آموزش انتخاب پسورد قوی و جلوگیری از هک شدن آن!

انتخاب یک پسورد خوب توی دنیای مجازی بسیار بسیار مهم و حیاتی است . همان طور که در دنیای واقعی هیچ گاه درهای ماشینمون رو باز نمیذاریم ، توی دنیای مجازی هم برای *حفاظت از اطلاعات محرمانه* و شخصی خودمون از پسورد استفاده میکنیم . مشکلی که منو وادار کرد تا این مطلبو بنویسم اینه که متاسفانه خیلی از عزیزانی که از اینترنت استفاده میکنند این موضوع رو اصلاً توجهی بهش ندارند . خود **انتخاب یک پسورد خوب** و قابل اطمینان یک مهندسی لازم داره و عواملی در اون دخیل هستند . عدم رعایت این نکات و هک شدن پسورد زیان های جبران ناپذیری رو به شخص وارد میکنه و حتی زندگی وی رو تا مرز نابودی ممکنه بکشونه)اگه طرف یه شخصیت معروف باشه که دیگه خدا به خیر بگذرونه! (

درای ماشینمونو باز نمیذاریم چون دوست نداریم هر کسی بیاد داخل ماشینمون ، داشبوردشو باز کنه ، توی جاهای مختلفش سرک بکشه و ... توی دنیای مجازی هم دوست نداریم این اتفاقات برای حساب های بانکی ، ایمیل هامون ، حساب کاربری سایت دانشگاه و ... بیفته ! نگرانی ما از جایی بیشتر میشه که بدونیم اکثر مردم دنیا (توجه کنید نگفتم ایران ، گفتم دنیا !) از اهمیت انتخاب یک پسورد خوب بی اطلاع هستند و خودشون رو در معرض خطرهای بسیاری قرار میدن . آکادمی لرن فایلز میخواد شما رو قدم به قدم برای انتخاب یک پسورد قوی ، قابل اطمینان و ماندگار کمک کنه پس با ما باشید.

یک شرکت خاص توی این زمینه **SplashData**است که بیشترین پسوردهایی که مردم دنیا از سال ۲۰۱۱ تا ۲۰۱۵ استفاده میکردند رو جمع آوری کرده ، نتیجه ی این گزارش فاجعه است!

2011	2012	2013	2014	2015
password	password	123456	123456	123456
123456	123456	password	password	password
12345678	12345678	12345678	12345	12345678
qwerty	abc123	qwerty	12345678	qwerty
abc123	qwerty	abc123	qwerty	12345
monkey	monkey	123456789	123456789	123456789
1234567	letmein	11111	1234	football
letmein	dragon	1234567	baseball	1234
trustno1	111111	iloveyou	dragon	1234567
dragon	baseball	adobe123	football	baseball

همون طور که داریم میبینیم پسوردهای "۱۲۳۴۵۶" و "password" بیش ترین استفاده رو داشتند !چیزی که مشخصه اینه که این پسوردها ناشی از تنبلی افراد هستند و اکثراً کاراکترهای کنار همِ کیبرد رو تشکیل میدن ! از اون بدتر اینه که با گذشت زمان تغییر چندانی توی این لیست شاهد نیستیم و این بیراهه از سال ۲۰۱۱ تا ۲۰۱۵ خیلی ها رو داره به سمت خودش میکشونه . خب با این آمار و ارقامی که دیدیم با هم اگه شما هم بخواید به حساب یک نفر حمله کنید (هکش کنید) هیچ نیازی ندارید که از ابزار خاصی استفاده کنید و با کنار هم قرار دادم این حروف و ارقام ساده به راحتی رمز عبور طعمه تون رو پیدا خواهید کرد!

شاید الآن با خودت این فکرو بکنی که "مگه میشه آدم برای اطلاعات مهمش همچین پسوردای ضعیفی قرار بده ؟" یا اینکه بگی "پسوردای من که به این سادگیا نیستن !" بسیار عالی ... بیاید قبل از اینکه به پسوردای خودمون ببالیم ببینیم یک پسورد قابل اطمینان باید از چه عواملی پیروی کنه و بعد نتیجه گیری کنیم.

انتخاب یک پسورد قابل اطمینان و قوی قوانین پیچیده ای نداره و با گذشت زمان هم تغیرات چندانی نکردند ؛ با این حال عده ی کمی توی دنیا هستند که به طور صحیح از این قوانین پیروی میکنند و از اهمیت اون با اطلاع هستند . برای این امر باید چند عامل رو درنظر بگیریم.

عوامل مهم جهت انتخاب یک پسورد قوی:

طول پسورد : پسوردهای قوی طولانی هستند ! یک قانون کلی وجود داره که میگه هر چقدر پسورد انتخابی شما طولانی تر باشه ، احتمال کرک شدن اون کمتر خواهد بود ! دلیلشم اینه که اکثر نرم افزارهایی که توی این زمینه قرار دارند از روش دیکشنری (Dictionary Method)استفاده میکنند (یعنی طبق یک الگوریتم کلمات بیشتر استفاده شده توسط مردم رو همین جور تست میکنند تا پسورد رو پیدا کنند) و حدس زدن چنین عباراتی بسیار مشکل خواهد بود . همیشه سعی کنید عبارات طولانی از پسوردتون بسازید ؛ حتی اگر دارید عضو سایتی میشید که از شما میخواد طول پسوردتون حداقل ۶ کاراکتر باشه ، تنبلی نکنید و عبارات طولانی تری بسازید.

