید، شرکت در دوره آموزشی مبانی امنیت در سیستم عامل مک درسنامه را فراموش نکنید.

سیستم عامل لینوکس

یکی دیگر از سیستم عامل های مطرح فعلی دنیا که اتفاقا در میان بلاگرها هم به خوبی جای خود را باز کرده، لینوکس است. کاربران و طرفداران آن بیشتر به طرفداری از رعایت حقوق تولید کننده و دنیای نرم افزارهای باز متن مشهورند . زیرا اصل لینوکس بر باز متن بودن و تا حد فراوانی رایگان بودن است. هم اکنون هم نسخه های بسیار فراوانی از آن را می توانید بیابید که به صورت رایگان و یا هزینه بسیار کمی به صورت قانونی قابل تهیه هستند.

دیگر مزیت لینوکس این است که معمولا شما برای هر نوع سخت افزار و کامپیوتری می توانید یک نسخه مناسب از این سیستم عامل را بیابید. خواه لپ تاپ شما دارای آخرین نوع پردازنده Core i7 اینتل باشد و یا اینکه همچنان از یک سلرون ۲۳۳ بهره ببرید. اینکه کامپیوترتان ۸ گیگابایت رم داشته باشد یا فقط یک رم ۲۶۵ مگابایتی روی آن سوار باشد. بالاخره نسخه ای از لینوکس را می یابید که به آسانی روی آن بالا آمده و با راحتی کامل جواب نیازهای تان را بدهد.

در گذشته کابران لینوکس بیشتر به دانش بالای کامپیوتری و استفاده دائمی از خط فرمان مشهور بودند. کاربران عادی هم می ترسیدند طرف این سیستم عامل قدرتمند و سخت بروند و همگان فکر می کردند که یادگیری آن مستلزم به خاطر سپردن تعداد زیادی دستورات مختلف است و انجام هر کاری تنها از طریق تایپ آن در خط فرمان امکان پذیر می شود. اما در سال های اخیر شرکت های زیادی مشغول تولید لینوکس با رابط کاربری گرافیکی شده اند که کار را برای کاربر تازه کار و معمولی بسیار آسان نموده و محیط کاری را به ویندوز و مک او اس شبیه کرده است.

از نظر امنیتی، اغلب لینوکس را یکی از امن ترین سیستم عامل ها می دانند. حتی برخی آن را از سیستم عامل اختصاصی اپل هم امن تر و غیرقابل نفوذتر می دانند. البته لینوکس به دلیل متن باز بودن و امکان تنظیمات گسترده توسط کاربر برای کارهای مختلف، کمی از این نظر خطرناک است. اگر توسط یک کاربر خبره و ماهر تنظیمات امنیتی آن به درستی انجام شوند، نیاز چندانی به برنامه های ویژه امنیتی و آنتی ویروس نخواهد داشت و از هر سیستم عامل دیگری می تواند امن تر باشد. اما در صورتی که تنظیمات آن اشتباه باشند، حتی ممکن است نفوذ به آن از ویندوز XP هم راحت تر باشد. با این حال استفاده از نسخه های مطمئن لینوکس، هم چون اوبونتو و ردهت، مطمئنا امنیت بالاتری نسبت به ویندوز در اختیار شما قرار می دهد. اما باید تاکید کنیم که لینوکس هم مانند مک او اس از امنیت ۱۰۰ درصد و کامل برخوردار نیست.

لطفا این نکته را همیشه و همه جا به خاطر داشته باشید: عبارات امنیت ۱۰۰ درصد، امنیت کامل، رمز عبور یا کامپیوتر غیرقابل نفوذ و مانند آن تنها یک افسانه و دروغ تبلیغاتی هستند .ما تنها می توانیم سعی کنیم کار را برای افراد نفوذگر سخت و سخت تر کنیم تا از خیر کارشان گذشته و دست از سرمان بردارند. اما در دنیای امنیت هیچ امر غیر ممکنی وجود ندارد. یک نفوذ با ۱ دلار هزینه و یک ساعت وقت انجام می شود و یک نفوذ هم با ده میلیون دلار هزینه و ده سال وقت!

اگر قصد خرید لپ تاپ و کامپیوتر جدید ندارید، اما می خواهید یک سیستم اختصاصی برای وبلاگ نویسی تان آماده کنید. بهترین گزینه می تواند فرمت کردن کامل کامپیوتر و حذف تمام فایل ها و بدافزارهای احتمالی باشد. آنگاه با نصب آخرین ورژن از یک لینوکس خوب و انجام تنظیمات لازم، امنیت شما به میزان بسیار زیادی افزایش می یابد.

درست است که کاربران لینوکس هم مانند مک او اس چندان در اطراف شما زیاد نیستند، اما مهمترین برتری لینوکس، فروم ها و گروه های کاربری فعال فارسی زبان آن است که کاربران کاملا حرفه ای آن در کوتاه ترین زمان، معمولا برای همه مشکلات شما راه حلی در آستین دارند.

خب انتخاب شما برای سیستم عامل وبلاگ نویسی تان چیست؟ قدم اول را همین امروز برداشته و سیستم عامل تان را انتخاب کنید. به گمان مان این گونه برای طی دوره هم آماده تر خواهید بود. تنها یک بار دیگر تاکید می کنیم: جدا از اینکه کدام سیستم عامل را انتخاب می کنید، از نصب آپدیت های سیستم عامل و نرم افزارهای نصب شده بر روی آن غافل نشوید. حتما از برنامه های امنیتی استفاده کنید (مخصوصا در ویندوز)، همیشه آنرا را به روزرسانی کنید. از نصب نرم افزارهای قفل شکسته (کرک شده) خودداری کنید و اگر هم انتخاب اول و آخر شما ویندوز است، لطفا و تحت هیچ شرایطی طرف ویندوز XP نروید. ویندوز ۷ را برای شما ساخته اند.

درس دوم– انتخاب میان سرویس های وبلاگ نویسی رایگان یا سایت شخصی

برای شروع وبلاگ نویسی معمولا گزینه های بسیار زیادی پیش روی شما قرار دارد .سایت های ایرانی و غیر ایرانی فراوانی سرویس های وبلاگ نویسی با امکانات جذابی را ارائه کرده و وبلاگ اختصاصی رایگانی را در اختیار شما می گذارند .در کنار آن می توانید با هزینه ای مناسب و خرید یک دامنه دلخواه و حجم مناسب هاست، سایت اختصاصی خود را راه اندازی کرده و وبلاگ نویسی را آغاز کنید.

اما واقعا بهترین انتخاب کدام است؟ چه گزینه هایی را در تصمیم گیری باید دخیل بدانیم؟ آیا پرداخت هزینه سالیانه برای سایت شخصی معقول و مقرون به صرفه است، یا باید به همان سرویس های رایگان اکتفا کنیم؟ و مهمتر از همه اینکه کدام یک امنیت بیشتری دارند؟ و در میان انواع سرویس های رایگان یا برنامه های مدیریت محتوای سایت یا وبلاگ (CMS)، کدام یک را باید انتخاب کرد تا امنیت ما و مطالب مان تا حد لازم تامین شود؟ در این درس قصد داریم به صورت خلاصه همین سوالات را دنبال کرده و پاسخ مناسبی برای آنها بیابیم. لذا ابتدا به بررسی سرویس های وبلاگ نویسی عمومی پرداخته و سپس سراغ سایت شخصی می رویم. در انتها هم نتیجه گیری و مقایسه امنیتی میان این دو را خواهیم داشت.

سرویس های وبلاگ نویسی عمومی

امروزه با کمی جستجو در اینترنت می توانید ده ها سرویس ارائه دهنده خدمات وبلاگ نویسی رایگان را بیابید که هر کدام امکانات و قابلیت های جذاب و گوناگونی را هم در اختیارتان می گذارند. در این میان شرکت های ایرانی هم حضوری فعال داشته اند و نام های فراوانی در حال رقابت با یکدیگر هستند. اما از آنجایی که در این دوره درباره امنیت وبلاگ نویسی صحبت می کنیم، بیشتر از جنبه امنیت عمومی، امنیت محتوا و اطلاعات کاربری به سرویس های مختلف نگاه می کنیم و چندان در خصوص امکانات و قابلیت های سرویس های وبلاگ نویسی صحبت نمی کنیم.

بگذارید در ابتدا یک نکته مهم را یادآوری کنیم. وقتی شما از سرویس های رایگان استفاده می کنید چه ایرانی و چه خارجی باید در حیطه قوانین و مقررات آن سرویس وبلاگ نویسی و کشوری که در آن قرار گرفته عمل کنید و به قوانین آن احترام بگذارید. برای مثال اگر یکی از سرویس های وبلاگ نویسی ایرانی استفاده می کنید باید علاوه بر اینکه به موضوع امنیت کلی آن سرویس توجه می کنید، این نکته را در نظر داشته باشید که مطالب شما بایستی با رعایت و احترام به قوانین کشور ایران باشند. این موضوع در مورد استفاده از سرویس های وبلاگ نویسی خارجی هم صادق است و در صورت تخلف از قوانین هر کدام از سرویس ها امکان پیگیری های رسمی و قضایی در مورد نوشته های شما وجود خواهد داشت.

سرویس های وبلاگنویسی متنوعی وجود دارند که حتما نام برخی از آنها به گوش شما خورده است. اما در میان آنها دو گزینه هستند که بیش از همه مشهور شده و محبوبیت فراوانی پیدا کرده اند.

سرویس Blogger متعلق به گوگل و از قدیمی ترین سرویس های وبلاگ نویسی رایگان است. از بهترین مزایای بلاگر، راحتی کار و تنظیمات بسیار آسان و سریع آن است. خدمات این سرویس دهنده رایگان بوده و از نظر آپ تایم (Uptime) بهتر و دسترسی دائم به وبلاگ، یکی از مطمئن ترین سرویس های موجود است (منظور از آپ تایم همان مدت زمان در دسترس بودن وب سایت/ وبلاگ یا به اصطلاح بالا بودن وب سایت است .(این سرویس از نظر امکانات نیز بسیار خوب و متنوع عمل کرده است و البته همانطور که گفتیم برای مقایسه فنی و... بهتر است سراغ دوره آموزش وبلاگ نویسی درسنامه بروید . این سرویس دهنده از زبان فارسی هم به طور کامل پشتیبانی کرده و حتی می توانید محیط مدیریتی و منوهای آن را هم فارسی کنید.

از نظر امنیتی هم با توجه به قرار داشتن داده های شما بر روی سرورهای شرکت گوگل، می توانید با خیال نسبتا آسوده به استفاده از آن پرداخته و تقریبا نگران حملات معمول به سایت ها نباشید. البته بخشی از امنیت که به خود شما بر می گردد، همچنان می تواند یک نقطه ضعف برای وبلاگ تان محسوب شود.

دیگر سرویس محبوب وبلاگ نویسان، Wordpress است که توانسته به رقیبی جدید برای بلاگر گوگل تبدیل شود. این سرویس علاوه بر ارائه خدمات رایگان برای وبلاگ نویسی، به عرضه برنامه مدیریت محتوای رایگان برای راه اندازی وبلاگ بر روی هاست شخصی هم می پردازد. برای کسانی که می خواهند مقداری از وقت شان را جهت یادگیری امکانات و قابلیت های جدید بگذارند و در ازای آن امکانات فراوان و حرفه ای تری به دست آورند، سرویس وبلاگ نویسی وردپرس می تواند یک انتخاب مناسب باشد. در وردپرس شما ابزارهای بیشتری برای کار با محتوا، ویجت های گسترده تر، دسترسی بهتر به شبکه های اجتماعی و امکان شخصی سازی بیشتر هر بخش را در اختیار خواهید داشت.

به دلیل استفاده از سرورهای امن و برنامه مدیریت محتوای مطمئن، این سرویس هم از امنیت بالا و قابل قبولی برخوردار است. البته هنگام انتخاب میان یکی از این دو سرویس دهنده، نیاز نیست از نظر امنیت چندان نگرانی به خود راه داده و به بررسی بپردازید. بلکه تنها به مقایسه امکانات مورد نظرتان جهت وبلاگ نویسی پرداخته و دست به انتخاب بزنید.

البته یکی از مزیت های مهم بلاگر که ممکن است انتخاب را برای شما راحت تر کند، امکان اتصال رایگان دامنه دلخواه است. به صورتی که از آن پس آدرس شما به جای زیر دامنه ای از سایت بلاگ اسپات، تبدیل به آدرس مستقیم و دلخواهی می شود که خودتان خریداری کرده اید. اما انجام این کار در وردپرس مستلزم پرداخت هزینه سالیانه ای در حدود ۱۲ دلار است.

یک نکته مهم را فراموش نکنید که امنیت در وبلاگ نویسی شامل دو بعد اصلی است:

۱ -اینکه چقدر شما اصول و قوانین امنیتی را رعایت کنید؛ این شامل موارد متعددی می شود که در این دوره به آن می پردازیم، مانند سیستم عاملی که که با آن به اینترنت متصل می شوید، امنیت مروگر و. ...

۲ -اینکه سیستم وبلاگ نویسی شما و سروری که آن را میزبانی می کند چقدر از نظر امنیتی کامل و قدرتمند باشد. وقتی از یک سیستم وبلاگ نویسی رایگان استفاده می کنید، پرداختن به این بُعد از امنیت به عهده شما نیست و سرویس دهنده وبلاگ این موضوع را کنترل می کند. این کار مزایا و معایب خودش را دارد. اگر شما از یک سرویس دهنده قدرتمند استفاده کنید خیالتان تا حد زیادی از این مورد راحت خواهد بود. در این مورد هم بیشتر صحبت خواهیم کرد.

خرید هاست اختصاصی و راه اندازی سایت شخصی

گزینه دیگری که برای راه اندازی یک وبلاگ پیش روی شما است، خرید یک فضای اختصاصی در اینترنت (هاست) و یک نام ویژه برای خود (دامنه) و راه اندازی سایت و وبلاگ اختصاصی خودتان است. با انجام این کار دست شما برای هرگونه تنظیمات و استفاده از امکانات مختلف باز است. می توانید برنامه های مدیریت محتوای مختلف را انتخاب کرده و قالب های متنوعی را امتحان کنید. قالب اختصاصی خودتان را طراحی کرده یا گالری عکس و پادکست تان را روی هاست خود راه اندازی و مدیریت کنید.

هزینه انجام این کار هم با توجه به میزان فضای مورد نیاز و شرکتی که انتخاب می کنید، چندان زیاد نخواهد بود و معمولا به صورت سالیانه پرداخت می گردد. اما در صورتی که اهمیت فراوانی برای امنیت وبلاگ تان و محتوای آن قائل هستید، این هزینه ها تا حد زیادی بالا می رود. اما در قبال آن، از سرورهای بسیار امن تر و با خدمات پشتیبانی بهتری بهره می برید که احتمال وقوع مشکل برای وبلاگ شما را تا حد زیادی کاهش می دهد.

