✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

امنیت اطلاعات

و

نحوه صحیح پسورد

گردآورنده :

مهندس ایمان اشکاوند راد

http://ashkavand.blogfa.com

Email : i81a@yahoo.com

امنیت اطلاعات

امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری.

واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاها به اشتباه به جای هم بکار برده می شود. اگر چه اینها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آنها وجود دارد. این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله، و موضوعاتی که تمرکز کرده اند دارد.

امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، و یا اشکال دیگر.

امنیت کامپیوتر در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم کامپیوتری تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می شود.

کنترل امنیت اطلاعات :کنترل امنیت به اقداماتی گفته می شود که منجر به حفاظت، مقابله، پیشگیری و یا به حداقل رساندن خطرات امنیتی است. این اقدامات را میتوان به سه دسته تقسیم کرد.

مدیریتی :کنترل مدیریتی (کنترل رویه ها) عبارتند از سیاست ها، رویه ها، استانداردها و رهنمود های مکتوب که توسط مراجع مسئول تایید شده است. کنترل‌های مدیریتی چارچوب روند امن کسب و کار و مدیریت افراد را تشکیل می دهد. این کنترل‌ها به افراد نحوه امن و مطمئن انجام کسب و کار را می گویند و نیز چگونه روال روزانه عملیات‌ها هدایت شود. قوانین و مقررات ایجاد شده توسط نهادهای دولتی یک نوع از کنترل مدیریتی محسوب می شوند چون به شرکت‌ها و سازمانها نحوه امن کسب و کار را بیان می کنند. برخی از صنایع سیاستها، رویه ها، استانداردها و دستورالعمل‌های مختص خود دارند که باید دنبال کنند مثل استاندارد امنیت داده‌های صنعت کارتهای پرداخت (PCI-DSS) مورد نیاز ویزا و مستر کارت. نمونه‌های دیگر از کنترل‌ها مدیریتی عبارتند از سیاست امنیتی شرکت‌های بزرگ، سیاست مدیریت رمز عبور، سیاست استخدام، و سیاست‌های انضباطی. کنترل‌های مدیریتی پایه ای برای انتخاب و پیاده سازی کنترل‌های منطقی و فیزیکی است. کنترل‌های منطقی و فیزیکی پیاده سازی و ابزاری برای اعمال کنترل‌های مدیریتی هستند.

منطقی : کنترل منطقی (کنترل فنی) استفاده از نرم افزار، سخت افزار و داده‌ها است برای نظارت و کنترل دسترسی به اطلاعات و سیستم‌های کامپیوتری. به عنوان مثال: کلمه عبور، فایروال‌های شبکه و ایستگاه‌های کاری، سیستم‌های تشخیص نفوذ به شبکه، لیست‌های کنترل دسترسی و رمزنگاری داده‌ها نمونه‌هایی از کنترل منطقی می‌باشند.

فیزیکی : کنترل فیزیکی برای حفاظت و کنترل محیط کار و تجهیزات کامپیوتری و نحوه دسترسی به آن‌ها است که جنبه فیزیکی دارند. به عنوان مثال: درب، قفل، گرمایش و تهویه مطبوع، آژیر دود و آتش، سیستم دفع آتش سوزی، دوربین‌ها مدار بسته، موانع، حصار کشی، نیروهای محافظ و غیره.

ده قانون تغییرناپذیر در رابطه با امنیت اطلاعات

امنیت اطلاعات و ایمن سازی زیر ساخت فن آوری اطلاعات (فردی، سازمانی، ملی) از جمله وظایف یکایک کاربران و استفاده کنندگان شبکه های کامپیوتری است. به منظور ایمن سازی و ایمن نگهداشتن زیرساخت منابع اطلاعاتی تاکنون مقالات متعددی نوشته شده و توصیه های فراوانی ارائه شده است. اگر بخواهیم برخی از نکات مهم و کلیدی در این رابطه را لیست نماییم، می‌توان به ده قانون تغییر ناپذیر در این زمینه اشاره نمود که صرف نظر از نوع سیستم کامپیوتری، با رعایت آنان یک سطح مطلوب امنیتی و حفاظتی برای کاربران ایجاد می‌گردد.

•**قانون اول :** زمانی که یک برنامه را جهت اجرا انتخاب می نمایید، در واقع شما این تصمیم را گرفته‌اید که کنترل کامپیوتر خود را به آن واگذار نمایید. یک برنامه پس از فراهم شدن شرایط لازم جهت اجرا، قادر به انجام هر کاری می‌باشد و حتی می‌تواند محدودیت هائی را به منظور استفاده از سیستم برای شما ایجاد نماید

> در صورتی که یک مهاجم بتواند شما را ترغیب به اجرای برنامه خود بر روی کامپیوتر نماید، دیگر کامپیوتر متعلق به شما نخواهد بود.

•**قانون دوم :** یک سیستم عامل (نظیر سایر برنامه های کامپیوتری) از مجموعه ای صفر و یک تشکیل می‌گردد که پس از تفسیر توسط پردازنده، باعث انجام عملیات خاصی در کامپیوتر می‌شود. در صورتی که صفر و یک‌ها تغییر یابند، سیستم عامل کارها را به گونه ای دیگر انجام می‌دهد. صفر و یک‌ها در فایل هائی بر روی کامپیوتر شما ذخیره شده‌اند و اگر یک مهاجم بتواند به آنان دستیابی و آنان را تغییر دهد، می‌تواند مشکلات متعددی را برای سیستم ایجاد نماید.

> در صورتی که یک مهاجم بتواند سیستم عامل موجود بر روی کامپیوتر شما را تغییر دهد، دیگر کامپیوتر متعلق به شما نخواهد بود.

•**قانون سوم :** در صورتی که افرادی بتوانند به طور فیزیکی به کامپیوتر شما دستیابی داشته باشند، می‌توانند کنترل کامپیوتر شما را به طور کامل در اختیار گرفته و هر کاری را که دوست دارند انجام دهند (تغییر داده، سرقت اطلاعات، سرقت سخت افزار و یا ایجاد اشکال فیزیکی در کامپیوتر(

در صورتی که یک مهاجم بتواند به طور فیزیکی به کامپیوتر شما دستیابی داشته باشد، دیگر کامپیوتر متعلق به شما نخواهد بود.

•**قانون چهارم :** در صورتی که دارای یک وب سایت می‌باشید، می‌بایست محدودیت‌های لازم در خصوص این که کاربران قادر به انجام چه نوع عملیاتی می‌باشند را ایجاد نمایید (تائید کاربران و صدور مجوزهای لازم با توجه به سطوح دستیابی تعریف شده جهت استفاده از منابع موجود بر روی یک وب سایت). بر روی یک وب سایت صرفاً می‌بایست برنامه هائی را اجرا نمود که توسط افراد و یا شرکت های تائید شده نوشته شده باشند. در بسیاری از موارد رویکرد امنیتی فوق به تنهائی کافی نخواهد بود و در صورتی که وب سایت شما بر روی یک سرویس دهنده مشترک host شده باشد، می‌بایست اقدامات احتیاطی بیشتری را انجام داد. در صورتی که یک مهاجم بتواند به سایر سایت‌های موجود بر روی یک سرویس دهنده دستیابی نماید، در ادامه می‌تواند فعالیت خود را گسترش و سایر سایت‌های موجود را نیز مدیریت و متناسب با خواسته خود با آنان برخورد نماید.

در صورتی که یک مهاجم بتواند فایل هائی را بر روی وب سایت شما ارسال نماید، دیگر وب سایت متعلق به شما نخواهد بود.

•**قانون پنجم :** در صورتی که یک مهاجم بتواند به رمز عبور شما دستیابی پیدا نماید، وی می‌تواند به کامپیوتر شما log on نموده و هر نوع عملیاتی را انجام دهد. سعی نمایید که همواره از رمزهای عبور مناسب و در عین حال پیچیده استفاده نمایید. رمزهای عبوری نظیر تاریخ تولد، شماره شناسنامه، شماره تلفن، شماره دانشجوئی، شماره پرسنلی و مواردی از این قبیل، گزینه های مناسبی در این زمینه نمی‌باشند. در ضمن، هرگز واژه password را به عنوان رمز عبور انتخاب ننمایید.

رمزهای عبور ضعیف، مشکلات امنیتی متعددی را ایجاد می‌نمایند و مانع جدی ایجاد یک سیستم ایمن و با ضریب امنیتی بالا می‌باشند.