میزان پیچیدگی : یه قانون دیگه رفقا ! یادتون باشه از کلمات ساده استفاده نکنید ! نام مکان ها ، اسم اشخاص ، اسم حیوان خانگی شما ، اسم مدرسه تون ، رنگ مورد علاقتون ، اسم گروه موسیقی که عاشقش هستید ، اسم شهرتون ، تاریخ تولد و از این دست اسم ها رو کلاً بریزید دور و یه فاتحه هم براشون بخونید ! برای پیچیده کردن پسوردتون میتونید از موارد بالا یک ترکیب بامعنی بسازید مثلاً از کلمات Cat، Shoe، Redمیتونید عبارت پیچیده ی MyCat$Shoe!sRed رو بسازید) . ترکیب بامعنی که گفتم نه که حالا خیلی ادبی و فرهنگی باشه ، منظور چیزی هست که توی خاطرتون بمونه و هماهنگی داشته باشه(.

منحصر به فردی پسورد : **این یکی واقعاً با اهمیت تر از بقیه است** !دوستان عزیز مهم تر از داشتنِ یک پسورد خوب اینه که شما برای هر سایت پسورد منحصر به فردی داشته باشید و با هم فرق کنند . متاسفانه خیلی ها این طوری هستند که پسورد ایمیل و رمز عابر بانک و پسورد هر سایتی که توش عضو هستن یکی هست و دلیلشون هم اینه که برای چی پسورد جدا بذارم تا یادم بره ! به این میگن عذر بدتر از گناه ! دلیل میخوای چرا این کار خیلی زشتِ و بد ؟ ببین عزیزم شما ممکنه بهترین پسورد دنیا رو هم داشته باشی ، جوری که سوپر کامپیوترها هم بخوان بفهمن چیه اون پسورد سال ها درگیرش باشن و با این منطق میای و هر جا که رسیدی و پسورد ازت خواستن اونو میدی ! اگر خدای نکرده کل سیستمای یکی از اون جاهایی که این پسوردو گذاشتی به خطر بیفته و هکر ها متوجه اون پسورد بشن دیگه عملاً و رسماً و شرعاً کارت تمومه چون حالا اونا دسترسی به همه چیز شما دارند ! خطرش اینه که شما ایمیلتو دادی ، پسوردتم که میدونن چیه و رسماً زحمت کشیدی و کلید خونه رو دادی به جناب هکر ، صبحانه و ناهار و شام هم براش گذاشتی و تمام!

خب رفقا ، عامل دیگه ای نیست که بخوایم مرور کنیم . پس شد یک پسورد ***طولانی و پیچیده و منحصر به فرد*** که بهش برچسب قابل اطمینان زدیم!

حالا شاید بپرسی از خودت که مگه میشه آدم این همه سایت عضو باشه و برای هر کدوم این قانونا رو بخواد رعایت کنه و توی ذهنشم بمونه ؟ سوال شما کاملاً درست و منطقی ئه ، یک پاسخ منطقی هم برای این سوال وجود داره : استفاده از یک برنامه مدیریت پسورد!

چطور ما برای مدیریت دانلودهامون از برنامه استفاده میکنیم ، برای اینکه هم بهتر بتونیم مدیریت کنیم دانلودهامونُ ، هم طبقه بندی کنیم فایل های دریافتی رو و دلایل مثبت دیگه ! پس برای این امر ضروری دنیای مجازی هم باید از یک برنامه مدیریت پسورد خوب استفاده کنیم . استفاده از برنامه ای مثل **برنامه LastPass** به شما تضمین میده تا از پسوردهای طولانی ، پیچیده و منحصر به فرد به هر تعداد استفاده کنید و به راحتی اونا رو مدیریت و پیگیری کنید . در واقع کار این برنامه ها این طوری ئه که شما رو همیشه و همه جا همراهی میکنند و حتی قابلیت این رو دارند که با تلفن هوشمند شما Sync بشن و هر جا که رفتید و نیاز به پسورد داشتید ، زحمت اون رو میکشن و لازم نیست شما انگشتان مبارک رو حتی روی یک کلید هم ببرید و شما رو به طور خودکار وارد یا اصطلاحاً loginمیکنند ؛ این کار بسیار راحت ، امن و به نظر من شیکِ!

برای سرویس ها و سایت هایی با اطلاعات شخصی مهم مثل بانک ها بسیار اهمیت داره که از روش های تامین امنیت چند لایه استفاده کنند . فناوری که چند سالی است داره استفاده میشه به احراز هویت دو-عاملِ یا Two-factor authentication معروفه . یعنی شما برای ورود علاوه بر پسورد باید کد ۶ رقمی که به شماره تلفن همراهتون ارسال میشه رو هم بزنید تا وارد بشید که توی اکثر برنامه های چت و گفتگو ، سرویس های ایمیل و بانک مورد استفاده قرار گرفته و بسیار برای ایجاد امنیت برای کابران راه حل مناسب و مفیدیه.

خب حالا وقتش رسیده تا بریم برای نتیجه گیری:

.شیوه های انتخاب پسورد پر زرق و برق نیستند اما فریب نخورید ، رعایت اونا فوق العاده لازم هستند.

.یک پسورد خوب باید طولانی ، پیچیده و منحصر به فرد باشه . پسوردی که برای ایمیلتون وارد میکنید نباید با پسوردی که برای عضویت در یک سایت استفاده میکنید یکی باشه.

.استفاده از یک برنامه مدیریت پسورد مثل LastPass ، Dashlaneو ... امروزه برای مدیریت سه عامل بالا (طولانی ، پیچیده و منحصر به فرد) برای هر فرد ضروری و لازم میباشد . یادتون باشه ، اطلاعات محرمانه شما بسیار با ارزش هستند و نباید دست هر کسی بیفتند ! تنبلی » ممنوع!

تهیه و تنظیم : بلاگ ترادف