البته در کنار انتخاب هاست امن و مطمئن، نکته بعدی انتخاب برنامه مدیریت محتوا یا CMS با امنیت بالا و پشتیبانی مناسب است که بتوان با اتکا به آن با خیالی آسوده به استفاده از وبلاگ پرداخت. امروزه انواع مختلفی از برنامه های مدیریت محتوا جهت وبلاگ نویسی و مدیریت سایت وجود دارد که بسیاری از آنها هم رایگان هستند. از مهمترین و معروف ترین این برنامه ها می توان به نام هایی همچون وردپرس، دروپال، جوملا و موویبل تایپ اشاره کرد. از آنجایی که صحبت درباره جزئیات این برنامه ها در موضوع درس ما نیست، تنها به این نکته اکتفا می کنیم که از نظر امنیت و کارکرد، بهترین گزینه های موجود برای شما وردپرس خواهد بود که به صورت اختصاصی روی یک سیستم وبلاگ نویسی تمرکز کرده است. در کنار آن استفاده از دروپال به شما امکان توسعه بیشتری را خواهد داد، اما بیشتر برای کسانی مفید است که به دنبال راه اندازی یک وب سایت با امکانات متنوع هستند.

انتخاب میان سایت شخصی و سرویس های عمومی از نقطه نظر امنیت

شاید در نگاه اول به نظر برسد که سایت شخصی برای راه اندازی وبلاگ بسیار امن تر است، زیرا بسیاری از تنظیمات امنیتی آن در دست خودمان است. به صورت اختصاصی برنامه نویسی آن را خودمان انجام می دهیم. به روز رسانی آن توسط خودمان انجام می شود و هزار و یک دلیل دیگر.

در مقابل ممکن است بگویید که در سرویس های عمومی، وبلاگ شما در کنار هزاران وبلاگ دیگر بر روی سرورهای مشترکی قرار دارد که همین خود مشکل امنیتی بزرگی می تواند برای شما باشد.

اما حقیقت این است که سرویس های وبلاگ نویسی عمومی همچون وردپرس و بلاگر معمولا از سایت های شخصی امن تر هستند. زیرا همانطور که گفتیم مدیریت سرورها و کنترل ترافیک و ارتباطات آنها، به خوبی و توسط بهترین گروه های متخصص انجام می شود. به روز رسانی های امنیتی لازم برای سرور، زبان های برنامه نویسی آن و همچنین برنامه های مدیریت محتوای نصب شده روی آن در سریع ترین زمان ممکن انجام می شود و زودتر از هر سایت شخصی آپدیت ها را دریافت می کند.

ولی در یک هاست شخصی، بخش مهمی از امنیت شما، در گرو کارکرد امنیتی تیم فنی شرکت خدمات دهنده شما است. مانند این که تا چه حد در کنترل ارتباطات و ترافیک خبره بوده و به روزرسانی و آپدیت های مختلف را به موقع نصب کنند .ضمن اینکه ممکن است بسیاری از این مسوولیت ها به عهده خود شما باشد.

بخش دیگری از امنیت یک سایت شخصی، در دستان دیگر همسایه های شما بر روی سرور شرکت خدمات دهنده هاست است. شرکتی که شما از آن فضای مورد نیازتان را خریداری می کنید، معمولا بر روی یک کامپیوتر سرور، هاست های فراوانی در اختیار سایت های مختلف می گذارد. حال کوتاهی مدیران یکی از این سایت ها و نفوذ افراد خرابکار به آن، می تواند به راحتی امنیت شما را هم به خطر بیاندازد.

و مهم ترین بخش هم خود شما هستید (در صورتی که نگهداری از سیستم وبلاگ نویسی تان مانند وردپرس به عهده خودتان باشد). اینکه تا چه حد در رعایت نکات امنیتی مربوط به اطلاعات کاری و شخصی آنلاین تان و اکانت های مختلف تان دقت به خرج می دهید. یا اینکه تا چه میزان مراقب به روزرسانی و آپدیت سیستم عامل و برنامه های آن بر روی کامپیوترتان هستید. و همچنین آیا به روزرسانی های لازم برای برنامه مدیریت محتوا و دیگر بخش های سایت را به صورت مرتب انجام می دهید؟ همه اینها تاثیر فراوانی در امنیت وبلاگ شما خواهند داشت.

درس سوم– ترفندهای امنیتی وردپرس برای سایت های شخصی

در صورتی که انتخاب شما برای وبلاگ نویسی یکی از سرویس های رایگان عمومی باشند، دیگر مسوولیتی بابت امنیت برنامه های مدیریت محتوا و اپلیکیشن های مورد استفاده بر روی سرور نخواهید داشت و امنیت شما در این بخش به عهده شرکت ارایه کننده این خدمات است و فراموش نکنید که همه آنها در این رابطه با کیفیت خوب و دقت لازم عمل نمی کنند. اما اگر برای استقلال و امکانات بیشتر به سراغ خرید هاست و دامنه رفته و سایت شخصی خودتان را راه اندازی کرده باشید، بخش اعظمی از سنگینی بار امنیتی آن، بر دوش خودتان است.

با توجه به اینکه بسیاری از افرادی که سایت های شخصی را برای وبلاگ نویسی راه اندازی می کنند، به سراغ برنامه مدیریت محتوای وردپرس می روند، در این درس قصد داریم به ذکر برخی نکات مهم و ترفندهای امنیتی ضروری در خصوص این CMS بپردازیم.

به طور کلی وردپرس مشهورترین سیستم وبلاگ نویسی است که به خاطر راحتی کار، امنیت خوب و امکانات متنوع کاربران زیادی را به سوی خود جلب کرده است.

توجه :در صورتی که برخی نکات گفته شده در این مطلب برای تان ناآشنا یا گنگ هستند، قبل از اجرای آنها حتما با یک متخصص، طراح سایت یا مدیر سرورتان مشورت کنید. زیرا در صورت استفاده اشتباه از برخی دستورات ممکن است مشکلاتی برای وبلاگ شما پیش آمده و حتی باعث از بین رفتن برخی اطلاعات یا عدم دسترسی شما به وبلاگ تان شود.

الف) نکات و ترفندهای امنیتی

۱ -به روز و آپدیت باشید :سعی کنید همیشه آخرین نسخه به روز رسانی وردپرس را بر روی سایت خود داشته باشید و همیشه اخبار آپدیت های آن را دنبال کنید. زیرا توسعه دهندگان و برنامه نویس های آن در کنار افزودن امکانات جدید، در حال کار بر روی کاستی ها و ضعف های امنیتی وردپرس هستند و در هر مرحله با رفع آنها، آپدیت جدیدی را عرضه می کنند.

این کار تنها چند دقیقه وقت شما را می گیرد، به صورت خودکار انجام می شود و کاملا امن است، زیرا وردپرس قبل از انجام آن، بک آپ کاملی از وبلاگ شما می گیرد. تنها کافی است در داشبورد وردپرس بر روی دکمه Update یا به روز رسانی کلیک کنید. پس هیچ گاه در انجام این کار کوتاهی نکنید.

علاوه بر این، دقت کنید که پلاگین ها و تمپلیت (قالب)های نصب شده بر روی وردپرس هم، همیشه آخرین نسخه به روزرسانی را دریافت کنند. زیرا آنها هم مانند وردپرس دارای نقاط ضعف و باگ هایی هستند که به مرور زمان رفع شده و در آپدیت های جدید عرضه می شوند.

۲ -از رمزهای عبور قوی و مطمئن استفاده کنید :احتمالا شما که کاربر حرفه ای اینترنت هستید، این توصیه را زیاد شنیده اید و مطمئنا رمزهای عبور مطمئن و خوبی را هم به کار می برید. اما این موضوع در امنیت مجازی آنچنان مهم است که تکرار آن هیچ گاه اضافی و بیهوده نخواهد بود .از رمز عبور طولانی، حاوی حروف کوچک و بزرگ، اعداد، علائم و سمبل ها استفاده کنید. تعداد کاراکترهای رمز عبورتان کمتر از ۱۴ حرف نباشند. از رمز عبور تکراری استفاده نکنید. باید رمز عبور ایمیل تان، با رمز عبور لاگین وردپرس و رمز عبور کنترل پنل ادمین هاست تان متفاوت باشند.

۳ -همیشه نسخه پشتیبان مناسب و مطمئنی از وبلاگ تان داشته باشید :بگذارید که روی این نکته تاکید کنیم که حتما بک آپ و پشتیبان هفتگی مناسبی از سایت تان تهیه کنید. زیرا جدا از اینکه تا چه حد سایت و وبلاگ امن و مطمئنی داشته باشید، هیچ گاه نمی توانید پیش بینی کنید که قرار است چه اتفاقی بیُفتد. برخی اوقات، اتفاقات از اختیار و قدرت شما هم خارج هستند و ممکن است به قیمت از دست دادن تمام اطلاعات تان تمام شوند. مثلا اگر سرورهای شرکت خدمات دهنده هاست شما هک شده و به طور کامل پاک شوند، چه کاری از دست تان بر می آید؟ این شرکت ها معمولا پشتیبان فایل ها را در سروری مجزا هم نگهداری می کنند اما واقعیت این است که نمی توان به صورت ۱۰۰ درصد به آنها اطمینان داشت و ممکن است بعد از نابودی اطلاعات با این پاسخ مواجه بشوید که: ببخشید پشتیبان های اطلاعات هم از دست رفته است.

با کمی جستجو در اینترنت می توانید سرویس های آنلاین رایگان و غیر رایگان فراوانی را برای این کار پیدا کنید. همچنین پلاگین های زیادی برای پشتیبان گیری از وردپرس نوشته شده که به خوبی از پس این کار بر می آیند. در درس مربوط به پشتیبان گیری در این خصوص بیشتر صحبت خواهیم کرد.

۴ -از فایل wp-config.php محافظت کنید :این یکی از مهم ترین فایل های درون پوشه وردپرس شما است. زیرا اطلاعات اتصال به پایگاه اطلاعاتی یا دیتابیس سایت/وبلاگ شما، به همراه دیگر اطلاعات امنیتی ضروری وردپرس درون آن ذخیره شده اند. بنابرین باید به خوبی از آن محافظت شود.

راحت ترین کار این است که آن را از پوشه اصلی وردپرس، به پوشه دیگری انتقال دهید. به این شکل تا فردی جای آن را نداند، نمی تواند از این فایل سوء استفاده کند. وردپرس هم از نسخه ۲,۶ به بعد، هوشمند شده و می تواند به صورت خودکار فایل wp-config را جستجو کرده و بیابد. علاوه بر این، شما می توانید با ساخت یک فایل .htaccess و چند خط کد ساده این فایل مهم را از دید عموم مخفی کنید. با این کار دیگر هکرها و ربات های اینترنتی به سادگی نمی توانند این فایل را پیدا کرده و از این طریق به وبلاگ شما حمله کنند.

روی کامپیوترتان، درون یک ادیتور متنی ساده مانند notepad فایل جدیدی باز کرده و کد زیر را درون آن کپی کنید:

```
# protect wpconfig.php
<Files wp-config.php>
order allow, deny
deny from all
</Files>
```

حال فایل را با نام .htaccess ذخیره کرده و آن را درون پوشه ای که فایل wp-config.phpقرار دارد آپلود کنید. اگر از قبل فایلی با نام .htaccess درون آن پوشه وجود دارد، مراقب باشید که جایگزین نشود. بلکه باید آن را دانلود کرده و این کدها را به انتهای آن اضافه کنید. سپس فایل را در جای خود آپلود کنید.

۵ -نام کاربری پیش فرض را تغییر دهید :هنگامی که شما وردپرس را نصب می کنید، اولین اکانتی که به صورت خودکار ایجاد می شود، دارای نام کاربری پیش فرض admin است .استفاده از این نام کاربری و عدم تغییر آن، کار بسیار خطرناکی است زیرا همه ربات های اینترنتی و هکرها از ساخت آن توسط وردپرس آگاه هستند و هنگام حمله به وبلاگ شما، در حقیقت نیمی از راه را رفته اند. زیرا نام کاربری را دارند و تنها باید رمزعبور را پیدا کنند.

در نسخه های وردپرس ۳,۰ و بالاتر شما این امکان را دارید که هنگام نصب وردپرس، نام کاربری پیش فرض (Admin) را به عبارت دلخواه دیگری تغییر دهید .اگر به هر دلیلی وردپرس شما نسخه قدیمی تری است (چیزی که خود خطر بالقوه ای محسوب می شود) یا اینکه وردپرس نسخه ۳,۰ و بالاتر خود را قبلا با نام پیش فرض نصب کرده اید، می توانید از طریق کنترل پنل هاست خود به phpMyAdmin رفته و با اجرای یک Query در بخشSQL ، اقدام به تغییر نام کاربری پیش فرض از Admin به هر نام دیگری کنید. تنها کافی است نام جدید را به جای عبارت your_new_login جایگزین کنید.

```
UPDATE wp_users SET user_login = 'your_new_login' WHERE user_login =
'admin';
```

۶ -پیشوند جداول دیتابیس را تغییر دهید :وردپرس هنگام نصب به صورت پیش فرض از پیشوند wp_ برای جداول دیتابیس استفاده می کند. از آنجایی که این برنامه یک سیستم بازمتن است، اگر شما پیشوند جداول را دست نخورده باقی بگذارید، هر کسی می تواند دقیقا بداند که هر table دیتابیس شما چه نامی دارد و هر بخش اطلاعات وبلاگ تان دقیقا در کجا ذخیره شده اند. حال فقط باید به نوعی بتواند به دیتابیس شما دسترسی پیدا کرده و یا اینکه جداول آن را فراخوانی کند، تا همه اطلاعات را خوانده یا دست کاری کند.

شما می توانید هنگام نصب وردپرس جدید، پیشوند جداول دیتابیس را با وارد کردن پیشوند جدید در فایلwp-cofig.phpتغییر دهید. اگر هم بعد از نصب وردپرس و اتمام کار به فکر چنین تغییری افتاده اید، می توانید از پلاگینی همچون WP Secure Scan استفاده کنید. هرچند خطر چنین کاری در این مرحله کمی بالا است و بهتر است این کار را هنگام راه اندازی اولیه انجام دهید.

البته توجه داشته باشید که پیشوند انتخابی تان هم چندان قابل حدس زدن نباشد. اگر قرار بود وبلاگ درسنامه را با وردپرس راه اندازی کنیم، پیشوندهای dn_ یا dar_ گزینه های مناسبی به نظر نمی رسند.

۷ -کلید های رمز پیش فرض را تغییر دهید : اگر فایل wp-config.php را باز کنید، به راحتی می توانید ۴ خط کد زیر را در آن بیابید که ۴ کلید رمزنگاری پیش فرض وردپرس را در خود جای داده اند:

```
1
define('AUTH_KEY','');
2
define('SECURE_AUTH_KEY','');
3
define('LOGGED_IN_KEY','');
4
define('NONCE_KEY','');
```

و جای شگفتی دارد که بسیاری از افراد در سراسر جهان این کلیدها را بدون تغییر می گذارند و هم اکنون همگی از کلید های رمزنگاری یکسانی در حال استفاده هستند. وردپرس از این کلیدهای رمز هش شده با الگوریتم Salt به همراه رمز عبور شما استفاده می کند، تا آن را قوی و ایمن تر گرداند.

برای تغییر این کلیدها، تنها کافی است به این آدرس مراجعه کرده و ۴ کد رمز جدید ساخته شده را در فایل wp-config.php کپی کنید. به همین راحتی مشکل حل می شود. زیرا این صفحه با هر بار باز شدن ۴ کد رمز هش شده جدید را در اختیار شما می گذارد.

