چگونه وبلاگ هک می شود، آشنایی با روند هک وبلاگ و روشهای تقویت امنیت مدیریت وبلاگ

دوستان عزیز شاید از برخی شنیده باشید که فلان وبلاگ هک شده است ،در اصل سرویس ارایه دهنده وبلاگهای رایگان رایج مانند میهن بلاگ ، بلاگفا ، پرشین و پارسی بلاگ دارای امنیت فوق العاده هستند پس چگونه یک وبلاگ هک می شود!!! جواب ساده است ایمیل مدیروبلاگ هک می شود!!! به سادگی و با استفاده از نرم افزارها و با ترفندهای مختلف هکر ، پسورد یا کلمه عبور پست الکترونیکی مدیر وبلاگ را می یابد !! وارد ایمیل شما شده و با ترفنددیگر و با بهره گیری از سرویس فراموشی رمز عبور و به جای مدیروبلاگ درخواست رمز وبلاگ قربانی می کند خوب!!! برای پست الکترونکی تصرف شده رمز عبور فرستاده می شود واز این پس هکر با رمز عبور وبلاگتان وارد وبلاگ شده و آن را فتح می کند به همین سادگی !! پس سوال این است چگونه وبلاگمان هک نشود!! جواب امنیت وحفاظت از ایمیل مربوط به وبلاگ و جواب به این سوال را در ادامه از زبان مدیر پشتیبان سایت مهین بلاگ و از وبلاگ مدیر میهن بلاگ مرور می کنیم :

توضیح:

هک : به عملی گفته می شود که با دست یابی به مدیریت وب سایت یا وبلاگ از روشهای مرسوم ، هکر مدیریت وراهبری وب سایت یا وبلاگ را در دست می گیرد.

هکر : به فردی که عمل هک انجام می دهد هکر گویند. هکرها انواع مختلف دارند که در مجموع برای به رخ کشیدن سواد فن آوری اطلاعات خود وهمچنین اعلان ضعف امنیت مدیر وبلاگ یا وب سایت و حتی اخاذی و دزدی به هک دست می زنند!!!

قربانی : وبلاگ یا وب سایت یا ایمیلی که مورد حمله موفق آمیز هکر قرار می گیرد.

کرک رمز عبور : در این نوع هک ، هکر به رمز عبور مدیریت وب سایت یا وبلاگ قربانی دست پیدا نموده و با استفاده از رمز عبور و پسورد و تغییر آن عملا اختیارات را از مدیروبلاگ قربانی موقت یا دایم سلب می کند در این گفتار منظورمان کرک پسورد و رمز عبور است.

آشنایی با نرم افزار کرک رمز عبور!!!

کی لوگرها:

نرم افزارهایی هستند که کلیه کلید های کی بورد که توسط شما فشار داده می شوند را ذخیره نموده و در اختیار هکرها قرار می دهند این نرم افزار که به نرم افزارهای جاسوسی نیز مشهور هستند می توانند کلیه نام ها کاربری و رمزهای عبور شما را بی انکه شما متوجه باشید از طریق ایمیل و یا راه های دیگر در اختیار افراد دیگر قرار دهند.

تروجان ها:

این نرم افزار ها می توانند کنترل سیستم شخصی شما را در اختیار هکرها قرار دهند به این معنی که وقتی شما به اینترنت وصل می شوید یک هکر می توانند به سیستم شما متصل شده و کنترل سیستم شما در اختیار بگیرد مثلا سیستم شما را خاموش کند - به فایل های شما دسترسی داشته باشد - نرم افزارهای شما را اجرا کند و...

با توجه به توضیحات فوق افراد عادی که اطلاعات چندانی راجع به مطالب فوق ندارند به راحتی طعمه هکرها شده و ممکن است کلیه اطلاعات شخصی آنها در اختیار دیگران قرار بگیرد!

آلودگی سیستم قربانی

اولین سئوالی که پیش می آید این است که این افراد چطور این نرم افزارها را بر روی کامپیوتر شما نصب می کنند؟ جواب ساده است ، از ضعف مدیریت امنیت مدیر وبلاگ سو استفاده می کنند!!!