•**قانون ششم :** یک مدیر غیرقابل اعتماد می‌تواند سایر اقدامات انجام شده در خصوص امنیت اطلاعات را خنثی نماید. این نوع مدیران با توجه به جایگاه خود قادر به انجام هر گونه عملیاتی می‌باشند. تغییر مجوزها، تغییر سیاست‌های امنیتی سیستم، نصب برنامه های مخرب و تعریف کاربران خیالی، نمونه هائی در این زمینه می‌باشد. عملکرد این گونه مدیران تمامی اقدامات پیشگیرانه در سیستم عامل را بی اثر می‌نماید، چرا که آنان به

طور کامل به سیستم دستیابی داشته و قادر به انجام هر نوع عملیاتی می‌باشند. از همه بدتر، آنان می‌توانند عملیات اشاره شده را به گونه ای انجام دهند که هیچ گونه ردپایی از خود را بر جای نگذارند. در صورتی که شما از یک مدیر غیرقابل اعتماد استفاده می نمایید، عملاً (نمی‌توانید امنیت را در سازمان خود ایجاد نمایید.)

یک کامپیوتر و یا سیستم کامپیوتری صرفاً زمانی می‌تواند ایمن گردد که مدیریت آن در اختیار افراد قابل اعتماد باشد.

•**قانون هفتم :** تعداد زیادی از سیستم‌های عامل و محصولات نرم افزاری رمزنگاری، این امکان را فراهم می‌نمایند تا بتوان کلیدهای رمزگشایی را به صورت مخفی بر روی کامپیوتر ذخیره نمود. بدین ترتیب کاربران در خصوص مدیریت این کلیدها نگران نبوده و همه چیز با استفاده از امکانات نرم افزاری موجود مدیریت می‌گردد. صرف نظر از این که کلیدها به چه صورت مخفی شده‌اند، همواره این احتمال وجود دارد که بتوان به آنان دستیابی داشت. حتی‌المقدور سعی نمایید که از فضای ذخیره سازی offline برای کلیدها استفاده نمایید (امکان دستیابی به کلیدها توسط سایر کاربران online وجود نداشته باشد).

رمزنگاری اطلاعات و رمزگشایی اطلاعات دو کفه یک ترازو می‌باشند که هر یک دارای جایگاه خاص خود می‌باشند و نمی‌توان اهمیت یکی را بیش از دیگری در نظر گرفت. بنابراین، می‌بایست به منظور حفاظت از کلیدهای رمزگشایی تدابیر لازم اندیشیده گردد.

•**قانون هشتم** : نرم افزارهای آنتی ویروس با مقایسه داده موجود بر روی کامپیوتر با مجموعه ای از الگوهای ویروس، قادر به تشخیص آلودگی آنان می‌باشند. هر الگو خصایص منحصربه‌فرد یک ویروس را مشخص می‌نماید که پس از یافتن آن در یک فایل و یا email، پیام لازم از طرف برنامه در اختیار کاربر گذاشته می‌شود. نرم افزارهای آنتی ویروس صرفاً قادر به یافتن ویروس هایی می‌باشند که قبلاً الگوی آنان مشخص و مستند شده باشد. بدیهی است با توجه به این که به طور مستمر ویروس‌های جدیدی نوشته و عرضه می‌گردد، می‌بایست برنامه های آنتی ویروس را به هنگام نگه داشت تا بتوانند با ویروس‌های جدید نیز برخورد نمایند.

داشتن یک نرم افزار آنتی ویروس به هنگام نشده بهتر از نداشتن یک برنامه آنتی ویروس است.

•**قانون نهم :** بهترین روش حفاظت از حریم خصوصی خود در اینترنت، رعایت مسائل ایمنی است (مشابه حفاظت از حریم خصوصی خود در زندگی روزمره). در زمان استفاده از وب سایت‌ها قبل از هر چیز privacy آنان را مطالعه نموده و صرفاً (با افراد و یا مؤسساتی ارتباط برقرار نمایید که نسبت به privacy آنان شناخت کاملی وجود داشته باشد. در صورتی که نگران کوکی هستید، آنان را غیرفعال نمایید.)

گمنامی مطلق نه در زندگی عادی امکان پذیر است و نه در وب

•قانون دهم : امنیت کامل نیازمند یک سطح تکاملی قابل قبول است که در عمل امکان آن وجود ندارد. پیاده سازی نرم افزار یک علم غیر کامل است و از لحاظ مجازی تمامی نرم افزارها دارای باگ هستند که برخی از آنان ممکن است باعث ایجاد حفره های امنیتی خطرناک در سیستم گردند. حتی در صورتی که یک نرم افزار به نظر کامل باشد، نمی‌تواند تمام مسائل امنیتی را به طور کامل برطرف نماید. چرا که درصد بسیار زیادی از حملات مبتنی بر مهندسی اجتماعی می‌باشند که گرچه ساختار امنیتی یک نرم افزار می‌تواند یک سطح حفاظتی مناسب را ایجاد نماید ولی در مقابله با این نوع حملات نمی‌تواند نقش موثری را داشته باشد.

۱۲ نکته مهم در مورد امنیت رمز عبور

برای ما امنیت در یکی از درجات بالای اهمیت قرار دارد. بدون مقدمه‌ی خاصی سعی می‌کنیم دوازده مورد مهم در مورد نحوه‌ی انتخاب بهترین رمز عبور را به شما ارائه دهیم.

۱. از آن‌چه واضح است، به پرهیزید

از عباراتی مثل نام خودتان، کلمه‌ی"password" ، نام کاربریتان، تاریخ تولدتان و چنین موارد آشکاری به عنوان پسورد استفاده نکنید. ممکن است از این مورد به سادگی بگذرید، ولی باورتان نمی‌شود چه تعداد از کاربران اینترنت هنوز هم چنین رمزهایی را استفاده می‌کنند.

۲. پسوردهای ایجاد شده به صورت اتوماتیک را تغییر دهید

اگر پسورد سرویس شما به صورت خودکار ایجاد شده و در اختیار شما قرار داده شده است، در اولین فرصت آن را تغییر دهید تا هم به یاد داشتن آن آسان‌تر باشد و هم مجبور نباشید همیشه آن را از داخل ایمیلتان کپی کنید.

۳. رمز عبور خود را یادداشت نکنید

منظور، نگه داشتن آن‌ها در ایمیل، اسناد روی کامپیوترتان یا یادداشت کردن آن‌هاست. به یاد داشته باشید که همیشه می‌توانید رمز عبور خود را به صورت آنلاین بازیابی نمایید.

۴. در مورد سؤال و جواب‌های امنیتی دقت کنید

سؤال امینتی برای این است که در صورت فراموش کردن رمز عبور، بتوانید با پاسخ دادن به آن، رمز خود را بازیابی کنید. دقت کنید که ممکن است اشخاص نزدیک به شما پاسخ برخی از این سؤال‌ها را بدانند. مثلاً در این مورد، اگر در Hotmail ایمیل داشته باشید، کسی که نام پدر شما را بداند به سادگی می‌تواند به ایمیل‌های شما دسترسی داشته باشد؛ لذا سعی کنید در صورت امکان، پرسش امنیتی را خودتان بنویسید و پاسخ دهید. حتی می‌توانید یک سؤال امنیتی ایجاد کنید و جواب نادرست برای آن تعیین کنید که فقط خودتان آن را می‌دانید.

۵. برای اکانت‌های مختلف، پسوردهای متفاوت داشته باشید

این ممکن است کار شما را کمی سخت کند؛ اما به یاد داشته باشید که همیشه احتمال هک شدن سایت‌ها وجود دارد و همچنین مشکلات امنیتی در سایت‌های شبکه‌های اجتماعی اندک نیست. کسانی که از رمزهای عبور یکسان برای سایت‌های مختلف استفاده می‌کنند، ساده‌تر از دیگران هک می‌شوند.

۶. رمز عبور خود را هر از گاهی تغییر دهید

باز هم این مورد ممکن است کمی طاقت‌فرسا به نظر بیاید، ولی ضریب اطمینان را بسیار بالا می‌برد.

۷. پسورد قوی انتخاب کنید

انتخاب کلماتی که در فرهنگ لغت موجود هستند، یک اشتباه بزرگ است. سعی کنید رمز شما حاوی حروف، اعداد و علائم خاص باشد. هر چه رمز عبور طولانی‌تر باشد، بهتر است.

۸. رمز عبور خود را فاش نکنید

هیچ‌کس نباید به رمز عبور شما دسترسی داشته باشد. حتی اگر یک منبع معتبر از شما درخواست رمز عبور کرد، آن را به او ندهید.