۸ -هر چیز زائد و غیر کاربردی را حذف کنید : هیچ گاه چیزی را به امید اینکه شاید در آینده به کار آید، بر روی سایت خود نگه ندارید. زیرا همین موارد ممکن است در آینده تبدیل به نقاط ضعف و محل نفوذ به وبلاگ شما شوند. نام های کاربری اضافی و بدون استفاده را حذف کنید .تمپلیت هایی را که لازم ندارید و کاربرد ندارند را پاک کنید. پلاگین های به درد نخور را غیر فعال کرده و حذف نمایید. در یک کلام، همانطور که خرت و پرت های اضافی گوشه حیاط یا انباری می توانند لانه موش ها و موریانه ها شوند، فایل ها و اپلیکیشن ها و دسترسی های بی مورد وبلاگ هم می توانند تبدیل به تله و لنگرگاهی برای نفوذگران و هکرها گردند.

ب) پلاگین های امنیتی

۱ :WP Security Scan -این پلاگین قابلیت های امنیتی فراوانی دارد که از امکانات اولیه آن می توان به حذف ورژن وردپرس از صفحات آن اشاره کرد. وقتی هکر نسخه دقیق وردپرس شما را بداند، بهتر می تواند ایرادات امنیتی آن را پیدا

کرده و برای شیوه حمله تصمیم گیری کند. همان طور که قبلا هم گفتیم، از دیگر امکانات این پلاگین تغییر پیشوند جداول دیتابیس وردپرس است.

علاوه بر این، این پلاگین به صورت دوره ای وردپرس شما را کنترل کرده و نقاط ضعف امنیتی آن را یافته و پیشنهادات لازم برای رفع آنها را ارائه می کند.

۲ :BulletProof Security -این پلاگین از وبلاگ شما در مقابل حملات مختلف امنیتی همچون XSS و RFI و CRLFو Base64، تزریق کد و تزریق SQL مراقبت می کند. علاوه بر این امکان حفاظت از فایل های مهم وردپرس از جمله wp-config.php و php.ini و install.php و .htaccessرا هم دارد. این پلاگین می تواند نمایش پیغام های خطای دیتابیس، اخطارهای سیستم و اعلان های سطح دسترسی پوشه و فایل ها را هم خاموش کند.

۳ :Better WP Security -این پلاگین یک دستیار امنیتی همه کاره برای شما است که همه چیز را یکجا برایتان جمع کرده است. در عرض چند دقیقه کل سایت را اسکن کرده و نقاط ضعف را پیدا و مشکل را حل می کند. متا تگ های ساخته شده توسط وردپرس را یافته و حذف می کند. پیغام های خطای لاگین را خاموش می کند. آدرس صفحات مهمی همچون لاگین و ادمین را به راحتی تغییر داده و نام دلخواه شما را جایگزین می کند. با این کار یک مانع مستحکم اضافی در برابر فرد خرابکار می کشید. برای زمان های مشخصی که نیازی به دسترسی به سایت را ندارید، امکان لاگین کردن را به طور کامل غیر فعال می کند.

و البته تمام اینها بخشی از امکانات این دستیار همه فن حریف پرکار شما هستند که به تنهایی از پس بسیاری خطرات امنیتی بر می آید .

حتما شما با ترفندها و پلاگین های بسیار بیشتری در زمینه امنیت وردپرس آشنایی دارید که در این درس به آنها اشاره ای نشد. شاید این مجال کوتاه جایی برای ذکر تمام نکات لازم در خصوص امنیت وردپرس نباشد و تنها مجبور باشیم به مهمترین نکات اشاره کنیم. البته هنگام استفاده از پلاگین ها این نکته را به یاد داشته باشید که حداقل پلاگین ممکن را نصب کنید و هیچ گاه پلاگینی را که استفاده از آن ضرورت ندارد را بر روی وبلاگ خود نگه ندارید. زیرا هر پلاگین امنیتی امروز، ممکن است فردا تبدیل به یک باگ بزرگ و نقطه ضعفی برای نفوذ گردد. ضمنا به روزرسانی مرتب پلاگین ها به همراه خود وردپرس را هم از یاد نبرید.

درس چهارم– نکات امنیتی ضروری برای وبلاگ نویسان

حفظ امنیت و حریم خصوصی در فضای اینترنت برای یک وبلاگ نویس از اهمیت ویژه ای برخوردار است. زیرا در صورت ایجاد مشکلات امنیتی، نه تنها اطلاعات شخصی وی به خطر افتاده، بلکه مهم تر از آن وجه عمومی و جایگاه وی به عنوان یک وبلاگ نویس در اجتماع و گروه خوانندگانش هم در معرض تعدی و تخریب قرار خواهد گرفت.

تا زمانی که مرکز توجه قرار نگرفته باشید، خطرات کمتری شما را تهدید می کنند، ولی به محض اینکه تعداد بازدیدکننده های وبلاگ شما زیاد شود، به همین نسبت احتمال حمله به شما نیز بیشتر می شود. به خصوص اگر یک وبلاگ با نگاه انتقادی داشته باشید یا مطالب شما با منافع اقتصادی و تجاری گروهی در تضاد باشد، آنگاه باید بسیار مراقب زندگی آنلاین خود باشید.

در این شرایط هک شدن شما فقط نابودی وبلاگ تان را به دنبال ندارد، بلکه امنیت خود شما و حتی بازدیدکنندگان و کاربران شما را نیز از بین می رود. تعدادی از نکات مهم امنیتی که در درس امنیت وردپرس به آن پرداختیم، در همه جا و همه سرویس های وبلاگ شخصی و عمومی کاربرد دارند و پیشنهاد می کنیم آنها را دوباره مطالعه کنید. در این درس هم به برخی نکات مهم دیگر اشاره می کنیم و یا نکات قبلی را کامل تر شرح می دهیم.

انتخاب رمز عبور مناسب و ایمن

شکی نیست که اولین و شاید مهمترین قدم در حفظ امنیت، انتخاب رمزهای عبور مناسب است. چیزی که در درس قبلی هم روی آن تاکید کردیم. برای انتخاب رمز عبور به چند نکته کلیدی باید توجه کنید:

۱ -روی رمزهای عبورتان حساس باشید و هرگز برخی از آنها را کم اهمیت تر از بقیه تلقی نکنید. زیرا ممکن است همان اکانت ساده و بی اهمیت شما، راه ورود هکرها به دنیای خصوصی اطلاعات مهم تان باشد.

۲ -از رمزهای عبور طولانی و حاوی حروف بزرگ، کوچک، اعداد و نشانه ها استفاده کنید.

۳ -احتمالا می گویید چنین رمز عبوری را که نمی توان به خاطر سپرد! خب، می توان از نرم افزارهای مناسب برای نگهداری آنها مانند Last Passو KeePassاستفاده کرد.

۴ -هرگز از روش های خطرناکی مانند یادداشت رمز عبور درون دفترچه یادداشت یا فایل متنی بر روی کامپیوتر استفاده نکنید.

۵ -از عباراتی که در هنگام سخن گفتن بر آنها تکیه می کنید به عنوان رمز عبور استفاده نکنید. زیرا از اولین گزینه های یک هکر در زمان حدس زدن رمز عبور شما، چنین کلماتی هستند.

۶ -در آخر از اطلاعات تماس خود و نزدیکان تان و یا اطلاعات شناسنامه ای و هویتی تان هرگز به عنوان رمز عبور استفاده نکنید.

با رعایت همین نکات ساده و کمی تدبیر در انتخاب رمز عبور تا حد زیادی به امنیت خودتان کمک کرده اید

حفظ امنیت در زمان ورود محتوا

به روز رسانی مداوم وبلاگ و آمادگی برای عرضه مداوم و منظم خوراک برای بازدیدکننده، شرط لازم زنده بودن یک وبلاگ است. خواننده های ثابت یک وبلاگ مرتبا از شما مطالب جدید می خواهند و این انتظار را دارند که طبق زمان بندی مشخص، محتوای جدیدی در دسترس داشته باشند. بنابراین ورود محتوا یکی از کارهایی است که شما به عنوان یک وبلاگ نویس به دفعات و در شرایط مختلف زمانی و مکانی انجام می دهید و این می تواند یکی از نقاط مهم آسیب پذیری شما در برابر حملات باشد. لذا باید همیشه در این خصوص مراقب بوده و نکات امنیتی لازم را رعایت کنید.

انتخاب مرورگر

اینکه برای وبگردی از چه مرورگری استفاده می کنید، بر روی امنیت شما تاثیر مستقیم دارد. حتما از یک مرورگر امن مانند فایرفاکس یا کروم استفاده کنید. اگر از فایرفاکس یا کروم استفاده می کنید، افزونه Noscriptرا بر روی آنها نصب کنید. با این کار از فعالیت کدهای مخرب در قالب Javascriptکه به صورت خودکار امکان اجرا بر روی کامپیوتر شما را دارند، جلوگیری می کنید.

یکی دیگر از راه های حفظ امنیت خود و وبلاگ تان، این است که مراقب مخفی ماندن و فاش نشدن آی پی تان باشید. زیرا از طریق شناسایی آی پی، هکر می تواند به راحتی محل کار و زندگی، یا حداقل ISP خدمات دهنده اینترنت شما را یافته و با نفوذ به آن، اطلاعات شما را پیدا کند. در این صورت به راحتی می تواند از طریق نفوذ فیزیکی به محل کار یا منزل تان و طی یک سرقت به ظاهر ساده، بسیاری از اطلاعات هویت آنلاین شما را تصاحب کند. زیرا تنها کافی است به کامپیوتر یا لپ تاپ شما دست پیدا کند تا شانس وی در دستیابی به رمزهای عبورتان چندین برابر گردد.

ایمیل اختصاصی وبلاگ

از ایمیلی که برای ساختن وبلاگ استفاده کرده اید، به هیچ وجه جهت ارتباط با دیگران استفاده نکنید. بهتر است به جای کار با ایمیل اصلی خود جهت ساخت اکانت وبلاگ و دیگر ارتباطات ویژه این چنینی، ایمیل جداگانه و اختصاصی در جیمیل ساخته و تنها برای همین کار از آن استفاده کنید.

زیرا در صورتی که با هک شدن ایمیل دوستان و همکاران تان، ایمیل شما به خطر افتاد و مورد حمله قرار گرفت، حداقل وبلاگ شما مورد تهدید واقع نمی شود. به خاطر داشته باشد که هیچ گاه ایمیل هایی را که از طرف افراد ناشناس ارسال می شود باز نکنید و در استفاده از محتوا و لینک های مشکوک ایمیل های افراد آشنا هم با احتیاط کامل رفتار کنید. (در دوره استاد بزرگی ایمیل و جیمیل درسنامه به طور مفصل در این مورد صحبت کرده ایم).

به روز رسانی از طریق ایمیل

در برخی از سرویس های وبلاگ نویسی امکان به روز رسانی وبلاگ و انتشار محتوا از طریق ایمیل را دارید. به این صورت که آنها یک اکانت ایمیل به شما می دهند که هر ایمیلی که به آن آدرس ارسال کنید، به عنوان یک پست در وبلاگ تان منتشر می شود. استفاده از این امکان بسیار منطقی است و بدین صورت دیگر مجبور به لاگین در پنل مدیریت و وارد کردن رمز عبور برای انتشار یک مطلب جدید نیستید. البته فراموش نکنید که این آدرس ایمیل باید نزد خودتان مخفی بماند و نگهداری آن همانند رمز عبور مهم و حیاتی است.

امنیت در سفر

همان طور که گفتیم، یک وبلاگ موفق به صورت منظم آپدیت می شود و حتی یک سفر کاری یا تفریحی هم نباید خللی در این روال منظم به وجود آورد. اما با توجه به شرایط ویژه دسترسی به اینترنت هنگام سفر، رعایت نکات امنیتی هم دقت ویژه و خاصی را می طلبد.

-اگر از سرویس های وبلاگ نویسی عمومی استفاده می کنید، حتما امکان ارسال مطلب از طریق ایمیل را فعال کنید. حال به صورت امن و از طریق یک اینترنت مطمئن، به ایمیل خود وصل شوید و از آن راه وبلاگ تان را به روز کنید.

-تا جایی که امکان دارد، از شبکه های وایرلس عمومی و ناآشنا استفاده نکنید .هنگام اتصال به شبکه های عمومی، با استفاده از اکانت VPN امن به اینترنت متصل شوید و به روز رسانی را انجام دهید.

-سعی کنید که حتما لپ تاپ شخصی خود را به همراه داشته و از آن برای اتصال به اینترنت و ارسال محتوا استفاده کنید. زیرا کامپیوترهای عمومی در کتابخانه، هتل یا کافی نت ها به احتمال زیاد به نرم افزارهایی آلوده هستند که رمزهای عبور شما را ثبت و برای فرد نصب کننده برنامه ارسال می کنند.

-در صورتی که مجبور به استفاده از سیستم های عمومی هستید، در ابتدا توسط یک آنتی ویروس پرتابل سیستم را Scanکنید و سپس از طریق FireFox پرتابل به اینترنت متصل شوید. به همراه داشتن یک کول دیسک اورژانسی با برنامه های پرتابل مورد نیاز، همیشه می تواند راه گشا باشد.

-و نکته آخر اینکه همیشه یک سی دی لینوکس به همراه داشته باشید و در صورت امکان کامپیوترهای عمومی را از طریق سی دی لایو لینوکس بوت کنید. با این کار دیگر از سلامت سیستم عامل و عدم آلودگی آن به بدافزار مطمئن خواهید بود.

امنیت کامپیوتر شخصی

کامپیوتر شخصی تان می تواند یکی از مهمترین نقاط ضعف امنیتی شما باشد، زیرا در صورت رعایت همه نکات و در نهایت آلوده بودن کامپیوترتان به ویروس، تروجان یا کی لاگر، در واقع همه زحمات شما به هدر می رود. فراموش نکنید که سیستم عامل تان را همیشه به روز نگه دارید و آخرین آپدیت های امنیتی را بر روی آن نصب کنید.

از نصب نرم افزارهای متفرقه و اجرای فایل هایی که نمی شناسید خودداری کنید .اگر از ویندوز استفاده می کنید یک آنتی ویروس مناسب روی آن نصب کنید. آنتی ویروس های رایگان مناسب و با کارایی خوبی همانند Avira یا Avast می توانند کمک فراوانی به امنیت کامپیوتر شما کنند.

در کنار آنتی ویروس ها، نرم افزارهای ضد جاسوس افزار هم می توانند مفید واقع شوند .Adaware و Spybotدو گزینه رایگان و کارآمد این نوع برنامه ها هستند. همچنین فراموش نکنید که حتما Firewall و دیگر امکانات امنیتی سیستم عامل خود را هم فعال کنید.

علاوه بر تاکید در به روز رسانی و آپدیت سیستم عامل و نرم افزارهای امنیتی آن، مراقب دیگر برنامه های نصب شده روی کامپیوتر باشید و همیشه آنها را به روز نگهدارید. زیرا یک برنامه عادی ویرایش عکس، پخش موسیقی یا نمایش فایل PDFهم می تواند به راحتی تبدیل به خطری مهلک و روزنه ورودی برای هکرها شود .