خودتان را آلوده می کنید!!!

- بیشتر اوقات خود شما هستید که با دست خودتان سیستم خود را آلوده می نمایید!شاید برای شما هم پیش آمده که فردی فایلی را برای شما از طریق ایمیل یا یاهو ارسال نماید!آنچه مشخص است این است که برخی از هکرها با تکنیک های خاصی اقدام به این کار می نمایند.

ممکن است فردی با یک ایدی که در ظاهر یک آیدی دخترانه باشد با شما ارتباط برقرار نماید و پس از اینکه شما را شیفته خود نمود از شما بخواهد که عکس وی را مشاهده نمایید و یا حتی خود شما از او این در خواست را بنمایید.

اینجاست که این آقای هکر ممکن است یک نرم افزار تروجان و یا کی لوگر را برای شما ارسال نمایید و شما هم که مشتاقانه در انتظار دیدن تصویر معشوق مجازی خود هستید!!!! فریب هکر را بخورید و بی اعتنا به مشخصات فایل روی آن کلیک کرده و ایمیل شخصی - آیدی یا هو - وبلاگ و ... خود را از دست بدهید!

گاهی اوقات این فایل های به اصطلاح ویروسی ممکن است از طریق ایمیل برای شما ارسال شود.

مثلا یک هکر که ایمیل یکی از دوستان شما را جعل نموده از شما بخواهد عکس های ..... که برای شما ارسال کرده است را مشاهده کنید!

این راه هم یکی از راه های معروف برای انتشار ویروس ها نیز می باشد پس از این به بعد حسابی دقت کنید

دیگران شما را آلوده می کنند!!!

ممکن است که از دوستان و آشنایان که به کامپیوتر شخصی شما دسترسی دارند مستقیما این نرم افزارهای ناخوانده را بر روی سیستم شما نصب نمایند- تا حد امکان سعی کنید یک نام کاربری و رمز عبور خاص برای خودتان بر روی ویندوز داشته باشید و هرگاه می خواهید کامپیوتر خود را در اختیار فرد دیگری قرار دهید از یک نام کاربری و رمز عبور دیگر برای ورود به محیط ویندوز استفاده کنید و در حد امکان سعی کنید که این نام کاربری به عنوان یک limited Account تنظیم شده باشد.

سی دی های آلوده کننده می شوند!!!

دیسکت ها و سی دی های آلوده یک راه دیگر برای آلوده شدن سیستمتان به تروجان، کرمها و دیگر نرم افزار جاسوس افزار هستند، با توجه به تجربیات قبلی بنده برای هک کردن ، این راه هم راه مناسبی برای انتقال و اجرای نرم افزار ها بر روی کامپیوتر اشخاص است ممکن است دوست شما سی دی را مستقیما در اختیار شما قرار دهد و یا اینکه از شما بخواهد چیزی بر روی آن رایت نمایید.
اینگونه سی دی به محض اینکه داخل درایو قرار داده شدند به صورت Auto Run نرم افزار مشخص شده را اجرا می نمایند و کامپیوتر شما را آلوده می سازند ! اتوران به معنی اجرا خودکار است بدین معنی که به محض گذاشتن سی دی در سی دی رام برنامه اجرا می شود مانند بسیاری سی دی های آموزشی ، نرم افزاری و ... که از این خصیصه کاربری تبعیت می کنند.

کافی نت ها محل های عمومی و آلوده !!!

کافی نت ها و مراکز اینترنت عمومی مثل مراکز اینترنت دانشگاه ها نیز محل بسیار خوبی برای نصب کردن نرم افزار های هک می باشد. به خصوص اگر مدیران این مراکز در زمینه این گونه نرم افزار ها اطلاعات کافی نداشته باشند. در صورت امکان به هیچ وجه از کافی نت ها برای وارد شدن به ایمیل شخصی ، کنترل پنل وبلاگ و یا یاهو مسنجر استفاده ننمایید!