۹. امنیت خود را بروز رسانی کنید

سعی کنید آنتی ویروس سیستم شما بروز باشد و سیستم خود را هر از گاهی برای تروجان‌ها، نرم‌افزارهای جاسوسی و ... که ممکن است خود را مخفی کرده باشند چک کنید. از این قانون ساده پیروی کنید: روی چیزی که مشکوک به نظر می‌رسد کلیک نکنید! سعی کنید اسکریپت های سایتتان همیشه بروز باشد و از افزونه‌های معتبر استفاده نمایید.

۱۰. منظم باشید

بدانید که اطلاعات شما کجا ذخیره شده است؛ مخصوصاً در مورد ایمیل‌ها و سایت‌هایی که در آن‌ها تراکنش مالی انجام می‌دهید.

۱۱. Logout کنید

سعی کنید پس از استفاده از سرویس خود، از آن خارج شوید و همچنین از اکانت خود روی کامپیوترهای عمومی استفاده نکنید.

۱۲. گارد خود را حفظ کنید

اگر از کامپیوتر یا موبایل خود در محیط‌های جمعی استفاده می‌کنید، همیشه حواستان به اطرافتان و کسانی که به دستان شما خیره می‌شوند باشد. دقت کنید موبایل‌هایی که به اینترنت متصل می‌شوند، معمولاً امنیت کافی برای ذخیره‌سازی رمز عبور شما را ندارند.

نحوه صحیح انتخاب پسورد

کلمات عبور بخش مهمی از امنیت کامپیوتر هستند و در حقیقت در خط مقدم حفاظت از اکانت کاربران قرار می‌گیرند. یک کلمه عبور نامناسب ممکن است منجر به سوءاستفاده از کل شبکه شود. به همین دلیل تمام کارمندان شامل پیمانکاران و فروشندگان که به سیستم شرکت دسترسی دارند مسئول انتخاب کلمه عبور مناسب و محافظت از آن هستند.

در این مقاله به نکاتی در مورد ایجاد کلمات عبور قوی و محافظت از آن‌ها و زمان انقضاء و تغییر آن‌ها اشاره می‌شود. در حقیقت مخاطب این مقاله تمام افرادی هستند که مسوول اکانت یا هر سیستمی هستند که از طریق آن به شبکه یا اطلاعات غیرعمومی دسترسی دارند.

سیاست کلی

- تمام کلمات عبور در سطح سیستم باید حداقل سه ماه یک‌بار عوض شوند.
- تمام کلمات عبور سطح کاربر (مانند ایمیل یا کامپیوتر) باید هر شش ماه تغییر کنند که البته تغییر چهار ماهه توصیه می‌شود.
- اکانت های کاربری که مجوزهای سطح سیستم دارند باید کلمات عبوری داشته باشند که با کلمات عبور دیگر اکانت های آن کاربر متفاوت باشد.
- کلمات عبور نباید در ایمیل‌ها یا سایر شکل‌های ارتباطات الکترونیکی درج شوند.
- باید رهنمون‌های زیر در تمام کلمات عبور سطح سیستم و سطح کاربر رعایت شود.

راهنمایی‌ها

راهنمایی کلی ساخت کلمه عبور

کلمات عبور برای اهداف گوناگونی در شرکت‌ها استفاده می‌شوند. تعدادی از استفاده های معمول این‌ها هستند:

- اکانت های سطح کاربر
- اکانت های دسترسی به وب
- اکانت های ایمیل
- حفاظت از مونیتور
- کلمه عبور صندوق پستی
- ورود به روتر محلی

چون سیستم‌های بسیار کمی از نشانه های یک بار مصرف استفاده می‌کنند (مانند کلمات عبور دینامیک که

فقط یک‌بار استفاده می‌شوند)، هرکسی باید از نحوه انتخاب کلمات عبور مناسب آگاه باشد.

کلمات عبور ضعیف معمولاً مشخصات زیر را دارند:

- کلمه عبور شامل کمتر از هشت حرف است.
- کلمه عبور کلمه ای است که در یک فرهنگ لغت یافت می‌شود.
- کلمه عبور کلمه ای است که کاربرد عمومی دارد مانند:
  - o نام خانوادگی، حیوانات اهلی، دوستان، همکاران، شخصیت‌های خیالی و غیره
  - o نام‌ها و اصطلاحات کامپیوتری، فرمان‌ها، سایت‌ها، شرکت‌ها، سخت افزار و نرم افزار.
  - o نام شرکت یا کلمات مشتق شده از این نام.
  - o تاریخ‌های تولد و سایر اطلاعات شخصی مانند آدرس‌ها و شماره های تلفن.
  - o الگوهای کلمات یا شماره‌ها مانند aaabbb، qwerty، zyxwvuts، 123321 و غیره.
  - o هرکدام از عبارات فوق به طور برعکس.
  - o هرکدام از عبارات فوق که تنها با یک رقم شروع یا به آن ختم می‌شود.

کلمات عبور مناسب مشخصات زیر را دارند:

- شامل هم حروف کوچک و هم بزرگ هستند (a-z و A-Z)
- علاوه بر حروف از ارقام و نشانه‌ها هم در آن‌ها استفاده می‌شود مانند 0-9 و! @/.?<>;[]{}’=~|_+()*&^%$#
- حداقل هشت حرف دارند.
- کلمه ای در هیچ زبان، گویش یا صنف خاص نیستند.
- بر پایه اطلاعات شخصی، اسم یا فامیل نیستند.
- کلمات عبور هرگز نباید نوشته یا جایی ذخیره شوند. سعی کنید کلمات عبوری انتخاب کنید که بتوانید به راحتی در ذهن داشته باشید. یک روش انجام این کار، ایجاد کلمه عبور بر پایه یک ترانه یا عبارت است. برای مثال عبارت ”This May Be One Way To Remember“ و کلمه عبور می‌تواند ” !TmB1w2R“ یا ”Tmb1W>r~“ یا انواع دیگری از همین الگو باشد.

توجه: این مثال‌ها را به عنوان کلمه عبور استفاده نکنید.

استانداردهای حفاظت از کلمه عبور

از کلمات عبور مشترک برای اکانت های شرکت و دسترسی‌های شخصی استفاده نکنید. تا جایی ممکن است، از کلمه عبور مشترک برای نیازهای مختلف شرکت استفاده نکنید. برای مثال، برای سیستم‌های مهندسی یک کلمه عبور انتخاب کنید و یک کلمه عبور دیگر برای سیستم‌های IT . همچنین برای استفاده از اکانت های

NT و UNIX کلمات عبور متفاوت انتخاب کنید.

کلمات عبور شرکت با هیچ کس از جمله دستیاران و منشی‌ها در میان نگذارید. باید با تمام کلمات عبور به صورت اطلاعات حساس و محرمانه برخورد شوند.

در اینجا به لیستی از "انجام ندهید" ها اشاره می‌شود.

- کلمه عبور را از طریق تلفن به هیچ کس نگویید.
- کلمه عبور را از طریق ایمیل فاش نکنید.
- کلمه عبور را به رئیس نگویید
- در مورد کلمه عبور در جلوی دیگران صحبت نکنید.
- به قالب کلمه عبور اشاره نکنید (مثلاً نام خانوادگی)
- کلمه عبور را روی فهرست سؤالات یا فرم‌های امنیتی درج نکنید.
- کلمه عبور را با اعضای خانواده در میان نگذارید.
- کلمه عبور را هنگامی که در مرخصی هستید به همکاران نگویید.

اگر کسی از شما کلمه عبور را پرسید، از ایشان بخواهید که این مطلب را مطالعه کند یا اینکه با کسی در قسمت امنیت اطلاعات تماس بگیرد.

از ویژگی "Remember Password" یا حفظ کلمه عبور در کامپیوتر استفاده نکنید.

مجدداً، کلمات عبور را در هیچ جای محل کار خود ننویسید و در فایل یا هر سیستم کامپیوتری ذخیره نکنید (شامل کامپیوترهای دستی) مگر با رمز کردن.

کلمات عبور را حداقل هر شش ماه عوض کنید (بجز کلمات عبور سطح سیستم که باید هر سه ماه تغییر کنند).

اگر هر اکانت یا کلمه عبور احتمال فاش و سوءاستفاده از آن می‌رود، به بخش امنیت اطلاعات اطلاع دهید و تمام کلمات عبور را تغییر دهید.

شکستن یا حدس زدن کلمه عبور ممکن است در یک زمان متناوب یا اتفاقی توسط بخش امنیت اطلاعات یا نمایندگی‌های آن رخ دهد. اگر کلمه عبور در طول یکی از این پیمایش‌ها حدس زده یا شکسته شود، از کاربر خواسته خواهد شد که آن را تغییر دهد.

رعایت موارد مذکور، به حفاظت بیشتر از اطلاعات و قسمت‌های شخصی افراد کمک خواهد کرد.