آپدیت برنامه مدیریت محتوای وبلاگ

علاوه بر سیستم عامل و نرم افزارهای آن که باید همیشه به روز باشند و آپدیت های امنیتی آنها نصب شده باشند، در خصوص امنیت برنامه های مدیریت محتوای سایت و وبلاگ تان هم باید مراقب و سخت گیر باشید.

در صورتی که از سرویس های عمومی همچون بلاگر یا وردپرس استفاده می کنید، کار چندانی از شما بر نمی آید و همه چیز بستگی به مدیران سرور این سرویس ها دارد. اما خیال تان راحت باشد که ارائه دهندگان چنین سرویس هایی، خود بیش از هر کسی نگران امنیت هستند و مرتبا برنامه های خود را به روز می کنند.

در صورتی که از هاست و فضای شخصی برای وبلاگ نویسی استفاده می کنید، همیشه مراقب و گوش به زنگ ارائه آپدیت های سیستم مدیریت محتوای وبلاگ تان باشید .همچنین اخبار مربوط به آن را دنبال کنید تا از مشکلات و خطرات احتمالی با خبر بوده و آماده مقابله با آنها شوید.

و نکته ای که دوباره لازم به ذکر است، اینکه شما هر میزان هم مراقب باشید، باز به پای توانایی سرویس دهندگان وبلاگ نویسی عمومی چون بلاگر و وردپرس نمی رسید. پس در صورتی که امنیت برای شما اهمیت زیادی دارد، امن ترین انتخاب می تواند استفاده از یک سرویس وبلاگ نویسی رایگان به جای سایت شخصی باشد.

تهیه و نگهداری نسخه پشتیبان از اطلاعات وبلاگ

اگر از سیستم های وبلاگ نویسی عمومی استفاده نمی کنید، لازم است که به صورت دوره ای از اطلاعات خود بک آپ تهیه کنید تا در صورت بروز مشکل، محتوای خود را از دست ندهید. این پشتیبان گیری می تواند روزانه، هفتگی یا ماهیانه باشد، که انتخاب بازه زمانی بستگی به میزان ورود محتوای شما و اهمیت مطالب وبلاگ دارد. از دیگر سو، امنیت این نسخه های پشتیبان هم مهم است، زیرا علاوه بر محتوای وبلاگ شما، اطلاعات بازدیدکنندگان شما شامل IP و نظراتشان نیز در این نسخه پشتیبان جای دارد.

نسخه های بک آپ را در محل های امنی نگهداری کنید و توسط نرم افزارهای مخصوص، رمزنگاری کنید. یکی از نرم افزارهای مناسب برای این کار، TrueCryptاست که همانند قفل یک گاو صندوق از اطلاعات شما محافظت می کند.

از نگهداری فایل های تاریخ گذشته و بی ارزش خودداری کنید و فقط نسخه های مورد نیاز را حفظ کنید. با این کار علاوه بر صرفه جویی در فضای لازم برای نگهداری نسخه های پشتیبان، مدیریت آنها هم برای تان راحت تر می گردد.

البته حتی در صورت استفاده از سیستم های وبلاگ نویسی عمومی، باز هم نیاز به پشتیبان گیری از اطلاعات خود دارید. درست است که این سرویس ها نسخه های پشتیبان دائمی دارند و از امنیت بالایی هم بهره می برند، اما تصور کنید که فردی وبلاگ شما را هک کند و تمام مطالب تان را پاک کند.

این سرویس ها گزینه هایی برای خروجی گرفتن از وبلاگ به عنوان Export یا Backup دارند که می تواند نسخه کاملی از وبلاگ شما تا حال حاضر را در اختیارتان بگذارد. بسته به سرویس مورد استفاده، این نسخه را می توان دوباره روی خود وبلاگ بازیابی کرد و یا حتی در صورت مهاجرت به سرویس وبلاگ نویسی دیگر یا سایت شخصی، از آن برای انتقال محتوای وبلاگ قدیم به محل جدید بهره برد.

درس پنجم– بررسی قالب وبلاگ از دیدگاه امنیت

یکی از بخش های وبلاگ که تنوع بسیار زیادی در آن دیده می شود و طرفداران فراوانی هم دارد، قالب یا تم (Template or Theme) آن است که در حقیقت نمای ظاهری سایت و وبلاگ را می سازد.

بسیاری از صاحبان سایت ها و وبلاگ ها در اولین قدم، به دنبال ظاهری زیبا، موجه و مورد پسند ذائقه خود و مخاطب شان هستند و گاها از قالب های آماده استفاده کرده یا اینکه به طراحی و سفارش قالب اختصاصی می پردازند.

در نگاه اول شاید قالب فقط تشکیل شده از چند خط کد و تعدادی عکس باشد که از نقطه نظر امنیتی اهمیت چندانی ندارد. اما در واقع، می تواند تبدیل به یکی از بزرگترین نقاط ضعف امنیتی وبلاگ گردد. زیرا برای نمایش وبلاگ، لازم است تمامی کدهای درون تمپلیت اجرا شده و مرتبا با دیتابیس در ارتباط باشند. لذا به راحتی می توان با قرار دادن برخی کدهای مخرب درون قالب و عرضه رایگان آن، سایت ها و وبلاگ های فراوانی را آلوده کرد.

در بحث انتخاب قالب، صاحبان وبلاگ و وب سایت معمولا دو رویه را دنبال می کنند. گروهی با پرداخت هزینه به طراحی قالب و تمپلیت اختصاصی روی می آورند و گروه دیگری هم از تمپلیت های آماده رایگان و غیر رایگان استفاده می کنند . در این میان هر دو گروه در معرض خطرات امنیتی مرتبط با قالب قرار دارند، اما میزان ریسک و آسیب پذیری گروه اول بسیار کمتر است. زیرا احتمال اینکه فردی با دریافت هزینه، تمپلیت اختصاصی برای شما طراحی کند که حاوی کدهای مخرب باشد، بسیار کمتر از این است که افرادی تمپلیت های آماده رایگانی حاوی کد مخرب در اختیارتان بگذارند.

پس بهتر است که تا حد امکان از قالب های اختصاصی استفاده کرده و آنها را به شرکت یا افراد معتبر و مطمئن سفارش دهیم. اما باز هم نباید ۱۰۰ درصد به این قالب اعتماد کنیم و لازم است کدهای آن را قبل از استفاده کنترل کنیم. در مورد قالب های رایگان هم که کاملا ضروری است قبل از هر کاری تمامی کدها و فایل های آن را کنترل کرده و مراقب دستورات مخرب باشیم.

توجه داشته باشید که آسیب پذیری قالب، تنها از کدهای اولیه قالب نیست و می تواند در اثر اضافه کردن برخی بخش ها به آن، ایجاد شود. مانند کدهای HTML یا جاوا اسکریپتی که برای باکس چت، شمارنده یا دیگر افزونه ها به قالب افزوده می شوند.

مثلا یک شمارنده بازدیدکنندگان شاید بخش مفیدی برای پیگیری میزان استقبال از وبلاگ شما باشد، اما به طور همزمان ممکن است مشغول جمع آوری اطلاعات در خصوص عادات آنلاین کاربران شما برای شرکت های تبلیغاتی باشد.

همچنین یک قالب رایگان می تواند حاوی کدهایی برای تبلیغات Pop-up بوده یا لینک هایی به سایت های خطرناک در پوشش نام های اعتماد برانگیز درون خود داشته باشد. یا اینکه حتی قالبی که به صورت فایل زیپ دانلود می شود، می

تواند هیچ خطری برای وبلاگ شما نداشته و حاوی کد مخربی برای آن نباشد، اما بدافزار یا تروجان خاصی را بر روی کامپیوتر شما نصب کند.

برای مقابله با چنین خطراتی چه باید کرد؟

۱ -قبل از استفاده از تمپلیت یا افزونه ها، کمی وقت برای بررسی کدهای آن بگذارید و به دنبال هر چیز ناشناخته یا مشکوکی باشید که در جای خود قرار ندارد. برای مثال اگر می خواهید یک ویجت آب و هوا در ستون کناری وبلاگ تان بگذارید، اما در کد این ویجت لینکی به یک سایت نامرتبط قرار دارد، این موضوع را به عنوان آژیر خطر در نظر گرفته و به دنبال ویجت دیگری باشید. به هیچ وجه دلیلی ندارد که یک ویجت آب و هوا درون خود دارای لینکی همانند زیر باشد:

```
<a href="http://completelyfreemoney.com">Make Money Online!</a>
```

بسیاری از کدهای مخرب یا تبلیغاتی درون یک تمپلیت به صورت رمزنگاری شده نگهداری می شوند تا به راحتی قابل شناسایی نباشند. همیشه به دنبال سرنخ هایی همچون عبارات رمزنگاری شده و دستوراتی مانند base64 باشید.

۲ -قبل از ذخیره کدهای تمپلیت جدید، ابتدا پیش نمایش آن را مشاهده کنید .طراحان تمپلیت های مخرب اغلب ممکن است از پنجره های تبلیغاتی خودکار و یا انواع دیگری از تبلیغات درون کدهای خود استفاده کرده باشند که با دیدن پیش نمایش، می توانید به راحتی آنها را یافته و از خیر استفاده از چنین قالبی بگذرید.

۳ -قبل از هرگونه تغییر در کدهای تمپلیت وبلاگ و یا اضافه کردن ویجت و افزونه خاصی به آن، ابتدا از تمپلیت سالم فعلی، نسخه پشتیبانی تهیه کنید. با این کار، در صورت بروز هرگونه مشکل و یا مشاهده کد مخرب، بازگشت به حالت امن سابق، به سادگی امکان پذیر خواهد بود.

۴ -پلاگین و تمپلیت مورد نیازتان را همیشه از سایت های معتبر و قابل اطمینان دانلود کنید. هیچ گاه به نتایج جستجوی موتورهای جستجو برای انتخاب تم اعتماد نکنید و تا از سایتی مطمئن نشده اید، از محتوای آن استفاده نکنید .البته بهترین حالت سفارش قالب اختصاصی به طراح و برنامه نویس شناخته شده و مورد اطمینان تان است.

برای مثال در این مقاله می توانید بررسی نتایج جستجوی صفحه اول گوگل برای عبارت Free Wordpress Themesو میزان آلودگی آنها را ببینید.

۵ -از پلاگین های امنیتی ویژه کنترل قالب استفاده کنید. برای مثال در وردپرس پلاگین Theme Authenticity Checker، قالب یا تمپلیت مورد نظر را پس از آپلود بر روی سرور (و قبل از استفاده به عنوان تم اصلی سایت)، کنترل کرده و به دنبال موارد مشکوک و لینک های مشکل دار درون آن می گردد و در صورت مشاهده، آنها را با محل قرارگیری شان در کد تمپلیت برای تان مشخص می کند.

همچنین پلاگین Exploit Scanner تمامی فایل ها و دیتابیس وبلاگ را برای یافتن نشانه هایی از کدهای مخرب و برنامه های نفوذگر و بدافزار، اسکن کرده و موارد مشکوک را به شما گزارش می دهد.

۶ -قالب های نصب شده روی وبلاگ را مرتبا کنترل کرده و آپدیت های عرضه شده برای آنها را به موقع نصب کنید. همچنین قالب های غیر ضروری که نیازی به آنها ندارید را حتما غیر فعال کرده و در صورت امکان، آنها را از روی هاست وبلاگ خود پاک کنید.

۷ -هنگام دانلود قالب دلخواه، مراقب باشید که آدرس سایت ارائه کننده قالب با محل دانلود فایل فشرده تمپلیت یکسان باشد. برای این کار تنها کافی است قبل از دانلود نگاهی به لینک دانلود بیاندازید و آدرس سایت آن را با سایت عرضه کننده قالب تطبیق دهید. زیرا برخی اوقات سایت های مخرب، تمپلیت های مشهور و زیبا را دستکاری کرده و روی سرورهای خود قرار می دهند. آنگاه از یک سایت معتبر عرضه تمپلیت به عنوان طعمه برای به دام انداختن شما استفاده می کنند.

۸ -مراقب پیام ها و موافقت نامه های عرضه شده هنگام دانلود تمپلیت های رایگان و غیر رایگان باشید. زیرا گاهی طی یک جمله گنگ، شما موافقت می کنید که سازنده تمپلیت این حق را دارد که هرگونه لینکی را به هر شکلی درون تم شما به نمایش بگذارد! همین موضوع می تواند دلیلی برای شک کردن به آن قالب باشد.

۹ -همیشه از قالب هایی که مرتبا آپدیت می شوند استفاده کنید. زیرا در این گونه موارد معمولا طراح آن تم، آنقدر نگران محصول خود است که دائما آن را کنترل کرده و با رفع نقاط ضعف امنیتی و کارکردی، آن را بهبود می بخشد.

اگر بخواهیم این درس را به صورت خلاصه بیان کنیم، باید بگوییم که برای امنیت وبلاگ تان از نظر قالب یا همان پوسته، بهتر است که از سایت اصلی عرضه کننده سرویس قالب ها، قالب مورد نظر خود را انتخاب کنید (مانند وردپرس فارسی) و علاوه بر آن کارآیی و امنیت وبلاگ تان را بر کارهایی مانند اضافه کردن ساعت، وضعیت آب و هوا و... ارجح بدانید زیرا با اضافه کردن هر یک از این ابزارها نه تنها امنیت وبلاگ خود را به خطر می اندازید، بلکه وبلاگ تان را به عنوان یک وبلاگ غیرحرفه ای و آماتور به بازدیدکنندگان معرفی می کنید!

درس ششم– همه چیز درباره ایمیل در وبلاگ نویسی

در صورتی که نگاهی به وبلاگ ها و سایت های هک شده یا مورد حمله قرار گرفته بیاندازیم، می بینیم که یکی از نقاط ضعف بسیار مهم، ایمیل وبلاگ و نویسنده آن است. زیرا در بسیاری مواقع از طریق ایمیل، فرد نفوذگر می تواند دست به حملاتی همچون فیشینگ و مهندسی اجتماعی بزند و یا بدتر از آن، با کمی سعی و خطا، کنترل کامل ایمیل را به دست گرفته و از طریق اطلاعات درون آن، وارد بخش مدیریتی وبلاگ یا سایت شود.

در این درس به برخی نکات امنیتی مهم در خصوص ایمیل می پردازیم که تا حد زیادی باعث کاهش این خطرات و امنیت بیشتر وبلاگ شما می گردند.

استفاده از ایمیل اختصاصی برای ثبت و مدیریت سطح بالای وبلاگ و سایت

یک ایمیل هر چه شلوغ تر باشد و تعداد پیام های دریافتی آن بیشتر باشد و با افراد بیشتری سر و کار داشته باشد، کنترل و مدیریت آن به همان اندازه مشکل تر شده و بیشتر در معرض خطر قرار دارد. علاوه بر این، چنین ایمیل پرکاری بدون شک بیشتر توجه نفوذگران و مهاجمین آنلاین را به خود جلب کرده و زودتر توسط بات های اینترنتی و اسپمرها کشف می شود.