سایتهای غیرمعتبر و در به در

سایت های مشکوک هم منبع آلودگی سیستم شما خواهند بود، برخی از افراد با مطلع بودن از نواقص و باگ های مرورگر ها اقدام به راه اندازی سایت هایی می کنند که ممکن است با ورود به این سایت ها نرم افزارهای آلوده به صورت خودکار بر روی سیستم شما نصب شوند.

نرم افزارهای غیرمعتبرو قلابی پاکستانی !!!

نرم افزارهای مشکوک و البته آلوده بیشتر هیجان انگیزند مثلا نرم افزارهایی برای هک سایت در یک ثانیه !! یا نرم افزار دانلود یا نرم افزاری برای ساخت اکانت و کارت اینترنت بی نهایت !!! و از این جور تبلیغات که نرم افزارهایی البته آلوده کننده وگاهی خطرناک خواهند بود، ممکن است به سایتی وارد شوید که نرم افزار خاصی را برای دانلود قرار داده و کلی از آن تعریف نموده تا زمانی که به اعتبار سایت و صحت نرم افزار اطمینان نیافته اید اینگونه نرم افزارها را دانلود و نصب ننمایید.

راه مقابله با آلودگی

در پایان یکی از راهای بسیار خوب برای مبارزه با روش های فوق استفاده از نرم افزارهای آنتی ویروس و فایروال می باشد.
اما باید توجه داشته باشید برای اینکه این نرم افزار بتوانند تا حد زیادی مفید واقع شوند باید هر از مدتی از طریق اینترنت آنها را به روز نمایید.
چنانچه فکر می کنید که قبلا سیستم شما توسط اینگونه نرم افزارها آلوده شده است بهترین راه فرمت کردن کل سیستم و نصب مجدد ویندوز است!

آلودگی با روش مهندسی اجتماعی

یکی دیگر از روش های مرسوم برای هک کردن که بیشتر افراد باهوش از آن استفاده می کنند استفده از روش مهندسی اجتماعی و یا حقه بازی می باشد.
در این روش ممکن است فردی خود را مدیر بلاگفا معرفی نماید و با ارسال ایمیل یا ارتباط از طریق آیدی یاهو از شما بخواهد که رمز عبور خود را برای او ارسال کنید.
شاید هم از شما بخواهد بر روی یک لینک کلیک کرده و مثلا برای فعال کردن وبلاگ خود و یا ... رمز عبور خود را وارد.
در مورد فوق مواظب صفحات جعلی باشید هیچ گاه از طریق هیچ لینکی وارد سایت بلاگفا نشوید و همیشه برای ورود به کنترل پنل مستقیما به سایت بلاگفا مراجعه نموده و آنجا نام کاربری و رمز عبور خود را وارد نمایید.
همچنین به هیچ وجه به ایمیل هایی که ممکن است از طرف سایت بلاگفا ارسال شوند و از شما درخواست رمز عبور و یا هر مورد دیگری که نیاز به وارد نمودن رمز عبور داشته باشد اعتنا ننمایید.

ممکن است فرد هکر ایمیل شما را هک نموده سپس از طریق لینک فراموشی رمز عبور وبلاگ شما را هک کند و پس تا حد از طریق روش های فوق مراقب ایمیل خود نیز باشید.

رمز عبور مناسب رمز عبور پیچیده است !!!

رمز عبور خود را تا حد امکان پیچده و ترکیبی از حروف و اعداد قرار دهید و در انتهای انها نیز چند Space یا همان فاصله قرار دهید. تا حد امکان طوری رمز عبور انتخاب کنید که نزدیک ترین دوستان شما هم نتواند ان را حدث بزنند و برای سایت های مختلف رمز های متفاوت انتخاب کنید به شرطی که آنها را فراموش نکنید

کلیه روش های فوق روش های متعارف می باشد پس حالا که برخی از این روشها آشنا شدید سعی کنید دست هکرها را بخوانید و در صورت مواجه شدن با روش های جدید آمادگی لازم را داشته باشید.

به زودی نیز سعی خواهدشد تعدادی از نرم افزارهای امنیتی مورد تایید در اختیار کاربران قرار گیرد تا برخی از مشکلات امنیتی آنها را حل نماید