برای انتخاب یک پسورد مطمئن باید حروف و اعداد غیر محتمل را پشت سر هم قرارداد. هرچه رمزتان نامفهوم‌تر باشد، هک کردن آن سخت‌تر خواهد بود. به این توصیه‌ها توجه کنید:

اگر شما نیز رمز ۱۲۳۴۵۶ را برای ایمیل خود انتخاب کرده‌اید هم‌اکنون آن را تغییر دهید چرا که ایمیل شما در معرض هک افراد سودجو قرار دارد. البته در صورت مثبت بودن پاسخ شما، باید بدانید که تنها نیستید چرا که ۳۲ میلیون نفر دیگر نیز رمزی شبیه به این برای خود انتخاب کرده‌اند.

به نوشته همشهری، با گسترش کارت‌های هوشمند بانکی، کارت سوخت و کارت‌های شناسایی متعدد دیگر، لزوم ایجاد و استفاده از رمزهای مختلف نیز مطرح شده است. برای این‌گونه کارت‌ها عمدتاً باید رمز عددی ایجاد کنید. پس برای جلوگیری از لو رفتن رمز کارتتان باید در نظر داشته باشید که به هیچ وجه اعداد مرتبط با تاریخ تولد، شماره شناسنامه، شماره ملی، پلاک منزل، تلفن همراه و تلفن ثابت خود را به عنوان رمز عددی این کارت‌ها تعیین نکنید چرا که در صورت سرقت کارت‌ها، به راحتی قابل حدس زدن توسط سارقین است.

همچنین به هیچ‌وجه رمزهای خود را در گوشی موبایل یا روی کارت‌ها ننویسید یا حتی رمزهای خود را روی کاغذ ننویسید و داخل کیف پولتان قرار ندهید. از سوی دیگر به خاطر استفاده از سرویس‌های متعدد اینترنتی مانند ایمیل، وبلاگ، وب‌سایت، شبکه داخلی، رایانه یا لپ‌تاپ یا شبکه‌های اجتماعی و رسانه‌های آنلاین شما نیاز به ایجاد رمزهای متعدد دارید. به یاد داشته باشید که به هیچ‌وجه از یک رمز برای همه این سرویس‌ها استفاده نکنید چون به محض لو رفتن یکی از آن‌ها، بقیه سرویس‌های شما نیز به صورت دومینو هک و سرقت می‌شود.

انتخاب و ایجاد رمزهای پیچیده برای اکانت های مختلف کاربران اینترنت، به کاری سخت و مشقت بار تبدیل شده است. از طرفی بسیاری از کاربران اساساً نمی‌دانند که چه نوع رمزهایی مصون از هک شدن هستند. هرچند اغلب سرویس‌های ارائه‌دهنده ایمیل، وبلاگ یا وب‌سایت در کنار گزینه ایجاد رمز، موتوری ایجاد کرده‌اند که قدرت رمز شما را می‌سنجد؛ یعنی اگر رمز شما به اندازه کافی قوی نباشد به شما اخطار می‌دهد. برخی از این سرویس‌ها حتی محدودیت‌هایی به لحاظ تعداد کاراکتر برای ایجاد رمز تعیین کرده‌اند.

اخیراً گروه LulzSec، بسیاری از وب‌سایت‌های معتبر دنیا از سونی، سگا، نینتندو تا سایت‌های دولتی آمریکا مانند CIA را مورد حمله قرار داده و اطلاعات محرمانه برخی را به دست آورده‌اند. این گروه که شامل هکرهای برجسته دنیا هستند ۶۲هزار آدرس ایمیل را به همراه رمز عبور برای عموم منتشر کردند. با بررسی رمز عبور ایمیل‌های هک شده می‌توان درس‌های مهمی گرفت. مهم‌ترین درسی که از اقدام اخیر این گروه می‌توان گرفت این است که باید برای ایمیل‌های خود رمز عبور پیچیده انتخاب کنیم.

سال پیش گروه RockYou.com اعلام کرد که ۳۲میلیون اکانت را که دارای رمز عبور ۱۲۳۴۵۶ بوده‌اند به دست آورده است. اکثر ایمیل‌های هک شده توسط گروه اخیر، رمز عبور ۱۲۳۴۵۶ داشته‌اند. پس از آن ۱۲۳۴۵۶۷۸۹ و password و abc123 از همه بیشتر استفاده شده‌اند.

رمزهای عبور دیگر که توسط LulzSec هک و منتشر شده‌اند دارای کلمات رایج و متداول مردم هستند، همچنین بیش از ۲۰درصد رمزهای عبور کاربران تنها شامل عدد است. پس لازم است بدانید که رمز عبور شما می‌بایست شامل حروف و اعداد باشد و حتماً در آن از ترکیب حروف بزرگ و کوچک استفاده شود. در رمز عبور خود می‌توانید از کاراکترهای خاص مانند $, # یا نقطه استفاده کنید. جالب است بدانید که تنها ۸۵صدم درصد از ایمیل‌های هک شده توسط LulzSec دارای کاراکترهای خاص بوده‌اند.

انتخاب پسورد مطمئن

برای انتخاب یک پسورد مطمئن باید حروف و اعداد غیر محتمل را پشت سر هم قرارداد. هرچه رمزتان نامفهوم‌تر باشد، هک کردن آن سخت‌تر خواهد بود. به این توصیه‌ها توجه کنید:

۱ – از انتخاب کلمات و عباراتی که برایتان اهمیت شخصی دارند خودداری کنید.

۲ – حروف، اعداد و علامت‌ها را با هم ترکیب کنید. بعضی حروف را با شکل بزرگ آن و بعضی دیگر را با شکل کوچک آن استفاده کنید.

۳ – راه خوبی برای به خاطر سپردن آن پیدا کنید. یک راه خوب برای انجام این کار این است که از نخستین حروف یک جمله‌ای که به خاطر دارید استفاده کنید. در وسط جمله می‌توانید از علامت‌های نشانه‌گذاری هم بهره ببرید.

۴ – هرچه طولانی‌تر بهتر. هیچ‌وقت پسوردی نسازید که کمتر از ۸ حرف داشته باشد.

۵ – راه دیگر این است که مثلاً از یک کلمه مثل mardoman استفاده کنید و روی کیبورد، دستتان را یک ردیف بالاتر ببرید. مثلاً mardoman می‌شود: jq4e9jqh.

۵ – در هر صورت یادتان باشد که نباید رمز خود را به هیچ‌کس دیگر بدهید. حتی اگر رمزهایی توسط سیستم، بانک یا به طور پیش فرض توسط رایانه برای شما ایجاد شده بلافاصله آن‌ها را تغییر دهید و اساساً به صورت دوره‌ای رمزهای خود را تغییر دهید.

۶ – هیچ‌گاه یک کلمه معنادار را به عنوان پسورد تعیین نکنید. برخی نرم‌افزارهای هک و نفوذ، کل کلمات یک دیکشنری یا لغت نامه را در چند دقیقه به عنوان پسورد احتمالی به سیستم می‌دهند و اگر رمز شما یکی از این کلمات باشد لو می‌رود!

۷ – هرگز به جز در سرویسی که عضو آن هستید رمز و شناسه خود را وارد نکنید. برخی نرم‌افزارهای هک رمز از صفحات قلابی مشابه صفحات اصلی برای سرقت رمز کاربران استفاده می‌کنند. همیشه به آدرس بالای صفحه دقت کنید، مثلاً آیا واقعاً این صفحه‌ای که از شما شناسه و پسورد خواسته است یاهو یا جیمیل است یا به جایی دیگر ختم می‌شود؟

۸ – تنظیمات ذخیره خودکار رمز روی سایت‌ها و رایانه‌های خود را غیرفعال کنید. در غیر این صورت هر وقت فردی به طور غیرمجاز یا تصادفی به رایانه شما دسترسی پیدا کند رمزهای شما هم لو خواهد رفت. این شیوه به ویژه در کافی نت‌ها بسیار رایج است.

حالا اگر به این توصیه‌ها گوش کردید می‌توانید قدرت پسورد خودتان را با استفاده از سایت سنجش پسورد به آدرس www.passwordmeter.com بیازمایید یا اینکه با استفاده از سرویس‌هایی مانند Password Strength Test مایکروسافت میزان امن بودن آن را آزمایش کنید.