علاوه بر این وقتی که تعداد دوستان و همکارانی که با ایمیل شما در ارتباط هستند زیاد باشد، به همان نسبت احتمال فریب شما از طریق اکانت هک شده آنها بیشتر می شود. اما اگر دوستان تان آدرس ایمیلی را نداشته باشند یا زیاد با آن در تماس نباشند، هرگونه ایمیل از طرف آنها با درخواست های غیرمعقول یا صمیمانه، زودتر شک شما را بر می انگیزد و شما را حساس تر می کند.

پس بهترین راه برای امنیت بیشتر وبلاگ، استفاده از یک ایمیل اختصاصی جهت ثبت و انجام کارهای مدیریتی آن است. با توجه به سرویس های رایگان و امن ایمیل، می توانید به سادگی برای مدیریت وبلاگ تان یک ایمیل جداگانه ایجاد کنید که تنها شما و شرکت خدمات دهنده هاست و دامنه از آن مطلع بوده و با این آدرس با شما در تماس است.

با این کار شما خطر حملات مهندسی اجتماعی را تا حد فراوانی کاهش داده اید .زیرا دیگر فرد مورد اطمینانی مانند دوست، همکار یا از اعضا خانواده، آدرس این ایمیل را نداشته و با آن در تماس نیستند. در نتیجه حتی در صورت هک شدن اکانت آنها، ایمیل های فریب دهنده و فیشینگ برای تان ارسال نمی شود.

همچنین شما با استفاده از ایمیل اصلی تان معمولا در بسیاری از سایت ها و شبکه های اجتماعی عضو هستید که در صورت عدم رعایت نکات امنیتی در این سایت ها و شبکه های اجتماعی، احتمال نفوذ به آنها و حتی استفاده از اطلاعات

شخصی درون آنها برای هک کردن ایمیل تان وجود دارد. اما در صورتی که ایمیل مدیریت وبلاگ شما به هیچ سایت یا شبکه اجتماعی متصل نباشد، حداقل این امتیاز از فرد مهاجم گرفته می شود.

به خاطر داشته باشید که از این آدرس ایمیل اختصاصی وبلاگ در هیچ جای دیگری استفاده نکنید و آن را به اکانت اصلی ایمیل تان هم متصل نکنید. زیرا در صورت به خطر افتادن یکی از این ایمیل ها، دیگری هم به خطر می افتد.

برای ساخت این ایمیل حتی لازم نیست که از نام زیبا، مرتبط، به خاطر ماندنی یا ساده استفاده کنید. زیرا هر چه نام بی ربط تر باشد، احتمال اینکه توسط افراد مهاجم حدس زده شده یا ارتباط آن با شما و دیگر اکانت های آنلاین تان کشف شود، کمتر است.

نکته مهم :این ایمیل فقط برای ثبت وبلاگ/سایت و تماس با شرکت خدمات دهنده هاست و دامنه، یا سرویس های رایگان وبلاگ نویسی خواهد بود. به هیچ وجه از آن به عنوان ایمیل بخش «تماس با ما»، ساخت اکانت در شبکه های اجتماعی برای وبلاگ، یا مانند این استفاده نکنید. برای چنین کارهایی می توانید از همان ایمیل معمول خود استفاده کرده و یا یک ایمیل دیگر با نامی شبیه به وبلاگ برای کارهای عمومی بسازید.

استفاده از سرویس جیمیل به جای دیگر ایمیل های رایگان و غیر رایگان

نکته مهم بعدی، انتخاب یک سرویس دهنده مناسب، کارا و ایمن برای ساخت ایمیل اختصاصی مدیریت وبلاگ است. اگر در دوره» استاد بزرگی ایمیل و جیمیل «درسنامه شرکت کرده باشید، حتما انتخاب شما جیمیل خواهد بود و آن را به دیگر سرویس دهندگان ترجیح می دهید.

مهمترین توصیه ما در این مرحله، عدم استفاده از سرویس ایمیل خصوصی هاست شخصی تان است. زیرا در صورتی که برای سایت شما اتفاقی افتاده یا هاست آن توسط فرد دیگری تصرف گردد، به سادگی می توان رمز عبور آن را عوض کرده و تنها نقطه ارتباطی امن شما با شرکت پشتیبان هاست و دامنه قطع می شود. علاوه بر این، سرویس های هاست شخصی معمولا چندان از نظر امنیت و در دسترس بودن دائم، قابل اطمینان نیستند.

اما از میان سرویس دهندگان رایگان و قدرتمندی همچون یاهو، هات میل، جیمیل و ...کدام یک را باید انتخاب کنیم؟ پیشنهاد قطعی ما جیمیل است. زیرا همانگونه که قبلا گفتیم: «چون محیط کاربری آسان و خوش دستی دارد. چون رایگان و دارای امکانات بسیار زیاد است. چون می تواند دیگر سرویس های ایمیل شما را به راحتی مدیریت کند. چون قابلیت لیبل زنی، فیلتر و جستجوی بی رقیبی دارد.» و در نهایت اینکه چون یکی از امن ترین سرویس های ایمیل است.

جیمیل یکی از معدود سرویس دهندگان ایمیل است که در تمامی مراحل کار از ارتباط امن https استفاده می کند. یعنی اینکه چه در مرحله لاگین و چه مرحله خواندن و ارسال ایمیل ها، ارتباط شما با سرور گوگل به صورت رمزگذاری شده SSL است.

از دیگر نقاط مثبت این سرویس ایمیل می توان به فضای ذخیره تقریبا بی پایان، رایگان بودن، دریافت اسپم کمتر و امکان انواع جستجو در تمامی بخش ها اشاره کرد. جیمیل فضای رایگان بزرگی در اختیار شما می گذارد که به صورت لحظه ای در حال افزایش است. همچنین از تکنولوژی اختراعی ویژه گوگل برای کنترل و بلوکه کردن ایمیل های اسپم بهره می برد.

نکاتی در خصوص امنیت ایمیل

حال که ایمیل اختصاصی وبلاگ تان را در جیمیل ساخته اید و از آن برای ثبت و راه اندازی وبلاگ/سایت خود استفاده نموده اید، بهتر است کمی بیشتر مراقب امنیت این اکانت ایمیل باشید.

۱ -همانند خود وبلاگ، به هیچ وجه از اینترنت عمومی و ناشناخته برای کنترل حساب ایمیل تان استفاده نکنید. حال این امر هر میزان هم که مهم باشد، به پای اهمیت وجودی وبلاگ شما نمی رسد.

۲ -علاوه بر اینکه از ایمیل اختصاصی سایت برای کارهای عادی خود استفاده نمی کنید، از این ایمیل برای ارسال مطلب به وبلاگ جهت انتشار هم استفاده نکنید .زیرا برای این کار ممکن است در برخی مواقع مجبور به استفاده از اینترنت ناامن برای ورود به ایمیل شوید. یا اینکه استفاده مداوم از ایمیل، توجه بات نت ها و اسپمرها را به آدرس ایمیل شما جلب کند.

۳ -از رمز عبور امن و قابل اعتمادی با حداقل ۱۵ کاراکتر، برای این اکانت ویژه استفاده کنید. با توجه به اینکه نیازی به استفاده دائم از این اکانت ندارید، لازم نیست که رمز عبور آن قابل حفظ کردن باشد. برنامه های مدیریت رمز عبور می توانند به راحتی و با امنیت بالا از این رمز طولانی و مشکل، حفاظت کنند.

در رمز عبور انتخابی از حروف کوچک و بزرگ، اعداد و علائم استفاده کنید. در صورت امکان از ابزار تولید رمز عبور تصادفی برای این کار استفاده کنید .بسیاری از برنامه های مدیریت رمز عبور، درون خود چنین ابزاری را دارند.

۴ -هر چه کامپیوتر امن تری داشته باشید، ایمیل شما کمتر در خطر خواهد بود .سعی کنید تنها از یک سیستم برای ورود به این ایمیل استفاده کنید و آن را به برنامه های امنیتی مورد نیاز، همچون آنتی ویروس، فایروال و... مجهز کنید.

۵ -مراقب باشید که همیشه ارتباط شما با سرور خدمات دهنده ایمیل به صورت رمزگذاری شده و امن (https) برقرار باشد. حتی برای امنیت بالاتر، بهتر است که هنگام استفاده از ایمیل، حتما از سرویس VPN قابل اطمینانی بهره ببرید . همچنین به پیام های خطای مرورگر در خصوص نامعتبر بودن و یا در معرض خطر بودن https سایت خدمات دهنده ایمیل تان کاملا دقت کرده و در صورت اخطار، از ورود به ایمیل اجتناب کنید. بهتر است که برای امنیت بیشتر در این خصوص، از مرورگر کروم برای ورود به ایمیل تان استفاده کنید.

۶ -سعی کنید یکی از مرورگرهای کامپیوترتان را به صورت اختصاصی برای چک کردن ایمیل و کارهای مدیریتی مهم وبلاگ تان اختصاص دهید. با این کار، دیگر بابت خطراتی که ممکن است از جانب دیگر سایت های باز شده در تب های مرورگرتان، شما را تهدید کنند (کوکی های آلوده، حملات فیشینگ، حملات XSS و غیره)نگرانی نخواهید داشت و یا حداقل این نگرانی بسیار کمتر است.

۷ -هیچ گاه از رمز عبور ایمیل تان در دیگر سایت ها و حتی وبلاگ تان استفاده نکنید. هر اکانت مهم شما باید دارای رمز عبور اختصاصی و امن برای خود باشد .زیرا در صورت مشترک بودن رمزهای عبور، فرد مهاجم با دست یابی به یک رمز عبور و کمی سعی و خطا، به همه اکانت های شما دسترسی خواهد داشت.

۸ -به صورت دوره ای رمز عبورتان را عوض کنید. بهترین حالت این است که هر ۳ تا ۴ ماه یک بار رمز عبور تمامی اکانت ها و به خصوص ایمیل خود را تغییر دهید. با این کار تلاش برنامه های مخربی که رمز عبور شما را یافته اند، بی اثر می شود.

درس هفتم– راهنمای پشتیبان گیری از وبلاگ

حتی با رعایت تمام نکات امنیتی و استفاده از مطمئن ترین سرورها و شرکت های هاست، باز هم باید گفت که داستان امنیت هیچ گاه ۱۰۰ درصد و کامل نیست. پس در کنار همه این اقدامات، باید به فکر روز مبادا بود و برنامه ای را جهت نجات وبلاگ در مواقع اضطراری، طرح ریزی کرد.

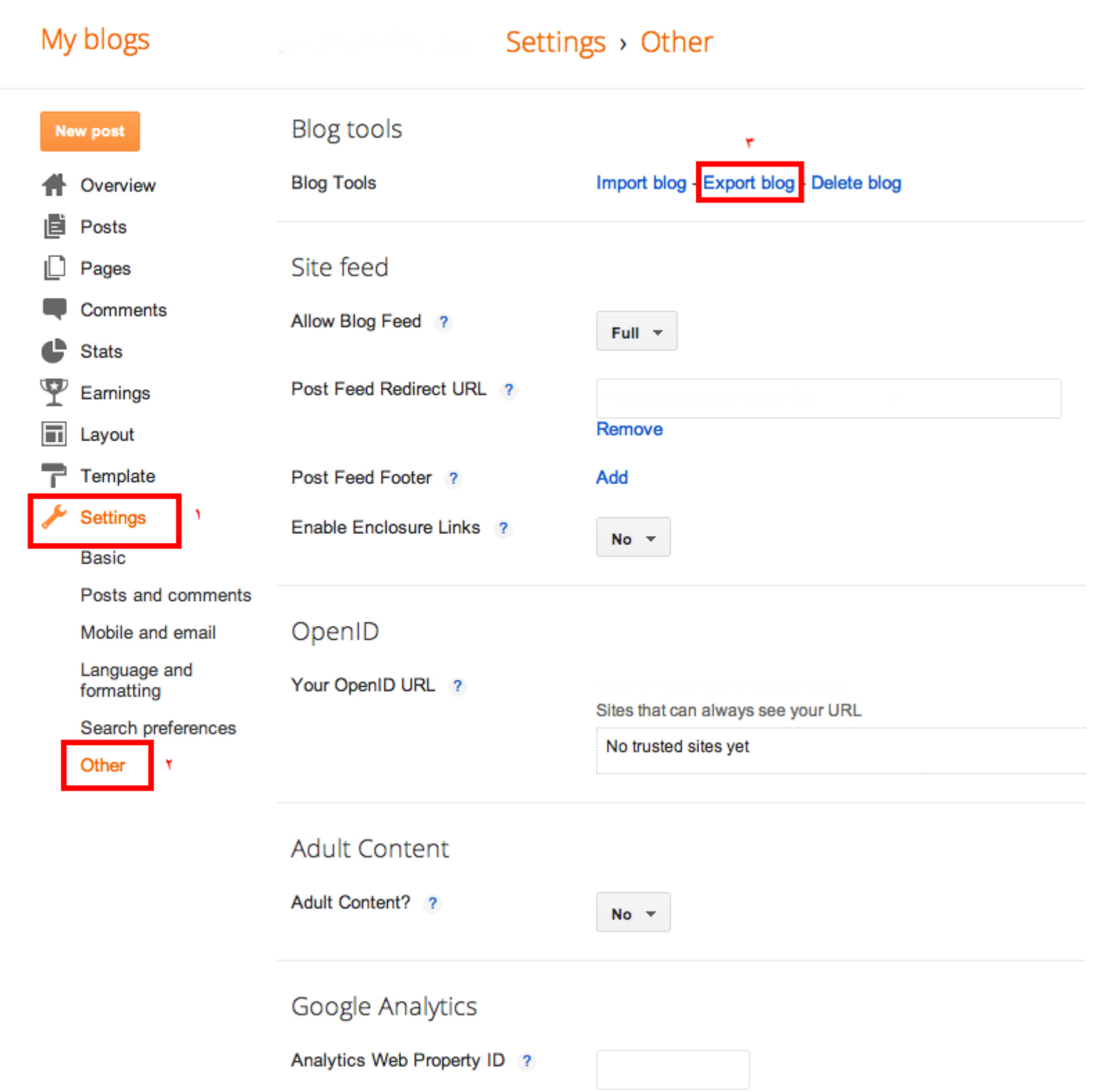
یکی از مهمترین کارهایی که می توان برای اطمینان خاطر بیشتر از مصونیت محتوا و داده های وبلاگ/سایت انجام داد، داشتن برنامه ای منظم و مدون برای پشتیبان گیری از اطلاعات آن است. اگر در دوره« مبانی پشتیبان گیری از اطلاعات » درسنامه شرکت کرده باشید، حتما با این موضوع آشنایی کامل داشته و برنامه صحیحی برای پشتیبان گیری از وبلاگ تان دارید. اما اجازه دهید در این درس هم به طور مختصر اصول و شیوه های پشتیبان گیری از سایت ها و وبلاگ ها (به خصوص وردپرس و بلاگر) را مورد بررسی قرار دهیم.

پشتیبان گیری از وبلاگ در سرویس های وبلاگ نویسی عمومی

علی رغم تمام تاکیدی که بر امنیت سرورهای وبلاگ بلاگر و وردپرس داشتیم و از تیم فنی خبره و پشتیبان گیری خودکار اطلاعات آنها گفتیم، باز هم بهتر است که خودمان هم همیشه نسخه بک آپ به روز از محتوای وبلاگ مان داشته باشیم. این کار در سیستم های وبلاگ نویسی بلاگر و وردپرس معمولا به صورت دستی باید انجام شود و تفاوت زیادی با یکدیگر ندارد.

