راهنمای انتخاب کلمات رمز

دانشگاه فردوسی مشهد

مرکز فناوری اطلاعات و ارتباطات دانشگاه

پاییز ۱۳۹۸

اکانت‌های بسیاری از کاربران فضای دیجیتال به دلیل بی‌دقتی در انتخاب رمز عبور بعد از مدتی توسط هکران از دسترس خارج می‌شود و بدین شکل اطلاعات شخصی افراد مورد سوء استفاده قرار می‌گیرد. داشتن یک رمزعبور مطمئن، احتمال هک شدن و لو رفتن اطلاعات را در فضای مجازی کاهش می دهد .

رمزعبور ضعیف چیست؟

یک رمز عبور ضعیف رمزی است که به راحتی توسط دیگران(فرد، کامپیوتر یا شبکه‌ای از کامپیوترها) قابل حدس‌زدن باشد. نمونه‌ای از این حملات و یا دسترسی ها بصورت زیر است:

۱. **حمله Brute-force:** امتحان‌کردن همه ترکیبات ممکن با کاراکتر و اعداد مختلف به فرم کلمه.
۲. **حمله Dictionary-Attack:** استفاده از رمزهای رایج مانند password۱۲۳ یا ۱۲۳۴۵۶.
۳. **حمله فیشینگ** :فیشینگ به معنی فریب کاربر برای فاش‌کردن اطلاعات مهم خود است. این فریب‌ها اغلب در صفحات ایمیل یا صفحات سرویس‌های مشهور قرار دارد که در هنگام لاگین‌کردن، اطلاعات خود را وارد می‌کنید. در این صفحات، کاربر با کمال میل رمز خود را به شخص اشتباه می‌سپرد. برای اجتناب از این نوع فریب، برروی لینک‌های مشکوکی که از شما اطلاعات حسابتان را می‌خواهند کلیک نکنید.
۴. **استفاده از کی‌لاگر:** هکرها می‌توانند بدون اطلاع شما روی دستگاهتان کی‌لاگر نصب کنند. برای مثال یک هکر می‌تواند با روش فیشینگ برای شما ایمیلی ارسال کند، به محض اینکه ضمیمه ایمیل را باز کنید و یا روی لینک آن ایمیل کلیک کنید، یک فایل جاوا اسکریپت روی مرورگر شما دانلود و نصب می‌شود. بدون اینکه متوجه شوید، هر چیزی که در مرورگر تایپ کنید از جمله آدرس وب‌سایت، نام کاربری، رمزعبور و غیره برای هکر فرستاده می‌شود.
۵. **از طریق مشاهده**: مشاهده کردن و زیر نظر گرفتن محیط و اطرافیان یکی دیگر از روش‌های هکرها برای بدست آوردن اطلاعات است. هکر می‌توانند به آرامی و زیرکی لپ‌تاپ یا موبایل شما را زیر نظر داشته باشند و اگر شما در این حین، وارد یکی از حساب‌های کاربری آنلاین شوید، آنها نام کاربری و رمزعبورتان را می‌بینند. عده‌ای عادت دارند رمزعبور سیستم یا ایمیل خود را روی کاغذی نوشته و روی میزکارشان بچسبانند، و هکرها فقط با نگاه کردن به میز کار یا میز شخصی بقیه، می‌توانند اطلاعات زیادی بدست آورند.
۶. **مهندسی اجتماعی**: مهندسی اجتماعی، هنر فریب دادن عوامل انسانی، جهت دسترسی به اطلاعات محرمانه‌ی آنها و از بین بردن آنها است. اطلاعاتی که این مجرمان به جستجوی آن می‌پردازند، متفاوت

است. اما زمانیکه، افراد را مورد هدف قرار می‌دهند، مجرمان تلاش می‌کنند تا آنها را فریب دهند، تا رمز عبور و یا اطلاعات بانکی آنها را دریافت کنند و یا به رایانه‌ی آنها دسترسی پیدا کنند تا نرم افزار مخرب را بر روی سیستم آنها نصب کنند و سپس رایانه را تحت کنترل بگیرند .

ساختن یک رمزعبور امن

۱. مبنا قرار دادن یک جمله یا عبارت با طول حداقل ۸ کاراکتر و استفاده از کاراکترهای خاص
۲. عدم استفاده از الگوهای ساده و مشخص در کلمه عبور[۱].
۳. رمزها حداقل باید شامل سه نوع از چهار نوع کاراکترها، حروف بزرگ (ABC) و حروف کوچک (abc) و ارقام (۱۲۳) و نماد ها+=_ *$^@!&%#) ؟ – (باشند.
۴. کلمه عبور نباید شامل یک لغت خاص و یا معکوس آن یا کلمات معنا دار باشد.زیرا در این حالت از طریق حملات Brute-force و Dictionary Attack به راحتی و با صرف حداقل زمان قابل یافتن است.
۵. بهترین و ساده‌ترین پیشنهاد برای به خاطر سپردن رمز عبور، استفاده از space یا فاصله بین کاراکترهای رمز عبور می‌باشد. (به عنوان مثال کاربری که در به خاطر سپردن رمز عبور مشکل دارد، می‌تواند تاریخ تولد خود را به عنوان رمز با قرار دادن کاراکتری خاص بین تک تک اعداد تاریخ تولد، تنظیم کند. برای نمونه قرار دادن فاصله بین اعداد تاریخ تولد: ۱ ۰ ۱ ۴ ۶ ۳ ۱)
۶. استفاده از کاراکترهای جایگزین حروف در رمز عبور. به عنوان نمونه در اینجا چند نمونه از این جایگزین های جالب را به شما معرفی خواهیم کرد:

حرف مورد نظر در کلمه عبور	جایگزین حرف مورد نظر
a	@
B	&
H	#
i	!
O	.
X	%
t	+
S	$
D	)
K	|<

[۱]- در سایت های نظیر github.com لیست ساده ترین و رایج ترین رمزهای عبور مورد استفاده و قابل حدس آمده است.

به همین شکل میتوانید با خلاقیت های خود جایگزین های مناسبی برای حروف خود انتخاب کنید.

۷. به روزرسانی رمز عبور حداقل ۲ بار در سال. هیچگاه از رمزهای یکسان برای لاگین های مختلف استفاده نکنید.

در جدول زیر انواع کلمه عبورها و مدت زمانی که یک رایانه پیشرفته نیاز دارد تا یک کلمه عبور را حدس بزند نشان داده شده است.

طول / اجزا	حروف کوچک	+ حروف بزرگ	+ اعداد و سمبل ها
۶ کاراکتر	۱۰ دقیقه	۱۰ ساعت	۱۸ روز
۷ کاراکتر	۴ ساعت	۲۳ روز	۴ سال
۸ کاراکتر	۴ روز	۳ سال	۴۶۳ سال
۹ کاراکتر	۴ ماه	۱۷۸ سال	۴۴۵۳۰ سال

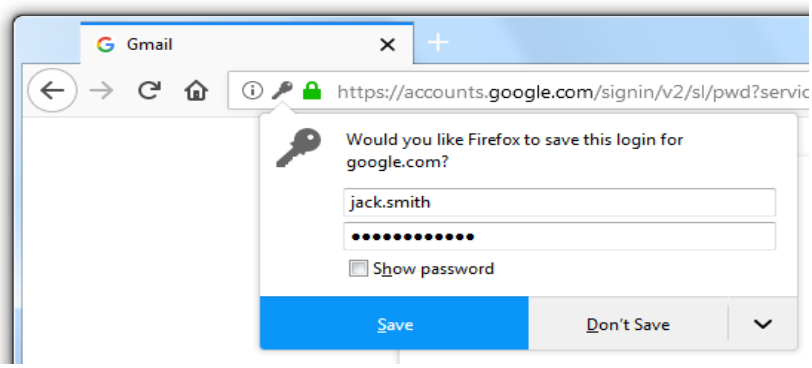
مشاهده می شود که هرچه طول کلمه عبور انتخابی بلندتر و ترکیب بین حروف کوچک، بزرگ، اعداد و نمادها، پیچیده‌تر باشد، امنیت کلمه عبور بیشتر خواهد بود.

رعایت نکاتی دیگر برای امنیت رمز عبور

برای داشتن یک **رمزعبور امن** نباید فقط به انتخاب کلمات پیچیده و دیگر مواردی که پیش از این گفتیم بسنده نمایید. بلکه رعایت نکاتی دیگر که در ادامه به آن ها اشاره خواهیم کرد هم می تواند به شما در اطمینان از هک نشدن و لو نرفتن رمز عبور کمک شایانی کند:

۱. اجتناب از ورود شناسه و رمز عبور در سایتهای غیر از https.
۲. عدم ارسال رمز عبور از طریق ایمیل.
۳. خروج از حساب کاربری پس از اتمام کار.
۴. عدم ذخیره شناسه و رمز عبور در مراکز مشترک مانند آزمایشگاهها و کافی‌نت ها.

در برخی مرورگرها مانند فایرفاکس و کروم، توسط password manager نام کاربری و رمزعبورهایی را که برای دسترسی به وب سایت ها استفاده می‌کنید، ذخیره می‌شوند و سپس در مراجعه بعدی به سایت، به طور خودکار، شناسه ورمز عبور در فیلدهای مربوطه پر می‌شوند.



چنانچه شما مطابق شکل بالا گزینه Save را انتخاب کنید، رمز عبور شما در مرورگر ذخیره خواهد شد. لطفا با جلوگیری از ذخیره رمز عبور در مرورگر از اطلاعات خود محافظت کنید.

چطور مطمئن شویم کلمه عبور به اندازه کافی امن است؟

پس از ایجاد رمز جهت تست آن، میتوانید با مراجعه به سایت هایی مانند سایت های زیر، میزان امنیت و قدرت رمزتان و نیز مدت زمانی که طول می کشد تا رمز عبور مربوطه، توسط نرم افزارها و حملات Brute-force هک شود، را مشاهده نمایید.

https://howsecureismypassword.net/
http://www.roboform.com/how-secure-is-my-password