علم انتخاب صحیح رمز عبور

طی تحقیقات تروی هانت – یکی از متخصصان برتر مایکروسافت در زمینه امنیت شبکه و کامپیوتر – در مورد نحوه انتخاب رمز عبور توسط کاربران، وی به این نتیجه رسیده بود اصولاً، رمزهای عبور انتخابی بسیار کوتاه (بین ۶ تا ۱۰ حرف)، ساده (کمتر از یک درصد از آن‌ها ترکیب حرف و عدد هستند) و قابل پیش بینی (بیش از یک سوم آن‌ها جزو عبارات رایج هستند) هستند .هانت در مقاله ای که در وبلاگ شخصی خود منتشر کرده، مدعی شده است برایش بسیار جالب و عجیب بوده که نتیجه تحقیقاتش در مورد حساب کاربری سیستم سونی نشان داده است ۹۲ درصد حساب‌های کاربری اعضای این سیستم، رمزهای عبور مشابه یکدیگر دارند. در همین راستا این سؤال برایش پیش آمده است که کاربران بر چه اساسی برای حساب‌های کاربری خود رمز عبور انتخاب می‌کنند .شاید بتوان با در نظر گرفتن ریشه و منبع کلمات و اعداد به کار رفته در رمز عبور یا پیش زمینه فکری فرد در مورد شاخصه های انتخاب، این سؤال را پاسخ داد .در واقع باید گفت بخش عظیمی از رمزهای عبور حول محور کوچک و مشخصی از انتخاب‌ها می‌چرخند. این یک تحقیق جالب در مورد کاربرانی است که رمزهای عبور ساده ای برای حساب‌های کاربری خود انتخاب می‌کنند.

منبع اطلاعات و روند تحلیل اطلاعاتی که در این جا از آن‌ها استفاده شده است از منابع مختلفی همچون وب سایت‌های سونی و Gawker که چندی پیش هک شده و حساب کاربری اعضایشان در اینترنت منتشر شد گرفته شده‌اند. این اطلاعات فقط شامل آدرس ایمیل و رمزهای عبور افراد است و هیچ اطلاعات بیشتری از آن‌ها، همچون آدرس شخص در دنیای واقعی وجود ندارد. در حدود ۳۰۰ هزار حساب کاربری در این تحقیق وجود دارند و هر کدام نکته قابل توجهی در مورد انتخاب رمز عبور دارند .سه تا از منابع اطلاعاتی اصلی مورد استفاده کاربران برای انتخاب رمز عبور را می‌توان موارد پایین معرفی کرد:

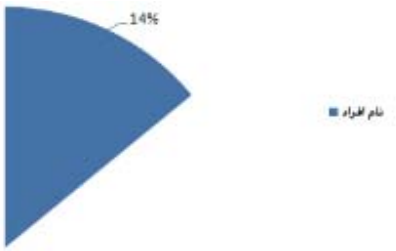
- نام افراد: شامل بیش از ۲۶ هزار نام و نام خانوادگی رایج است

- نام مکان: شامل نام منطقه، شهر، روستا و حتی کشور است که حدود ۳۲ هزار حساب با این نام‌ها ثبت شده‌اند.
- لغت نامه انگلیسی: حدود ۱۹۰ هزار کلمه در لغت نامه انگلیسی وجود دارد

با کمک سه منبع ذکر شده در بالا می‌توان ریشه و منبع اصلی رمزهای عبور انتخابی را مشخص کرد. سه گزینه بالا که از منابع مختلف و البته فراگیر و جامع گرفته شده‌اند، به هیچ وجه کامل نیستند. این به این معنا است که احتمال دارد گزینه ها و عبارت‌های اصلی و کلیدی در میان این سه آیتم نباشند. در این صورت، بدون شک حدس هایی که در مورد رمز عبور می‌زنیم بسیار ضعیف‌تر از زمانی است که فهرست کامل و دقیقی از احتمالات را در اختیار داریم . اما به هر حال، در اینجا قصد داریم این موضوع را کمی ساده تر فرض و احتمال وجود نقطه گذاری و نشانه های نوشتاری را رد کنم. البته این نشانه ها برای انتخاب رمز عبور بسیار مهم هستند و نقش سازنده ای دارند. اما در این تحقیق ما فرض را بر وجود نداشتن آن‌ها می‌گذاریم. چون همان طور که قبلاً هم گفتیم فقط حدود یک درصد از کاربران از این نشانه ها برای رمز عبور اکانت شان استفاده می‌کنند .برای انتخاب رمز عبور از نام خودمان، به هر صورتی که باشد، همچون Troy یا troy یا حتی به صورت ترکیبی با نام خانوادگی همچون Troy Hunt یا troyhunt باز هم از منابع منطقی مشابه استفاده می‌کنیم. منبعی که حدود ۴۵ درصد کاربران از آن برای نوشتن رمز عبور استفاده می‌کنند .در این تحقیق، ابتدا به سراغ اطلاعات فردی کاربر همچون نام او می‌رویم .بعد از آن به اطلاعات کلی‌تر همچون محل زندگی و بعد لغت نامه انگلیسی خواهیم پرداخت تا مشخص کنیم این گزینه ها تا چه حد در ساخت رمز عبور نقش دارند.

نام افراد تحقیق را با نام افراد شروع می‌کنیم زیرا نام، بارزترین مشخصه فردی هر کاربری به شمار می‌آید. البته نام مورد نظر الزاماً نام خود کاربر و دارنده حساب نیست. ممکن است نام همسر، فرزند و حتی حیوانات خانگی او باشد. در ضمن این که این نام می‌تواند اسم کوچک، نام خانوادگی و حتی اسم مستعار باشد. پس مسئله به آن سادگی که در ابتدا فرض می‌شد نیست .اگر به نمودارهای زیر توجه کنید متوجه می‌شوید چه تعداد از افراد از نام - با در نظر گرفتن بخش‌ها و احتمالات مختلف آن – برای رمز عبور خود استفاده می‌کنند.

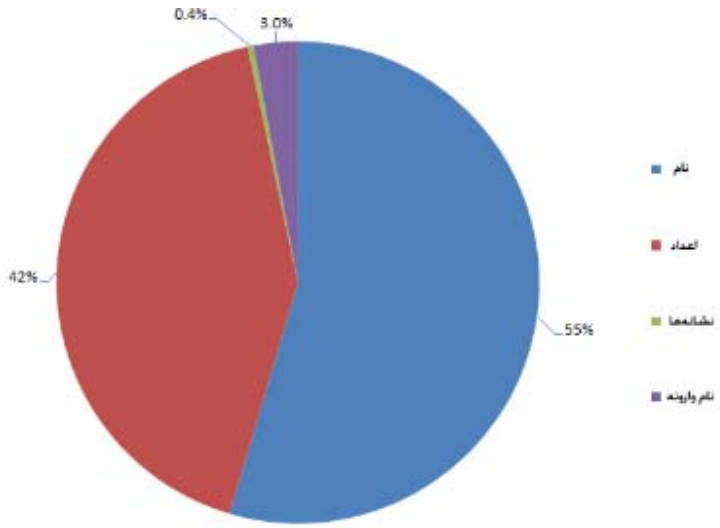
رمزهای عبوری که از نام خود کاربر ساخته شده‌اند



نمودار بالا نشان می‌دهد حدود ۱۴ درصد از کاربران برای انتخاب رمز عبور اکانت شان از نام خود استفاده می‌کنند. البته این پایان ماجرا نیست. هستند کاربرانی که به نام خود عدد یا نماد و نشانه های مختلفی اضافه می‌کنند. به طور مثال troy21 ، دقیقاً نام فرد نیست اما مشخص است ریشه آن از اسم کوچک وی گرفته شده است .با این حساب باید بدانید که سه روش رایج در میان کاربران برای استفاده از نام در رمز عبور وجود دارد :

- استفاده از اعداد در کنار اسم
- استفاده از نشانه ها و علامت‌های نقطه گذاری
- وارونه کردن نام بدون استفاده از عدد و علامت نمودار پایین، با احتساب سه احتمال ذکر شده در بالا شکل گرفته است.