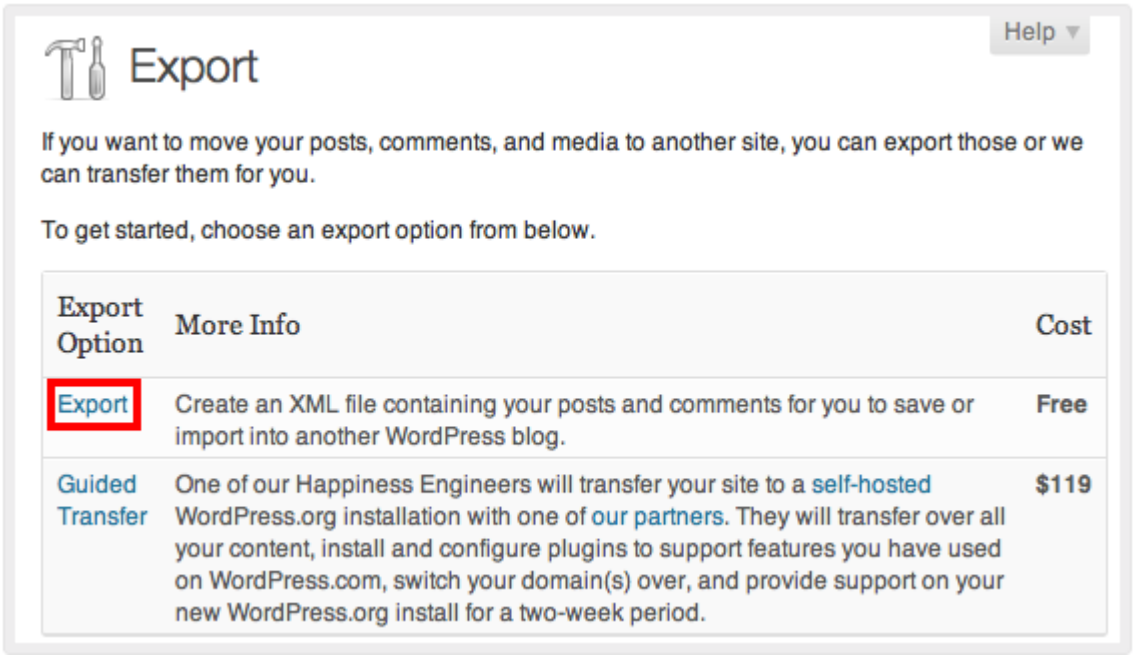
الف- پشتیبان گیری در بلاگر :خوشبختانه بلاگر امکان پشتیبان گیری از تمامی پست ها و نظرات وبلاگ را برای شما امکان پذیر کرده است. و البته در کنار امکان پشتیبان گیری، قابلیت بازیابی نسخه پشتیبان را برای مواقع ضروری پیش بینی کرده است.

با رفتن به تب Settings در داشبورد وبلاگ تان در بلاگر، به بخش Other بروید و از آنجا در بخش Blog tools به Import و Export دسترسی خواهید داشت. با استفاده از گزینهExport blog ، به آسانی نسخه پشتیبان کاملی از وبلاگ خود را بر روی کامپیوترتان خواهید داشت. همه محتوای وبلاگ به همراه نظرات خوانندگان، در قالب یک فایل XMLروی کامپیوتر شما ذخیره خواهند شد.


My blogs
Settings › Other
New post
Overview
Posts
Pages
Comments
Stats
Earnings
Layout
Template
Settings
۱
Basic
Posts and comments
Mobile and email
Language and formatting
Search preferences
Other
۲
Blog tools
Blog Tools
۳
Import blog - Export blog - Delete blog
Site feed
Allow Blog Feed ?
Full
Post Feed Redirect URL ?
Remove
Post Feed Footer ?
Add
Enable Enclosure Links ?
No
OpenID
Your OpenID URL ?
Sites that can always see your URL
No trusted sites yet
Adult Content
Adult Content? ?
No
Google Analytics
Analytics Web Property ID ?

ب- پشتیبان گیری در وردپرس :وردپرس هم مانند بلاگر با گزینه های Import و Export امکان پشتیبان گیری و بازیابی را برای شما فراهم نموده است. برای تهیه نسخه پشتیبان از وبلاگ وردپرسی خود، تنها کافی است از منوی Toolsگزینه Export را انتخاب کنید .حال در صفحه بعد گزینه All content را انتخاب کرده و بر روی دکمه Download Export Fileکلیک کنید. با این کار نسخه ای از وبلاگ شما با پسوند XML روی کامپیوترتان ذخیره خواهد شد.

بازیابی فایل پشتیبان هم به سادگی از طریق گزینه Import در منوی Tools وردپرس امکان پذیر است.



پشتیبان گیری از وبلاگ بر روی هاست اختصاصی

درست است که شرکت خدمات دهنده هاست شما ادعا می کند که به صورت روزانه و دائمی، از تمام اطلاعات نسخه پشتیبان تهیه می کند و شما هیچ گاه نباید نگران از دست دادن اطلاعات تان باشید، اما فراموش نکنید که این ادعا همیشه

هم درست نیست و برخی مواقع شما را به دردسر می اندازد. پس بهتر است در خصوص پشتیبان گیری از وبلاگ و سایت شخصی حساسیتی بیشتر از وبلاگ های سرویس عمومی نشان داده و این کار را به صورت مداوم و منظم انجام دهید.

یک روش تهیه نسخه پشتیبان از سایت و وبلاگ شخصی این است که به صورت دستی، طی زمان های معین، تمامی فایل های متعلق به سایت را بر روی کامپیوترتان دانلود کرده و در محل امنی نگهداری کنید. البته در این شیوه علاوه بر تهیه نسخه پشتیبان از فایل ها، لازم است که از طریق بخش مدیریت دیتابیس سایت، از پایگاه داده سایت هم نسخه پشتیبان کامل و مناسبی تهیه کرده و به همراه فایل ها نگهداری کنید. این بخش در Cpanel با نام phpMyAdmin شناخته می شود.

در بسیاری از کنترل پنل های مدیریت سایت، شما امکان تهیه نسخه پشتیبان یا Backupکاملی از تمامی اطلاعات سایت و همچنین دیتابیس و ایمیل ها دارید. در این شیوه شما دستور تهیه نسخه پشتیبان را در کنترل پنل صادر کرده و منتظر اتمام کار می شوید. سپس نسخه پشتیبان سایت را در قالب یک فایل فشرده در اختیار دارید که می توانید آن را بر روی کامپیوترتان دانلود کرده و در محل امنی نگه داری کنید.

راه حل دیگر تهیه نسخه پشتیبان، استفاده از ماژول ها و افزونه های سیستم مدیریت محتوای وبلاگ است. تقریبا تمامی برنامه های مدیریت محتوا این امکان را دارند که با استفاده از چند ماژول و پلاگین، به صورت خودکار یا دستی نسخه پشتیبانی از وبلاگ تان تهیه کنند. حال بسته به برنامه و پلاگین مورد استفاده، این نسخه پشتیبان می تواند بر روی خود هاست ذخیره شود، یا اینکه به سرویس های کلود و هارد کامپیوتر شما منتقل گردد. در اینجا به معرفی دو پلاگین مفید و پرکاربرد وردپرس در این زمینه می پردازیم:

WordPress Backup to Dropbox: -احتمالا با سرویس دراپ باکس آشنایی داشته و از آن برای ذخیره امن فایل های خود در یک فضای کلود رایگان بهره می برید. با توجه به اینکه فضای دراپ باکس شما در ارتباط با کامپیوترتان است و هر فایلی را که درون فضای کلود دارید، نسخه ای از آن روی کامپیوتر شما هم موجود است، لذا این سرویس می تواند گزینه بسیار مناسبی برای نگهداری نسخه های پشتیبان باشد.

با استفاده از این پلاگین شما به راحتی و به صورت خودکار می توانید نسخه های بک آپ منظمی از وبلاگ خود تهیه کرده و آنها را به دراپ باکس منتقل کنید .سازنده این پلاگین می گوید: «تنها کافی است که روز و دفعات پشتیبان گیری در هفته یا ماه را مشخص کرده و دستور شروع کار برنامه را صادر کنید. اکنون دیگر نیازی به دخالت شما نیست و تنها باید منتظر اتمام کار بمانید، تا نسخه ای از تمامی فایل ها و دیتابیس سایت تان به صورت زیپ شده به حساب دراپ باکس تان منتقل گردد».

BackWPup: -این برنامه تقریبا یک راه حل کامل برای پشتیبان گیری از وبلاگ وردپرسی شما است. پلاگین BackWPupمی تواند از دیتابیس سایت شما و تمامی فایل ها و فولدرهای آن نسخه پشتیبانی تهیه کرده و آن را به صورت یک فایل زیپ شده در اختیار تان قرار دهد.

این پلاگین همچنین قادر است علاوه بر ذخیره نسخه پشتیبان بر روی هاست، آن را به سرور FTP دیگر، Google Storage، اکانت Amazon S3 و یا فضای کلود دراپ باکس تان انتقال دهد. از دیگر قابلیت های این پلاگین می توان به چک و اصلاح دیتابیس، بهینه سازی دیتابیس، انتقال نسخه پشتیبان به سرویس SugerSync و ارسال لاگ عملیات پشتیبان گیری به ایمیل اشاره کرد.

نکات امنیتی در پشتیبان گیری

۱ -به عنوان یک اصل مهم و حیاتی، همیشه نسخه پشتیبان وبلاگ خود را پس از دانلود کردن، یک بار روی کامپیوترتان امتحان کنید، تا از سلامت آن مطمئن شوید. بدترین سناریو این است که شما بک آپ منظم و کاملی از وبلاگ تان داشته باشید، اما هنگام نیاز به دلیل خراب بودن فایل پشتیبان، نتوانید از آن استفاده کنید.

۲ -برنامه ریزی مشخصی برای حذف نسخه های پشتیبان قدیمی داشته باشید. بسته به کاربرد، ارزش و حجم فایل های پشتیبان، می توان عمر مفید آنها را تعیین کرد .اما معمولا نیاز نیست که یک نسخه بک آپ را بیش از شش ماه نگهدارید.

پس برای اینکه جلوی اتلاف فضای ذخیره سازی و سردرگمی شما گرفته شود، مرتبا نسخه های قدیمی پشتیبان را به شکل امن و مطمئنی نابود کنید. در انتخاب شیوه حذف و نابودی نسخه پشتیبان هم دقت لازم را به خرج دهید، زیرا این فایل ها، حاوی اطلاعات مهم و حیاتی از شما و وبلاگ تان هستند. برای اطلاعات بیشتر در این مورد می توانید در دوره مبانی امنیت در کامپیوتر و اینترنت درسنامه شرکت کنید.

۳ -تا حد امکان نسخه های پشتیبان را رمزنگاری کرده و سپس به ابزارهای پشتیبان گیری همچون هارد دیسک، فلش مموری یا دی وی دی منتقل کنید. برای این کار می توانید از برنامه ای همچون TrueCryptاستفاده کرده و یا تنها هنگام فشرده سازی فایل پشتیبان، از برنامه هایی چون 7-Zipکمک بگیرید که امکان رمزگذاری بر روی فایل زیپ را دارند.

۴ -حتما و همیشه دو یا چند نسخه از اطلاعات پشتیبان گرفته شده را نگهداری کنید. اکتفا کردن به یک ابزار برای نگه داری فایل های بک آپ، آنها را در معرض خطر نابودی قرار می دهد. زیرا در صورت بروز مشکل برای آن ابزار، شما هیچ نسخه دیگری از اطلاعات را در اختیار نخواهید داشت. حتی برای امنیت بیشتر، بهتر است که دو یا چند نسخه از فایل های پشتیبان در مکان های فیزیکی جداگانه ای نگهداری شوند.

۵ -برای انتخاب پلاگین یا سرویس مناسب پشتیبان گیری وقت صرف کرده و گزینه های مختلف را امتحان کنید تا بهترین شیوه را بیابید. برای انجام این کار برنامه ریزی زمانی مشخص و دقیقی داشته باشید. پس از هر پشتیبان گیری از سلامت نسخه بک آپ اطمینان یابید.

همچنین فایل ها و بخش هایی از سایت/وبلاگ را که باید نسخه پشتیبان آنها تهیه شود، مشخص کنید. معمولا لازم است که علاوه بر تهیه بک آپ از تمامی فایل های اصلی برنامه مدیریت محتوا، از عکس ها و فایل هایی که بر روی هاست آپلود

کرده و در سایت استفاده نموده اید هم پشتیبان گیری شود. و مهمتر از آن اینکه از دیتابیس یا پایگاه داده سایت هم باید همیشه نسخه پشتیبان سالم و به روزی داشته باشید. زیرا تقریبا تمامی محتوای نوشتاری سایت شما درون آن قرار دارد.

۶ -و آخرین نکته درس امروز این است که حتما یک پلن و شیوه نامه مدون و مشخص برای پشتیبان گیری داشته باشید. اکنون علاوه بر انجام یک پشتیبان گیری درست و اصولی، عمل پشتیبان گیری کم کم تبدیل به یکی از عادت ها و کاری روتین می شود. همچنین در صورتی که زمانی بخواهید این مسئولیت را بر عهده شخص دیگری بگذارید، وی دقیقا می داند که چه کاری و به چه صورت باید انجام گیرد.

درس هشتم– آشنایی با مهمترین حملات به وبلاگ ها و وب سایت های شخصی

جدا از اینکه شما در رعایت مسایل امنیتی تا چه حد کوشا باشید و از خدمات امن و مطمئن برای وبلاگ یا سایت شخصی تان بهره ببرید و تمامی نکات پشتیبان گیری و وبلاگ نویسی اصولی را رعایت کنید؛ همیشه هستند افرادی که با شیوه های مختلف و ابزارهای متفاوتی به جنگ وبلاگ شما آمده و سعی در نفوذ به آن و یا از کار انداختنش خواهند داشت.

توجه کنید در این درس به حملاتی می پردازیم که به صورت آنلاین وبلاگ شما را هدف گرفته اند و باید بدانید که این همه حملات را شامل نمی شود. ممکن است یک هکر کامپیوتر یا تلفن هوشمند شما را هدف بگیرد که در این صورت روش های حمله متفاوت خواهد بود. برای جلوگیری از آن حملات نیاز است روی امنیت سیستم عامل، مرورگر و دیگر موارد مرتبط تمرکز کنید.

ممکن است آشنایی با برخی اصطلاحات تخصصی حملات امنیتی چندان کارایی برای شما نداشته باشد و حتی در جلوگیری از برخی از آنها کمکی هم نکند. اما به طور حتم آگاهی از اینکه آلودگی و نفوذ از چه راهی انجام گرفته، در حل سریع تر مشکل توسط مدیران سرور و همچنین تعامل شما با آنها کمک فراوانی خواهد نمود.

