کلمه عبور پیچیده

با گره خوردن زندگی امروز افراد با فضای مجازی و زندگی دیجیتال، اطلاعات فردی و ابزارهای ارتباط مالی از اهمیت ویژه برخوردار است و بی‌احتیاطی در این موارد می‌تواند صدمات جبران ناپذیری مانند از بین رفتن همیشگی اطلاعات یا ضررهای هنگفت مادی و معنوی را به همراه داشته باشد، بنابراین رعایت اصول اولیه امنیت اطلاعات در مقابل افردی که قصد نفوذ و آسیب رساندن و سو استفاده از این اطلاعات را دارند ، از ضروریات اولیه استفاده از این فضا می باشد.

نیاز به داشتن یک رمز عبور امن و غیر قابل حدس(Password Complexity)

افراد برای انجام هر کاری یا استفاده از هر نوع خدماتی ابتدا باید توسط سیستم مشخصی احراز هویت (Authentication) شوند و معمولا هر احراز هویت نیاز به دو عنصر دارد، نام کاربری و رمز عبور (Username & Password).

بنابراین رمزهای عبور حساب های کاربری، ایمیل ها و کارت های اعتباری و ... ، اولین و مهمترین سد دفاعی در برابر هکرها و یا هر عامل یا فردی که قصد نفوذ و آسیب رساندن و سوء استفاده از اطلاعات افراد را داشته باشد، هستند در نتیجه برای جلوگیری از این امر به کلمه عبور امن و غیر قابل حدس نیاز است اما سوالی که مطرح می شود اینست که چگونه یک کلمه عبور امن ایجاد نمود و در گام بعدی برای نگهداری آن چه اقداماتی باید انجام داد.

ویژگی های یک رمز عبور مطمئن ومناسب

رمزهای عبور ساده که از ترتیب حروف و یا اعداد مانندabc123 ، qwerty یا ۱۲۳۴۵۶ مورد استفاده کاربران قرار می گیرند جزء اولین گزینه هایی هستند که هکر ها نسبت به آزمایش آنها اقدام می کنند. بنابراین برای ساختن یک رمز عبور مطمئن و مناسب بهتر است که بدانیم یک کلمه عبور امن چه مشخصاتی دارد و چگونه باید ساخته و نگهداری شود:

برای ساختن یک رمز عبور مناسب، تکنیک‌های متفاوتی وجود دارد. با یک جست‌وجوی ساده در اینترنت، می‌توانید با بیشتر این روش‌ها آشنا شوید، اما به طور کلی کارشناسان مسائل امنیتی همواره تاکید می‌کنند یک رمز عبور مناسب باید ترکیبی از حرف کوچک، بزرگ، اعداد و علایم باشد.

البته شما می‌توانید روش خاص خود را هم داشته باشید، اما بد نیست که با برخی از روش‌های رمزگذاری معمول نیز آشنا شوید:

استفاده از ! به جای i یا @ به جای a (فقط به یاد داشته باشید که این کار را به صورت تصادفی انجام دهید و به‌عنوان یک قانون کلی استفاده نکنید). استفاده یکی در میان از کلید شیفت؛ مثلا رمزی مانند behnam را می‌توانید به شکل BeHnAm به کار برید.تایپ کردن با قراردادن انگشتان در خانه‌های اشتباه: در این روش کلمه یا جمله مورد نظر خود را انتخاب و آن را به خاطر بسپارید اما در هنگام تایپ حروف ردیف بالایی یا پایینی را جایگزین کلمه یا جمله مورد نظر خود کنید.به عنوان مثال کلمه behnam با جایگزینی حروف ردیف بالایی همین کلمه تبدیل می‌شود به کلمه نامفهومg3hqj ، البته همانطور که گفته شد سعی کنید در بین حروف از اعداد نامنظم مانند ۶،۸،۲،۵،۰ یا کاراکترهایی همچون@ ،&،*، $هم استفاده کنید.

یک روش دیگر انتخاب رمز عبور این است که کلمه یا جمله‌ای فارسی را به عنوان رمز عبور در نظر گرفته به جای حروف فارسی از حروف انگلیسی‌ای که روی آن حروف فارسی قرار گرفته است استفاده کنید. به‌عنوان مثال کلمه عبور «بهنام» در این روش" fikhm " می‌شود.

حال که با برخی شیوه ها و روش‌های رمزگذاری آشنا شدید، بهتر است با مشخصات یک رمز عبور مناسب نیز آشنایی داشته باشید:

- حتی الامکان دارای اطلاعات شخصی کاربر، مانند سال تولد، نام و... نباشد.
- طول کلمه عبور حداقل بیش از ۸ کاراکتر تشکیل شود.
- شامل کلمات رایج و موجود در فرهنگ لغت نباشد.
- ترکیبی از کاراکتر های متنوع، مانند حروف کوچک و بزرگ، اعداد، کاراکتر های خاص(& ، $، #، @، ^، %)و... باشد.
- از یک کلمه عبور برای سایت های مختلف استفاده نکنید چون در صورت لو رفتن یک کلمه عبور باقی اکانت های شما نیز به خطر خواهد افتاد.

از نکات فوق اینگونه می توان دریافت که معمولاً قدرت یک رمز عبور به عنوان تابعی از میزان پیچیدگی یا تصادفی بودن کاراکترهای آن محسوب می شود، یعنی اینگونه تصور می شود که هر قدر از نمادها ، اعداد و حروف بزرگ و کوچک بیشتری به صورت تصادفی استفاده کنید، ضریب امنیت پسورد بالاتر خواهد رفت ولی به یک نکته مهم دیگر هم باید توجه ویژه داشت که زمان هک شدن یک کلمه عبور رابطه نمایی (توانی) با تعداد کاراکترهای آن دارد، بنابراین تنها مقدار کمی افزایش در طول پسورد می تواند مدت زمان مورد نیاز برای هک کردن را به شدت افزایش دهد.(با توجه به جدول شماره ۱)

جدول شماره ۱

روش تست میزان امنیت رمز عبور

پس از ساختن رمز عبور، می توانید میزان امنیت آن را مورد آزمایش قرار دهید و قدرت آن را بسنجید. برای انجام این کار سامانه ها و سایت های بسیاری وجود دارند. به عنوان مثال، در گوگل عبارت " تست پسورد" را می توانید جستجو کنید."www.passwordmeter.com " توجه داشته باشید که ممکن است نتایج سایت های مختلف متفاوت باشند. یعنی، امکان دارد یک پسورد در سایتی، ضعیف تشخیص داده شود ولی در سایت دیگر متوسط یا قوی اعلام گردد. خلاصه اینکه اگر طول پسورد را به ۸ کاراکتر یا بیشتر برسانید و همینطور از کاراکترهای متنوع و خاص استفاده کنید، کلمه عبور شما قوی تر می شود. در نتیجه، حدس زدن آن توسط هکرها سامانه های نفوذ به سختی قابل انجام خواهد بود. ضمن اینکه سعی کنید هر چند وقت کلمه عبور حساب خودتان را تعویض کرده و به خاطر بسپارید.