رمزهای عبور برگرفته شده از نام کاربران

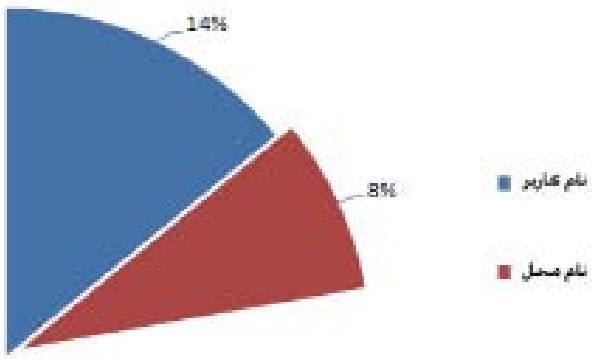


همان طور که در شکل بالا مشخص است، اضافه کردن اعداد به اسم، کاربرد بیشتری نسبت به دو گزینه دیگر دارد. جالب اینجا است که عدد یک رایج‌ترین رقم برای استفاده در رمز عبور حساب‌های کاربران است. اعداد دو رقمی و چهار رقمی همچون اعداد سال یا ماه تولد نیز استفاده فراوانی در شکل گرفتن رمزهای عبور دارند باز همان طور که در ابتدا اشاره کردیم، درصد استفاده از نشانه ها در رمز عبور بسیار پایین است. کمتر از یک درصد از کاربران از نقطه گذاری در نوشتن رمز عبور استفاده می‌کنند. برعکس و وارونه کردن نام نیز از آن جا که کمی گیج کننده و درهم است، یکی از روش‌های بسیار ساده برای امنیت بیشتر رمز عبور به حساب می‌آید .البته، از آنجا که تعداد حروف نام‌های برعکس شده با نام اصلی کاربر مغایرتی ندارد، احتمال لو رفتنشان زیاد است.

نام محل

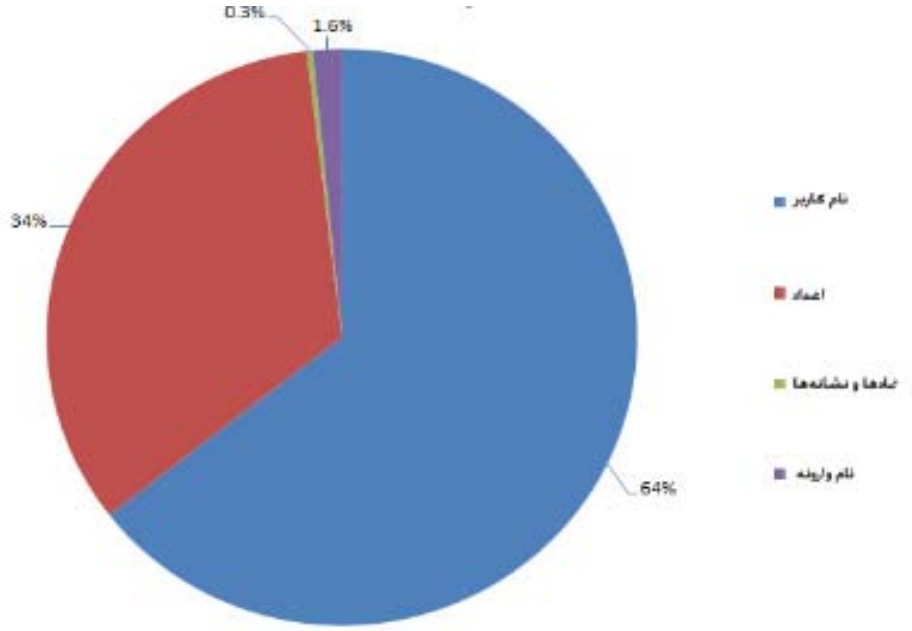
یکی دیگر از روش‌های رایج برای نوشتن رمز عبور، استفاده از نام مکان‌ها است. این مکان‌ها می‌تواند شامل شهر، خیابان، منطقه، نام شرکت و حتی کشور کاربر باشند. یا حتی نام محلی که برای کاربر اهمیت فراوانی دارد.

نمودار پایین نشان دهنده آمار استفاده از نام مکان در رمز عبور است.



همان طور که در شکل بالا می‌بینید حدود ۸ درصد از رمزهای عبور کاربران بر اساس نام محل یا مکان خاصی است. برخی از مکان‌ها نام مشابه انسان دارند همچون ویکتوریا یا جزو لغت‌های لغت نامه انگلیسی هستند. این مسئله تفاوت چندانی در اصل قضیه ندارد. اصل این است که این کلمات برگرفته از نام‌های رایجی هستند که ممکن است هر کاربری از آن‌ها استفاده کند.

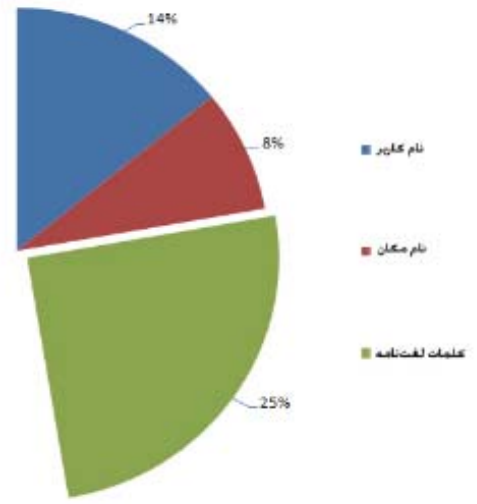
اگر نام مکان را نیز همچون نام کاربر به سه دسته نام، نام بعلاوه عدد و نماد و نام وارونه مکان طبقه بندی کنیم، آماری همچون نمودار پایین به دست می‌آید.



همان طور که قبلاً هم اشاره کردیم، عدد «یک» پرکاربردترین عدد میان دیگر اعداد است. بیشتر کاربران به جای استفاده از اعداد به صورت رندم سعی در استفاده از اعدادی دارند که به خاطر سپردنشان برایشان آسان باشد. البته ترکیب نام و عدد با هم برای ساختن رمز عبور، درصد امنیت آن را بالاتر می‌برد.

کلمات لغت نامه : استفاده از فرهنگ لغت رایج‌ترین منبع برای انتخاب رمز عبور میان کاربران است. شاید بتوان لغت نامه را بزرگ‌ترین منبع دانست.

رمزهای عبوری که از لغت نامه انتخاب شده‌اند:

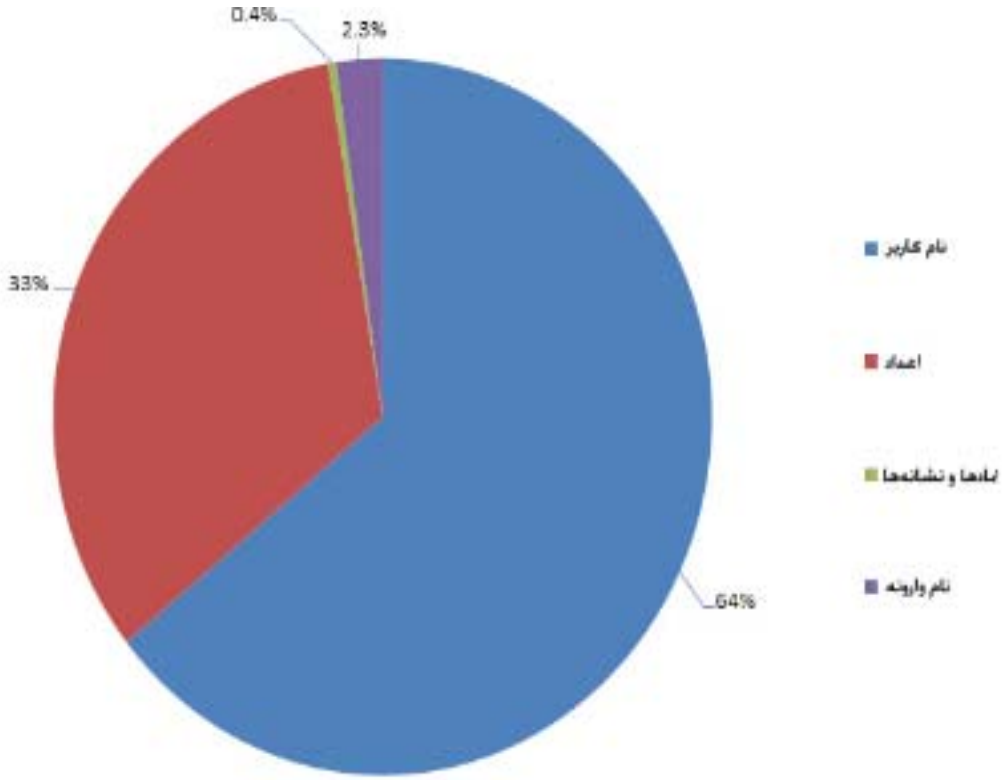


حدود ۲۵ درصد از رمزهای عبور از فرهنگ لغات انگلیسی استخراج شده‌اند. در پایین سه کلمه رایجی را می‌بینید که به عنوان رمز عبور، از دیکشنری انتخاب شده‌اند:

- رمز عبور password
- میمون monkey
- اژدها dragon

شاید گزینه اول برای شما هم جالب باشد که فردی از لغت پسورد به عنوان رمز عبور استفاده کند. جالب‌تر این که کاربران بسیاری به این کلمه فکر و آن را به عنوان رمز عبور انتخاب کرده‌اند. با داشتن نام کاربری و رمز عبور چند صد هزار اکانت (در ابتدای بخش اول به منابع این مقاله اشاره شد)، می‌توان به راحتی گفت رمز عبور حدود دو هزار و اندی از حساب‌های کاربری، کلمه password است .کلمات برگرفته شده از دیکشنری نیز در حالت ترکیبی ترتیبی همچون نام شخص و نام محل دارند. یعنی می‌توان برای ساختن رمز عبور با آن‌ها، از اعداد یا نشانه ها و علامت‌های نقطه گذاری در کنارشان استفاده کرد یا آن‌ها را وارونه و برعکس نوشت.