فیشینگ(Phishing)

فیشینگ یکی از تکنیک های مهندسی اجتماعی است که فرد حمله کننده از ارتباطات الکترونیک یا شبکه های اجتماعی، برای کلاهبرداری و تطمیع گیرنده استفاده می کند تا موفق به دستیابی به اطلاعات وی شود. شاید این شیوه را بتوان یکی از عمومی ترین و پرکاربردترین راه های نفوذ به اطلاعات شخصی و در دست گرفتن کنترل ایمیل، وبلاگ یا دیگر اکانت های افراد دانست. در بسیاری از مواقع این کار با استفاده از ایمیل انجام می شود و البته گاهی از ارسال پیام در شبکه های اجتماعی و پیامک موبایل هم بهره می برند.

در این حمله، پیام ارسالی قلابی برای شما، معمولا به ظاهر از طرف فرد یا شرکتی ارسال شده که کاملا مورد اطمینان شما است. مثلا به نظر می رسد که ایمیل از طرف شرکت فروشنده هاست و دامنه، بانک یا شرکت خدمات دهنده اینترنت شما است و درون ایمیل از شما درخواست برخی اطلاعات شخصی و حتی گاهی اوقات رمزهای عبور می شود.

در شکل دیگر ماجرا، ایمیل ارسالی حاوی لینک یا لینک هایی است که شما را به صفحاتی بسیار شبیه سایت های معمول مورد استفاده تان می برند و در آنجا شما با ورود رمز عبور و نام کاربری، علاوه بر ورود بدون مشکل به سایت مورد نظر خود، اطلاعات تان را در اختیار ارسال کننده ایمیل هم قرار داده اید.

همیشه مراقب ایمیل های دریافتی باشید و در صورتی که حاوی درخواست غیر عادی یا مهمی بودند، به بررسی بیشتر موضوع بپردازید. در صورت امکان قبل از ارسال هرگونه اطلاعاتی، به صورت تلفنی در خصوص صحت ایمیل سوال کنید. تا حد امکان حتی در صورتی که اطمینان نسبی به ایمیل دارید، اما امکان تایید تلفنی یا حضوری آن را ندارید، از ارسال پاسخ خودداری کنید.

به یاد داشته باشید که معمولا شرکت های خدمات دهنده به شما و مراکزی مانند بانک، هیچ گاه و به هیچ وجه به صورت ایمیلی از شما درخواست رمز عبور، نام کاربری یا اطلاعات خصوصی مهم نمی کنند.

در ایمیل های مشکوک و ناشناس به هیچ وجه بر روی لینک ها کلیک نکنید. در صورتی که می خواهید وارد سایتی شوید، آدرس آن را به صورت دستی در مرورگر تایپ کنید. قبل از ورود نام کاربری و رمز عبور در هر سایتی، ابتدا آدرس بار را کنترل کنید تا نشانی سایت کاملا درست و صحیح باشد. در سایت هایی که از ارتباط امن SSL و آدرس https استفاده می کنند، حتما مراقب این نکته باشید و کنترل کنید که آدرس صفحه ای که باز کرده اید به صورت امن و https باشد.

حمله Brute-force

در این شیوه فرد نفوذگر با استفاده از برنامه های ویژه ای، به صورت خودکار و مداوم ترکیبات مختلف نام کاربری و رمز عبور را امتحان می کند تا بالاخره به ترکیب مناسب برای ورود به سایت دست پیدا کند. در این سیستم معمولا از لغات و عبارت های موجود در دیکشنری و ابزارهایی مانند آن استفاده می شود و برنامه تا جایی به کار خود ادامه می دهد که موفق به پیدا کردن نام کاربری و رمز عبور شما شود.

یکی از مهم ترین شیوه های مقابله با چنین حملاتی، استفاده از پلاگین های امنیتی است که پس از دفعات مشخص ورود نام کاربری و رمز عبور اشتباه، جلوی دسترسی کامپیوتر وارد کننده نام های کاربری را بگیرد و به وی اجازه کار ندهد. این جلوگیری معمولا با بلاک کردن آی پی آن سیستم انجام می شود.

شما می توانید با افزونه ها و برخی کدها و دستورات برنامه نویسی، این امکان را فراهم آورید که مثلا فرد یا کامپیوتر مشکوک، با ورود سه رمز عبور اشتباه دیگر دسترسی این کار را نداشته باشد. و یا اینکه دسترسی به بخش لاگین را تنها برای آی پی های ویژه ای باز بگذارید و دیگران امکان ورود به این بخش را نداشته باشند.

نکته دیگر در مقابله با این حمله، استفاده از رمز عبور امن است که به اندازه ای طولانی باشد تا حدس زدن آن چندان ساده نباشد. همچنین عدم استفاده از نام کاربری پیش فرض برنامه مدیریت محتوا و یا استفاده از نام کاربری های شناخته شده ای چون Admin و administrator و user1 و moderator و... می تواند کار را برای نفوذگران دو چندان سخت تر کند.

علاوه بر این در برخی برنامه های مدیریت محتوا، می توانید آدرس صفحات مدیریتی سایت و وبلاگ را هم به طور کامل تغییر دهید. با این کار فرد حمله کننده قبل از اینکه امکان آزمون- خطا برای یافتن رمز عبورتان را داشته باشد، باید ابتدا صفحه مدیریت را برای ورود نام کاربری و رمز عبور پیدا کند. استفاده از نام های عجیب می تواند کمک خوبی در این زمینه باشد. چرا نام صفحه ورود به بخش مدیریت وبلاگ تان به جای Admin یا administrator و مانند آن، چیزی شبیه نام یک گیاه یا غذای مورد علاقه تان نباشد؟

مهندسی اجتماعی

این شیوه به روش های بسیار متفاوت و پیچیده ای انجام می شود که یکی از آنها را در بخش فیشینگ توضیح دادیم. به شکل ساده، مهندسی اجتماعی عبارت است از تکنیک های روانشناسی اجتماعی که فرد مهاجم سناریویی را آماده می کند و با استفاده از آن، شما را ترغیب به انجام کاری یا در اختیار قرار دادن اطلاعاتی می کند. این کار گاهی با تطمیع یا تهدید و بسیاری اوقات با جعل و حقه انجام می شود.

همان طور که در بخش فیشینگ گفتیم، مهم ترین و بهترین دفاع در برابر این حملات، عدم اطمینان کاذب به افراد آنلاین است. زیرا به راحتی امکان جعل آدرس های سایت ها، اکانت شبکه های اجتماعی و ایمیل ها وجود دارد. هنگام مواجه با هرگونه درخواست اطلاعات حساس، تا حصول اطمینان ۱۰۰ درصد از راه های مختلف، هیچ گونه اطلاعاتی را در اختیار کسی قرار ندهید. اگر درخواست ایمیلی برای دریافت اطلاعات دارید، حتما تلفنی و در صورت امکان حضوری، از صحت آن مطمئن شوید. اگر از طریق تلفن هم نمی توانید از هویت درخواست دهنده اطمینان حاصل کنید، حتما نیاز به مراجعه حضوری و تحویل آن اطلاعات دارید.

Packet Sniffer

در این شیوه حمله که می توان آن را نوعی شنود نامید، فرد نفوذگر به نوعی به یکی از کامپیوترهای اصلی درون شبکه بی سیم یا کل شبکه ISP شما دسترسی پیدا می کند و آنگاه با نصب برخی نرم افزارها، تمام پاکت های (Pockets) اطلاعاتی رد و بدل شده توسط افراد را کنترل و ضبط می کند. با این کار وی می تواند به هر چیزی اعم از محتوای ایمیل ها، سایت های وارد شده و حتی نام کاربری و رمز عبور وارد شده درون سایت های مختلف دست پیدا کند. زیرا تمامی این داده ها به صورت بسته های اطلاعاتی در شبکه ارسال می شوند و در صورتی که رمزگذاری نباشند، به راحتی قابل ردگیری و خوانده شدن هستند

اولین قدم در راه مقابله با چنین حملاتی، عدم استفاده از شبکه های بی سیم عمومی و ناشناس، و همچنین رمزگذاری و حفظ امنیت شبکه بی سیم خصوصی تان است. در صورتی که شبکه وایرلس شما توسط رمز عبور قدرتمندی محافظت شود و تنها دستگاه هایی که مک آدرس آنها درون شبکه ثبت شده، قادر به ارتباط با آن باشند، تا حد زیادی جلوی اسنیف شدن اطلاعات گرفته می شود.

مرحله بعد ارسال رمزنگاری شده اطلاعات درون شبکه و اینترنت است. در این حالت، حتی در صورتی که کسی بتواند بین راه اطلاعات را خوانده و ضبط کند، چیزی از آنها دستگیرش نمی شود. اینجا است که اهمیت بالای استفاده از SSL مشخص می شود. چرا که در این صورت هکری که به شبکه بی سیم شما نفوذ کرده امکان بازکردن و خواندن اطلاعات ارسالی و دریافتی را نخواهد داشت.

حملات تزریق کد (SQL Injection)

در این نوع از حمله فرد مهاجم از تکنیک هایی استفاده می کند تا با نفوذ و در اختیار گرفتن دیتابیس یا پایگاه داده های سایت، کنترل آن را در دست گرفته و به تخریب بپردازد. در این شیوه فرد نفوذگر معمولا از طریق راه های نفوذ مختلفی که ممکن است در وبلاگ شما باز باشد، دستورات دیتابیس (Quary) یا فرمان های برنامه نویسی خاصی را برای سایت ارسال و دیتابیس را مجبور به انجام آنها می کند.

در نتیجه این حملات در حالت ساده، فرد مهاجم قادر به پاک کردن و نابودی اطلاعات است و در حالت های پیچیده تر، وی بدون اطلاع شما و از طریق دسترسی به دیتابیس، امکان ورود به بخش مدیریت سایت را هم پیدا می کند. یکی از معمول ترین راه هایی که افراد می توانند کدهای مخرب را وارد دیتابیس وبلاگ کرده و آنها را اجرا کنند، فرم های موجود از قبیل تماس با ما، بخش نظرات و صفحات عضویت است. البته گاهی از طریق دستورات Get/Post هم انجام چنین کاری امکان پذیر است. به همین دلیل باید در تنظیمات برنامه مدیریت محتوا کاملا مراقب چنین حملاتی باشید و فرم ها به گونه ای ساخته شوند که قبل از ارسال و ذخیره هرگونه اطلاعاتی در دیتابیس، آنها را کنترل کرده و جلوی اجرای هرگونه دستور و کد برنامه ای را بگیرند.

حمله عدم پذیرش سرویس (DOS)

این شیوه در واقع یک حمله برای نفوذ به سایت و یا در اختیار گرفت آن نیست، بلکه تنها هدف از چنین حمله ای، هدر دادن منابع سیستمی سایت یا وبلاگ مورد نظر و از کار انداخت آن است. به گونه ای که در یک حمله سازمان یافته و کلاسیک DOS سایت هدف برای مدت زمانی به صورت کامل از دسترس کاربران خارج می گردد.

در این روش فرد مهاجم از طریق تعداد زیادی کامپیوتر آلوده که در اختیار وی هستند، یا یک کامپیوتر با پهنای باند بالا به ارسال درخواست های مداوم و تکراری به سایت هدف می پردازد. این درخواست می تواند تنها نمایش صفحه ای از سایت و یا سعی برای ارسال نظر یا پیشنهادی باشد و یا در مراحل پیشرفته، می تواند اجرای کد یا فرمانی بر روی سرور و ایجاد مشکل برای آن باشد.

از آنجایی که هر سایت و وبلاگ، بسته به سرور خدمات دهنده اش، میزان محدودی از منابع (همچون پهنای باند، قدرت پردازشگر مرکزی، ترافیک ماهیانه و...) را در اختیار دارد، این درخواست های پرشمار و بی پایان تا آنجا ادامه می یابند که دیگر سرویس دهنده وبلاگ پاسخگوی آنها نبوده و از دسترس خارج گردد.

متاسفانه در حملات این چنینی کار زیادی از دست شما بر نمی آید و باید تمام امیدتان به مدیر و تیم فنی خبره شرکت سرویس دهنده هاست تان باشد. آنها می توانند با اقداماتی همچون بلاک کردن آی پی کامپیوترهای مهاجم و جلوگیری از دسترسی آنها به سایت، تا حد زیادی در نجات به موقع وبلاگ شما موثر باشند.

البته گاهی هم چنین حملاتی موجب تحمیل هزینه های ناخواسته برای شما خواهند بود، برای مثال در صورت محدود بودن ترافیک ماهیانه وبلاگ شما، بعد از یک حمله DOSیا باید تا شروع ماه جدید وبلاگ تان در دسترس نباشد و یا اینکه با پرداخت هزینه ای، میزان ترافیک آن را افزایش دهید.

حملات تزریق اسکریپت (XSS)

در این شیوه فرد مهاجم با استفاده از کامپیوتر آلوده دیگری به جنگ کامپیوتر شما یا سرور وبلاگ تان آمده و با تزریق برخی کدهای خاص درون مرورگر وب تان، اطلاعاتی را که در مرورگر دریافت کرده یا ارسال می کنید، سرقت می کند و یا مسیر آنها را تغییر می دهد. این حمله معمولا از طریق ارسال یک آدرس خاص اینترنتی برای قربانی (با استفاده از شیوه هایی همچون فیشینگ) آغاز می گردد.

در صورتی که فرد مهاجم موفق به نفوذ شود، می تواند اطلاعات اشتباهی را به شما نشان دهد و یا به صورت کامل کنترل صفحه اصلی سایت را به دست گیرد. علاوه بر این می تواند به کلیه اطلاعات مورد استفاده شما در اینترنت دست یافته یا شما را بدون آگاهی خودتان، به آدرس و محل دیگری در اینترنت منتقل سازد .همچنین با تزریق اسکریپت در مرورگر، فرد مهاجم امکان سرقتSession ها و نفوذ به بخش مدیریت سایت و یا تغییر چهره کامل سایت و حذف اطلاعات صفحه آن را در اختیار دارد.

بخش مهمی از جلوگیری از حملات تزریق اسکریپت به بخش فنی و کدنویسی سایت و وبلاگ شما بر می گردد. به گونه ای که به هیچ وجه به کاربران تان امکان استفاده از کاراکترها و کدهای ویژه را در فرم ها یا آدرس های ارسالی شان ندهید. راحت ترین کار این است که تا حد امکان، کاربران امکان استفاده از HTMLو CSS را در هیچ بخشی نداشته باشند.

به طور کلی، بهترین دفاع در این حملات، کمترین امکان دسترسی کاربر است. سعی کنید که کاربران تنها و تنها به موارد مورد نیاز و ضروری دسترسی داشته باشند، تا نتوانند به چنین تخریب هایی بپردازند.

همانطور که گفتیم ممکن است شما نتوانید برای مقابله با برخی از این حملات شخصا کاری انجام بدهید. اما آگاهی داشتن خودش نیمی از مسیر است.

درس نهم– نکاتی برای بهبود کارایی و عملکرد وبلاگ

در پایان دوره کمی درباره کارایی و عملکرد وبلاگ و وب سایت های شخصی تحت برنامه مدیریت محتوای وردپرس صحبت خواهیم کرد. شاید در ظاهر این امر تنها در افزایش سرعت و راحتی بیشتر کاربران یا افزایش رتبه SEO سایت موثر باشد .اما باید این نکته را در نظر داشت که وقتی وبلاگ شما به شکل مناسبی بهینه شده باشد و به درستی از منابع سیستمی موجود استفاده کند، تا حد زیادی در برابر برخی حملات امنیتی هم تاب و توان بیشتری خواهد داشت و دیرتر از پا در می آید.

