

یک رمز عبور قوی به نگه‌داری امن تر اطلاعات شما کمک بسیار زیادی خواهد کرد. هنگامی که رمزهای عبور شما ضعیف باشند، خود را در معرض خطر قرار داده‌اید. یکی از آسان‌ترین مراحلی که می‌توانید برای جلوگیری از لو رفتن رمز عبورتان انجام دهید، این است که پسوردهای قوی‌تری ایجاد کنید.

۱ - از رمزهای عبور طولانی استفاده کنید

برای مدتی، رمزهای عبوری با طول ۶ تا ۸ کاراکتر کافی به نظر می‌رسید؛ اما حالا متخصصان توصیه می‌کنند که رمزهای عبوری به طول حداقل ۱۲ تا ۱۴ کاراکتر انتخاب کنیم تا بدین طریق اطمینان حاصل شود که رمز ما امنیت بیشتری دارد.

۲ - از رمزهای عبور آسان و قابل حدس زدن استفاده نکنید

رمزهای عبور ضعیفی نظیر ۱۲۳۴۵ و کلمه‌ی password همچنان از جمله رایج‌ترین رمزهای عبوری هستند که بسیاری از کاربران از آن‌ها استفاده می‌کنند. همچنین از به‌کار گرفتن اطلاعاتی که هر کسی می‌تواند با یک جستجوی ساده در مورد شما در اینترنت پیدا کند، خودداری کنید؛ مواردی از جمله نام، تاریخ تولد، نام همسر، نام حیوان خانگی یا هر چیز دیگری که به راحتی توسط دیگران قابل تشخیص و حدس زدن باشد. همچنین اطلاعاتی را که در شبکه‌های اجتماعی به اشتراک گذاشته‌اید؛ نباید در رمزهای عبور خود استفاده کنید.

۳ - از جملات استفاده کنید، نه کلمات

بسیاری از متخصصان می‌گویند اگر در انتخاب رمزهای عبور خود به جای استفاده از کلمات از جملات بهره ببریم؛ باعث خواهد شد تا امنیت آن افزایش یابد و در واقع در این حالت یک پسورد پیچیده را انتخاب کرده‌ایم.

به عنوان مثال عبارت summertimeandthelivingiseasy بهتر از summer1 است.

بهتر است اعداد، حروف بزرگ و کوچک و کاراکترهای مختلف را در کنار جملات بکار ببرید تا رمزهای عبورتان پیچیده‌تر شوند. بدین طریق یک رمز خوب می‌تواند چیزی شبیه به این عبارت باشد: \$summerT1meAndTheLivingIsEasy

۴ - از کاراکتر فاصله استفاده کنید

هنگامی که می‌خواهید از جملات به عنوان رمز عبور بهره ببرید کاراکتر فاصله را فراموش نکنید. در صورتی که از کاراکتر فاصله استفاده کنید، بسیاری از ابزارهای تشخیص رمز عبور قادر به شناسایی پسورد شما نخواهند بود؛ زیرا همین کاراکتر به پیچیده‌تر شدن عبارات انتخاب شده کمک می‌کند.

۵ - به رمز عبور ایمیل خود بی توجه نباشید.

از آنجا که معمولا ایمیل یکی از مهم ترین گزینه‌ها برای بازیابی رمز عبور سایر حساب‌های کاربری است؛ باید سعی کنید تا آنجا که امکان دارد یک رمز عبور امن و قوی برای آن تعیین کنید. به عبارتی می‌توان ایمیل را راه دسترسی به بسیاری از اطلاعات کاربر و نیز رمز عبور سایر حساب‌های کاربری وی دانست.

۶ - تغییر رمز عبور

اگر شما هم مثل بسیاری از افراد، از یک رمز عبور مشابه برای تمامی حساب‌های کاربری‌تان استفاده می‌کنید؛ در واقع شاه کلیدی برای هکر محیا کرده‌اید که در صورت دسترسی به آن، وی می‌تواند به همه‌ی حساب‌های شما دسترسی داشته باشد. متخصصان امنیتی پیشنهاد کرده‌اند که در هر ۶۰ تا ۹۰ روز، نسبت به تغییر رمز عبور خود اقدام کنید. اما باید به این نکته هم توجه داشته باشید که در این شرایط باید رمز عبور جدید خود را هم از نوع امن و پیچیده تعیین کنید. اگر رمز جدیدتان آسان‌تر از رمز عبور کنونی شما باشد، بهتر است در کل این کار را انجام ندهید.