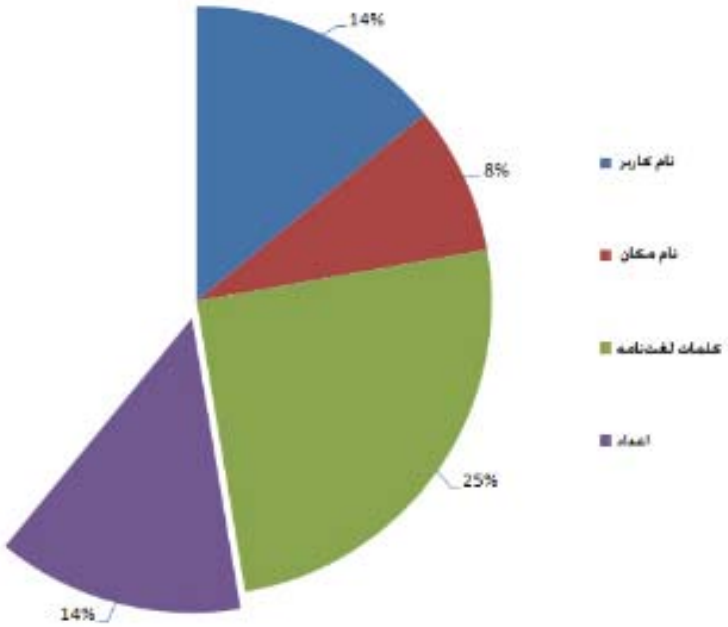
ساختار رمزهای عبوری که از دیکشنری استخراج شده‌اند:



اعداد

اعداد، یکی دیگر از منابع انتخاب رمز عبور هستند. منظور از عدد، فقط خود اعداد و ارقام به تنهایی هستند، نه اعدادی که در کنار کلمات، رمزهای عبور را می‌سازند. این اعداد تقریباً محبوبیت خوبی میان کاربران دارند و درصد استفاده آن‌ها زیاد است.

رمزهای عبور عددی

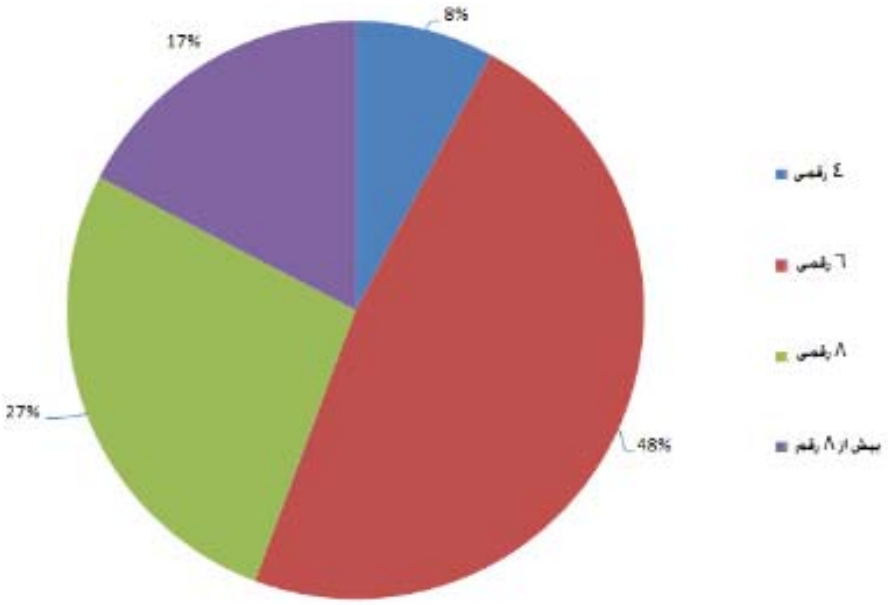


حدود ۱۴ درصد از رمزهای عبور حساب‌های کاربری، عددی هستند. بیشترین کاربرد را نیز سه ترکیب پایین به خود اختصاص داده‌اند:

- ۱۲۳۴۵۶
- ۱۲۳۴۵۶۷۸
- ۱۲۳۴۵۶۷۸۹

در مورد رمزهای عبور عددی، تعداد اعداد و طولانی بودن رمز عبور است که اهمیت دارد. نمودار زیر، درصد استفاده از تعداد ۴، ۶، ۸ و بیشتر عدد را نشان می‌دهد.

تعداد اعداد رمز عبور:



شاید دانستن آمار استفاده تعداد رقم‌های رمزهای عبور عددی برای شما هم جالب باشد. معمولاً رمزهای عبوری که در ساختشان از ارقام بین یک تا ۲۱ استفاده شده است، ۴، ۶ یا ۸ رقمی هستند. بیشترین استفاده از رمز عبور چهار رقمی را کد «۱۲۳۴» به خود اختصاص داده است. البته رمزهای عبور عددی چهار رقمی کمترین استفاده را بین دیگر کدها دارند و فقط ۸ درصد از کاربران از آن‌ها استفاده می‌کنند. بد نیست بدانید کد «۱۹۸۴» نیز کد چهار رقمی دیگری است که رواج بسیاری بین کاربران دارد. «۱۹۸۴» نام رمان بسیار جذاب و مشهور «جورج اورول» است.

البته رمزهای عبور عددی چهار رقمی می‌توانند از سال تولد، رمز عابر بانک، پین کد موبایل و موارد مشابه دیگر نیز گرفته شوند.

کدهای ۶ رقمی بیشترین آمار را میان رمزهای عبور عددی دارند. این کدها بیشتر بر مبنای تاریخ مشخصی – روز، ماه و سال (دو رقم آخر) – نوشته می‌شوند.

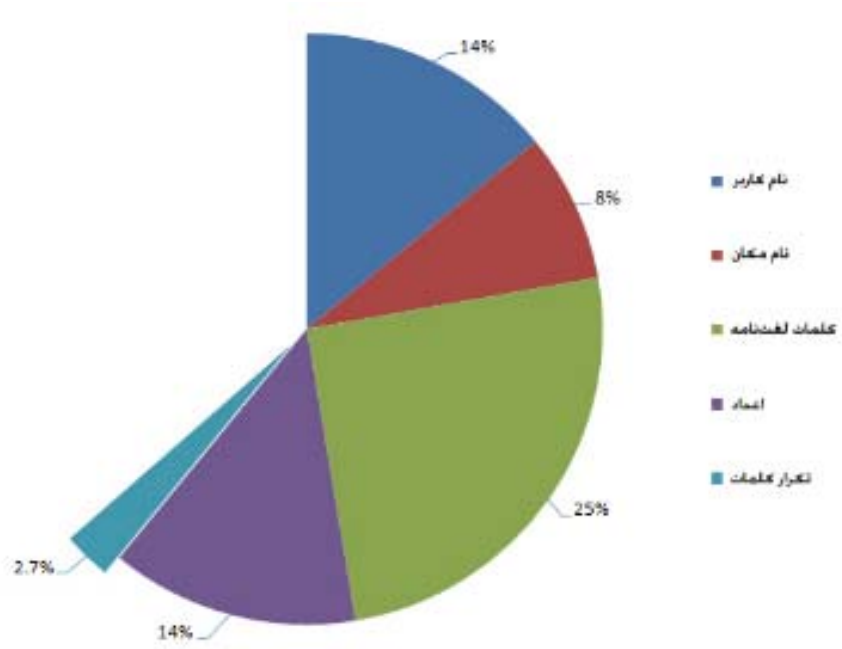
در مورد کدهای ۸ رقمی نیز می‌تواند بر مبنای تاریخ (با ذکر سال به طور کامل) باشد. ولی در نهایت باید گفت این کدها الگوی خاصی ندارند و هر ترکیبی می‌تواند این رمزها را تشکیل دهد. شاید بتوان از رایج‌ترین و ساده‌ترین
رمزهای عددی ۸ رقمی به کدهای «۱۲۳۴۵۶۷۸» و «۱۱۲۲۳۳۴۴» اشاره کرد.