استفاده از YSlow برای اندازه گیری مدت زمان لود صفحات وبلاگ

قبل از هرگونه بهینه سازی، باید معیاری برای سنجش سرعت وبلاگ تان داشته باشید تا بتوانید میزان سودمندی هر مرحله از بهینه سازی ها را بسنجید .یکی از افزونه های سودمند برای مرورگرهای مختلف است که صفحات وبلاگ شما را محک زده و مشخص می کند سرعت لود هر بخش چقدر است. این افزونه ضمن امتیازدهی به صفحات وبلاگ تان، ایرادهای معمول را که باعث کاهش سرعت شده اند مشخص نموده و برخی پیشنهادات را هم جهت رفع شان عرضه می کند. این افزونه از سرویس Smush.itیاهو برای انجام تست ها بهره می برد.

تنظیمات لازم برای cache وردپرس

در وردپرس و دیگر برنامه های مدیریت محتوا که اطلاعات به صورت دینامیک ارائه می شوند، در حالت عادی برای هر دفعه باز شدن صفحه ای از سایت، لازم است که درخواستی به دیتابیس ارسال شده و مطلب همراه با آدرس دهی لازم برای عکس و دیگر مدیا از آنجا خوانده شود. این کار در سایت های پربازدید، فشار فراوانی بر سرور وارد کرده و خود به تنهایی می تواند نوعی حمله DOS به سرور محسوب شود. زیرا اجزای هر فرمان یا Query درون دیتابیس به منابع سیستمی فراوانی نیاز دارد.

بهترین راه حل این مشکل، استفاده از سیستم کش (Cache) است. بدین صورت که با تولید هر مطلب و محتوا، سیستم یک بار آن را از سرور درخواست کرده و تبدیل به یک صفحه استاتیک معمولی می کند. اکنون برای پاسخ به هر درخواست کاربر جهت نمایش این صفحه، همان صفحه استاتیک به مرورگر وی ارسال شده و نیازی به ایجاد ارتباط با دیتابیس نیست. البته این صفحه در بازه های زمانی مشخص دوباره سازی می شود تا تغییرات صورت گرفته همچون کامنت های خوانندگان و یا ویرایش توسط شما را نمایش دهد.

بسیاری از سیستم های مدیریت محتوا درون خود به نوعی دارای امکان کش کردن صفحات را دارند که می توانید آن را فعال کنید. اما برای استفاده بهینه از امکان کش، پلاگین و افزونه های کارآمدی هم نوشته شده است.

در وردپرس شما می توانید به سادگی یکی از پلاگین های WP Super Cache یا W3 Total Cacheرا نصب کرده و نسخه کش شده بهینه و مناسبی از صفحات تان را در اختیار کاربر قرار دهید W3 Total Cache .یکی از پرکاربرد ترین پلاگین های کش وردپرس است که توسط برخی از سایت های مشهور همچون Mashableهم استفاده می شود. طبق نظر برخی منابع، این پلاگین ها، سرعت لود شدن صفحات سایت را تا ۱۰ برابر افزایش می دهند.

استفاده از شبکه توزیع محتوا(CDN)

یکی دیگر از مشکلاتی که ممکن است باعث کندی سایت شما شود، تمرکز محتوا بر روی یک سرور است که کاربران مختلف بسته به فاصله و شیوه دسترسی، ممکن است با مشکلاتی در مشاهده سایت مواجه شوند.

CDNیا Content Delivery Network به طور ساده، مجموعه ای از سرورهای بهینه شده در سراسر دنیا است که به صورت یک سرور مجازی یکپارچه عمل می کنند. با استفاده از چنین سرویسی، شما می توانید فایل های استاتیک دائمی مانند قالب، عکس ها، جاوا اسکریپت و CSS را بر روی CDN قرار دهید تا کاربر هنگام باز کردن وبلاگ شما، آنها را از نزدیک ترین سرور به خودش، دریافت کند.

البته به صورت معمول برای استفاده از CDN باید هزینه ماهیانه یا سالیانه ای پرداخت کنید و این هزینه بسته به میزان ترافیک درخواستی به صورت تصاعدی افزایش خواهد داشت. هر چند که به شکل محدود می توانید از برخی جایگزین های رایگان هم برای این کار استفاده کنید. یکی از بهترین جایگزین های رایگان برای این کار، Google App Engine است. اما تنها ایراد این سرویس گوگل، محدودیت پهنای باند آن است که روزانه تنها یک گیگابایت ترافیک در اختیار دارید.

این راهنمای گام به گام می تواند کمک خوبی برای استفاده از Google App Engine به عنوان یک CDN باشد.

تصمیم گیری درست در مورد ابزار و کارکردهای وبلاگ

هیچگاه تنها برای پر کردن فضای خالی صفحه و یا نشان دادن امکانات فراوان وبلاگ تان، هر چیزی را روی آن قرار ندهید. احتمالا شما هم وبلاگ/وب سایت های زیادی را دیده اید که فروم، باکس چت، شمارنده بازدیدکننده یا ساعت و تاریخ را در طراحی خود جای داده اند.

اگر به دنبال وبلاگی سریع هستید، تا حد امکان آن را سبک و خلوت نگه دارید و دکور الکی به آن آویزان نکنید. همه پلاگین های اضافی و بدون کاربرد را غیرفعال کنید و تنها از چیزهایی استفاده کنید که واقعا ضروری هستند. زیرا بسیاری از پلاگین ها و این امکانات اضافه، فایل های متعدد CSS و JS ایجاد کرده و برای فعالیت شان درخواست های مکرری را به دیتابیس می فرستند و حتی گاهی جداول اضافی به دیتابیس اضافه می کنند. همه این موارد علاوه بر اینکه می توانند باگ های امنیتی خطرناکی باشند، باعث پردازش بیشتر و سنگین تر در سرور و پایین آمدن سرعت وبلاگ خواهند شد.

بهینه سازی و کم حجم کردن عکس های مورد استفاده در وبلاگ

هر چه تعداد عکس بیشتری در قالب و مطالب وبلاگ تان استفاده کنید، به همان اندازه هنگام لود شدن صفحه، درخواست های http بیشتری به سرور ارسال می گردد. درباره بهینه سازی عکس، باید در دو بخش عکس های قالب یا تمپلیت و عکس های مورد استفاده در مطالب و پست ها صحبت کنیم.

۱ -بهینه سازی عکس های تمپلیت :یکی از بهترین راه ها برای بهینه سازی قالب، کاهش عکس های استفاده شده به حداقل ممکن است. هیچ گاه برای نشان دادن فونت از عکس آن استفاده نکنید .زیرا علاوه بر افزایش حجم وبلاگ، به همان تعداد درخواست http بیشتری تولید می شود. بهتر است که به جای آپلود یک فایل حجیم عکس و استفاده از آن برای فونت یک بخش خاص، همان فونت را (که حجم کمتری هم دارد) بر روی سرور قرار دهید و با دستوراتی از قبیل fontfaceآن را در جاهای مورد نیاز فراخوانی کنید. این کار علاوه بر کاهش حجم وبلاگ و کم کردن از درخواست هایhttp ، از نظر SEO هم تاثیر فراوانی دارد. زیرا با این کار بخش بیشتر و مهمتری از سایت (معمولا تیترها) توسط ماشین قابل خواندن خواهد بود و در موتورهای جستجو ایندکس می شوند.

= = = = = = using-css-sprites == = = = = = = = =

یک راه دیگر برای کاهش حجم و تعداد درخواست http قالب، استفاده از تکنیک CSS Sprites است. در این شیوه شما برای بخش هایی همچون منوها و Navigation Bar به جای استفاده از چندین عکس کوچک، از یک عکس بزرگ تر استفاده می کنید و با استفاده از دستوراتCSS ، همان قسمت مربوطه را در جای خود به نمایش می گذارید.

اکنون به جای چندین درخواست http برای لود شدن عکس ها، تنها یک درخواست ارسال شده و عکس در مرورگر کش می شود و هم اینکه معمولا حجم این فایل از مجموع فایل های کوچک مورد استفاده کمتر است.

این راهنما می تواند کمک خوبی برای یادگیری شیوه استفاده از CSS Sprites باشد.

۲ -بهینه سازی عکس مطالب و پست ها :اولین نکته در این خصوص، استفاده به جا و مناسب از عکس است. یک وبلاگ بدون عکس، روح و جان چندانی برای جذب مخاطب ندارد. اما به همان نسبت یک وبلاگ که تا خرخره با عکس های حجیم و سنگین پر شده، می تواند آن قدر دیر باز شود، که کاربر از خیر دیدن آن بگذرد.

قبل از استفاده از عکس در وبلاگ، اندازه و حجم آن را تا حد ممکن و به شکلی که افت کیفیت، چندان محسوس نباشد کاهش دهید. برای این کار ابزارهای آنلاین و آفلاین فراوانی وجود دارند. گزینه Save for web and devices در فتوشاپ یکی از انتخاب های مناسب جهت کاهش حجم و اندازه عکس است .در این مطلب می توانید تعدادی از گزینه های مناسب برای این کار را بیابید.

نکته مهم دیگر در خصوص اندازه و حجم عکس ها، این است که هیچ گاه از دستورات HTMLبرای کم کردن طول و عرض عکس و جا دادن آن در صفحه استفاده نکنید .زیرا با این کار، در حقیقت شما یک فایل حجیم و سنگین با طول و عرض بزرگ را در صفحه یتان لود کرده اید و آنگاه آن را به اجبار درون کادر کوچکی جا داده اید.

بهترین راه این است که عرض ثابتی را برای استاندارد عکس های وبلاگ تان تعیین کنید و همیشه قبل از آپلود و استفاده از عکس ها در سایت، آنها را با برنامه مناسبی، کوچک کرده و به اندازه استاندارد برسانید. با این کار حجم عکس هم تا حد فراوانی کاهش یافته و سریع تر لود می شود.

و نکته آخر اینکه هنگام قرار دادن عکس ها در قالب و یا مطالب، طول و عرض آنها را با دستور height و width مشخص کنید. با این کار مرورگر مکان لازم برای لود عکس را مشخص کرده و دیگر نیازی به محاسبه طول و عرض آن جهت تعیین فضای لازم ندارد.

ذخیره سازی کدهای جاوا اسکریپت و CSS به صورت فایل هایی مستقل ازIndex

وقتی که کاربر برای اولین بار به وبلاگ شما سر بزند، مرورگر کلیه فایل های حاوی مدیا یا دستوراتی را که خارج از فایل اصلی قالب قرار گرفته اند، دانلود کرده و آنها را برای استفاده های بعدی کش می کند.

مثلا اگر دستورات CSS لازم برای تمپلیت وبلاگ را درون فایل اصلی آن قرار دهیم، با هر بار باز شدن وبلاگ، تمامی این دستورات دوباره بازخوانی و اجرا می شوند، اما اگر کلیه دستورات CSS را درون فایل جداگانه ای ذخیره کنید، تنها یک بار نیاز به فرا خواندن آن است و در دفعات بعدی از فایل CSS کش شده استفاده می شود. در خصوص JS هم به همین شکل باید عمل کرد.

نکته دیگر در خصوص این دستورات، آن است که فایل سی اس اس را در ابتدای لود شدن وبلاگ فراخوانی کنید. برای این کار دستور فراخوانی آن باید در قسمت <head>باشد. اما فایل جاوا اسکریپ را بهتر است در پایان کار لود صفحه

فراخوانی کنید. برای این کار باید دستور لازم را در انتهای بسته شدن قالب و دقیقا قبل از </body>قرار دهید. بهتر است کدهای جاوا اسکریپتی مانند شمارنده یا کدهای گوگل آنالیتیکز را هم در پایان قرار دهید .برای اطلاعات بیشتر در مورد گوگل آنالیتیکز می توانید در دوره مبانی گوگل آنالیتیکز درسنامه شرکت کنید.

زیرا دستورات CSS برای پیکربندی و لود صحیح صفحه لازم هستند و باید در ابتدا قرار گیرند. اما دستورات جاوا اسکریپت معمولا پردازش سنگینی را لازم دارند و در مواردی هم باید برخی اطلاعات را از سایت های دیگر دریافت کنند. که این پردازش و دریافت اطلاعات می تواند تا حد زیادی باعث کند شدن وبلاگ شما شود و حتی در مواردی عدم دریافت اطلاعات از سایت بیرونی، باعث لود ناقص و یا توقف بارگذاری صفحه در میانه کار می شود.

اگر هم دستورات جاوا اسکریپت به گونه ای هستند که برای نمایش صحیح وبلاگ شما ضروری اند و باید در ابتدای کار لود شوند، بهتر است با استفاده از راه هایی مانند دستورdefer ، کار آنها را به بعد از لود کامل CSS موکول کنید.

کاهش کدهای PHP دینامیک و فراخوانیhttp

دلیل این کار که کاملا مشخص است و تنها با ذکر مثالی به توضیح آن می پردازیم:

اگر می خواهید سایتی با آدرس مشخص و یا بخشی از اطلاعات سیستم مدیریت محتوا را برای استفاده استاتیک فراخوانی کنید، دستور PHP آن را هم به صورت استاتیک بنویسید.

یعنی مثلا در کد زیر:

```
<?php bloginfo('home'); ?>
```

بهتر است به جای عبارت home برای فراخوانی آدرس از دیتابیس، مستقیما آدرس سایت تان را وارد کنید، مانند : http://www.darsnameh.com

یا اینکه در مثال زیر:

```
<?php bloginfo('name'); ?>
```

برای افزایش سرعت، بهتر است که به جای فراخوانی نام وبلاگ از دیتابیس، مستقیما نام وبلاگ تان را به جای عبارت nameوارد نمایید.

همچنین کدهای HTML را کنترل کنید تا هرگونه آدرس دهی داخلی مانند فایل هایCSS ، جاوا اسکریپت یا لوگو نیز آدرس استاتیک داشته باشند.

بهینه سازی (Optimize) دیتابیس وبلاگ

بهینه سازی دیتابیس به کامپیوتر سرور کمک می کند تا با سرعت بهتری به درخواست های ارسالی از طرف مرورگرها پاسخ دهد. ساده ترین روش برای چنین بهینه سازی، این است که در phpMyAdmin لاگین کرده و سپس تمامی جداول یا تیبل ها را انتخاب کنید. حال با انتخاب گزینهOptimize table ، کار بهینه سازی را بر روی جداول انجام دهید.

البته راه دیگر و بهتر انجام این کار استفاده از پلاگین هایی همچون WP-DBManagerو Optimize DBاست. حتی برخی از متخصصان عقیده دارند که با استفاده از چنین پلاگین هایی، بهینه سازی دیتابیس باید به صورت روزانه انجام گیرد.

و در پایان اگر به دنبال اطلاعات کامل و تخصصی تری در خصوص بهینه سازی وردپرس یا WordPress Optimizationهستید، این لیست سایت وردپرس می تواند شروع خوبی باشد.

امیدواریم با گذراندن این دوره، وبلاگ نویسی امن تر و سریع تری داشته باشید. برایتان آرزوی موفقیت داریم.

منابع:

درسنامه(https://darsnameh.com)

سلام برنامه(http://hiprogram.ir)

بهار 96-97