

# چطور یک رمز عبور قوی انتخاب کنیم

## 1. مطمئن شوید طول رمز عبور شما کافی باشد

رمزی انتخاب کنید که به اندازه کافی طولانی باشد. کاراکتر بیشتر، حدس زدن رمز عبور شما را مشکل تر می کند. هیچ مقدار حداقلی وجود ندارد که همه با آن موافق باشند، اما بسیاری از سیستم ها هنگام ساختن رمز عبور حداقل هایی را درخواست می کنند تا شما را با یک رمز عبور چهار کاراکتری که به راحتی قابل حدس زدن است به پایان نبرید. مایکروسافت پیشنهاد می کند طول رمز عبور شما حداقل هشت کاراکتر باشد. اگر طول رمز عبور از این هم بیشتر شد، امنیت بالاتری را به همراه خواهد داشت.

## 2. ترکیبی از اعداد، علائم، حروف بزرگ و کوچک باشد

رمز عبور می بایست ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص (نمادها مانند \$, @, و...) باشد تا هک کردن رمز عبور شما سخت تر شود.

## 3. یک کلمه معنادار یا ترکیبی از چند کلمه معنادار نباشد

از به کار بردن کلمات معنی دار ساده و یا ترکیبی از چندتایی آنها مانند نام، نام شرکت و... در ساخت رمز عبور خودداری نمایید. استفاده از هر کلمه معناداری اشتباه است و ترکیب چندتایی آنها که یک عبارت ساده را هم بسازد، اشتباهی دیگر. برای مثال "house" یک رمز عبور بسیار ضعیف است و به راحتی هک می شود؛ در عین حال "red house" هم بسیار نامناسب است. یا مثلاً: abcd یا 123456789 که خیلی سریعتر هک می شود.

## 4. در رمز عبور، از اطلاعات عمومی استفاده نکنید

نام شما، تاریخ تولد، نام اعضای خانواده، نام همسر، شماره موبایل و غیره به صورت عمومی در دسترس هستند. اگر هکر یا فردی که قصد بدست آوردن رمز عبور را دارد، تا حدودی از اطلاعات شخصی شما باخبر باشد، به راحتی و با صرف زمان اندکی می تواند با ساختن عبارات مرتبط، رمز عبور تان را حدس بزند.

## 5. از یک ترکیب ساده به همراه کاراکترهای جایگزینی واضح استفاده نکنید

برخی کاراکترها را به دلیل شباهت ظاهری به یکدیگر می توان جابجا کرد. مثلاً 0 (عدد صفر) و O (حرف الفبای انگلیسی) به هم بسیار شبیه هستند و یا استفاده از @ به جای a. پس بهتر است در انتخاب رمز عبور، عبارتی هایی مثل "house" هم خودداری کنید. چون به راحتی توسط هکرها قابل تشخیص هستند.

## 6. از یک رمز عبور برای چند حساب استفاده نکنید

شما هرگز نباید از یک رمز عبور یکسان برای چند حساب کاربری استفاده کنید. چون اگر یک هکر به آن رمز عبور دسترسی پیدا کند به تمام پروفایل‌ها و حساب‌های کاربری مهم شما نیز دسترسی پیدا می‌کند. همچنین باید اطمینان پیدا کنید که هر رمز عبور با رمز عبور قبلی و رمز عبورهای موجود متفاوت باشد.

## 7. کلمات عبور پس از مدتی تغییر داده شوند

رمز عبورهای خود را در بازه‌های زمانی مشخص تغییر دهید. این کار سبب می‌شود که در صورتی که شخصی رمز عبور شما را یافته باشد، با تغییر رمز عبور مجدد توسط شما، دسترسی‌های آتی او به اکانت مربوطه سلب خواهد شد.

## 8. از یادداشت کردن کلمه عبور خودداری و ترجیحاً آن را در جایی امن نگهداری نمایید

از یادداشت کلمه‌های عبور بر روی فایل‌های کامپیوترتان و یا روی کاغذ جدا خودداری نمایید. زیرا در این حالت به راحتی قابل دست‌یابی است. چنانچه می‌خواهید رمز عبورهای خود را در جایی ذخیره نمایید، بهتر است از نرم افزارهای امن مربوط به این کار استفاده نمایید.

## 9. رمز عبوری انتخاب کنید که بتوانید به خاطر بسپارید

رمز عبور مستحکمی که اغلب فراموش می‌کنید به کار شما نمی‌آید.