تکرار کلمات

نوشتن دو بار پشت سر هم یک لغت یا به اصطلاح تکرار آن برای ساخت رمز عبور نیز یکی از روش‌های معمول است. البته کمتر از ۳ درصد از کاربران از این روش استفاده می‌کنند.

شکل پایین همه منابع مورد استفاده در رمز عبور را با هم مقایسه کرده است.

رمزهایی که با تکرار دوباره یک کلمه ساخته شده‌اند:



همان طور که در شکل بالا می‌بینید، حدود ۲۰۷ درصد از کاربران از ترفند تکرار کلمات برای رمز عبور حسابشان استفاده می‌کنند. بیشترین آمار را نیز سه کلمه پایین در آمریکا از آن خود کرده‌اند:

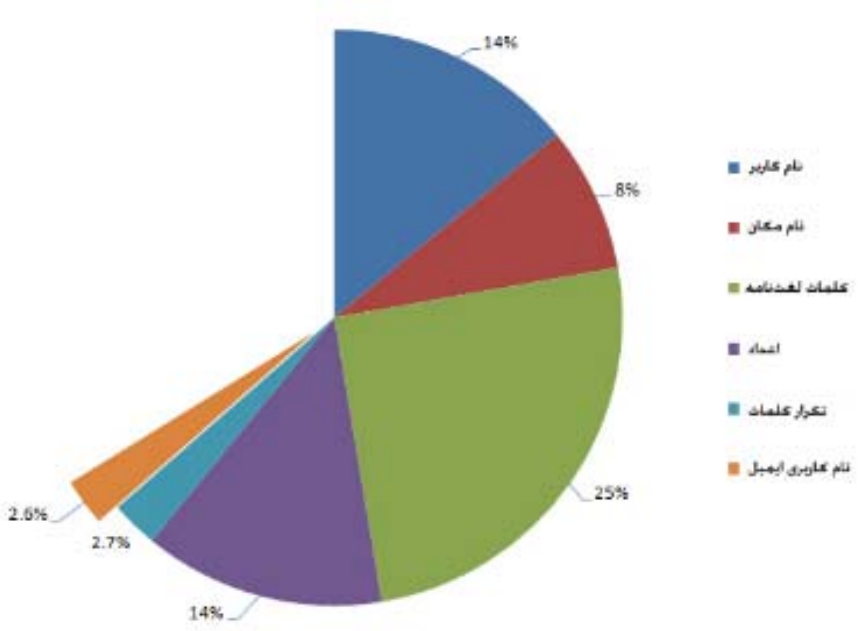
- blahblah
- poopoo
- lovelove

به نظر می‌رسد این گونه رمزهای عبور در واقع کلمات ساده و قابل حدسی باشند که برای جلوگیری از زود لو رفتن و البته برای بلند و طولانی شدن رمز عبور، تکرار می‌شوند. تعداد کلمات این نوع رمزهای عبور، معمولاً بیش از ۸ کلمه نیست. از نظر امنیتی نیز چندان معتبر نیستند زیرا یک سری حروف ساده‌اند که تکرار شده‌اند. اصولاً این گونه رمزها بدون هیچ گونه علامت، نشانه یا عددی نوشته می‌شوند.

رمز عبور به شکل خود نام کاربری

چرا باید برای به یاد ماندن رمز عبور ایمیل فسفر مصرف کنیم، وقتی می‌توان به آسانی از خود نام کاربری به عنوان رمز عبور هم استفاده کرد؟ متوجه منظور من شدید؟ به طور مثال، نشانی ایمیل فردی troyhunt@hotmail.com است و وی می‌تواند از troyhunt (نام کاربری) به عنوان رمز عبورش هم استفاده کند. این موضوع علاوه بر جالب بودن، همیشه هم در یاد می‌ماند. اما درصد امنیت آن چندان بالا نیست.

رمزهای عبوری که نام کاربری هستند:

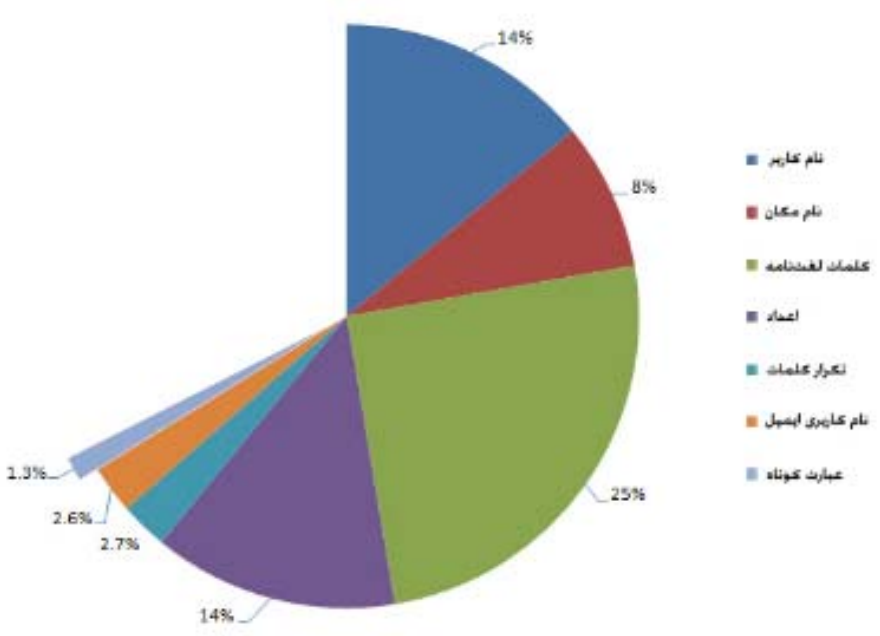


آمار استفاده از نام کاربری به عنوان رمز عبور کمتر از ۳ درصد است، اما باز هم میزان قابل توجهی است.

عبارات کوتاه

استفاده از عبارات کوتاه نوعی دیگر از روش‌های ساخت رمز عبور برای ایمیل است. شاید بتوان این روش را جزو دقیق‌ترین و امن‌ترین روش‌ها برای این منظور دانست. حدس زدن و پیدا کردن عبارات کوتاه، کار چندان ساده ای نیست .البته تعداد کمی از کاربران از این عبارات به عنوان رمز عبور استفاده می‌کنند.

نمودار پایین نمایشگر آمار استفاده عبارات کوتاه نسبت به دیگر منابع است.



در پایین سه نمونه از رایج‌ترین عبارت هایی که کاربران بیش از همه استفاده می‌کنند را مثال زده‌ایم:

- trustno1 (به هیچ کس اعتماد نکن - trust no one)
- letmein (بگذار بیایم داخل let me in)
- iloveyou (دوستت دارم - i love you)

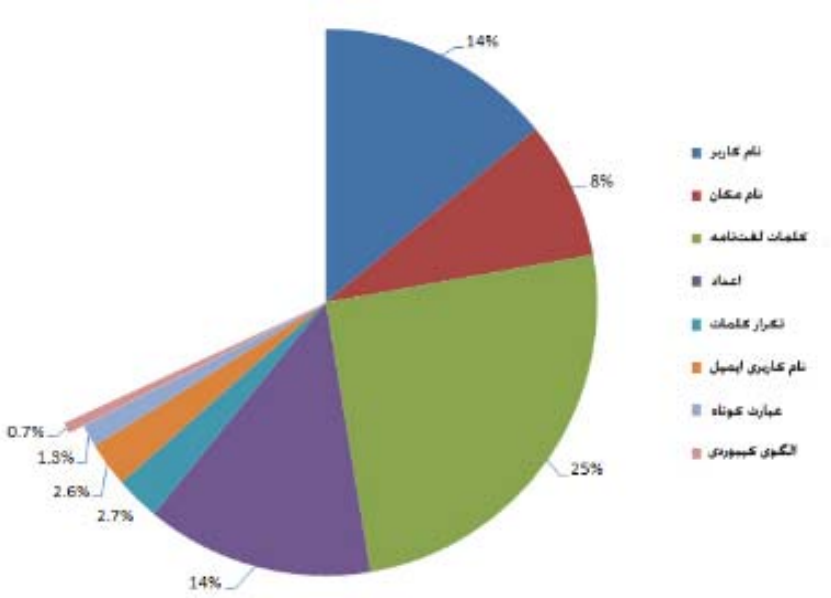
گزینه نخست کمی سخت‌تر از دو گزینه دیگر است. دو گزینه دوم و سوم موارد مصرف بسیاری دارند و زیاد شنیده می‌شوند. اما گزینه اول از آنجا که به جز حروف، ترکیبی از عدد نیز هست، به ظاهر امنیت بیشتری دارد و کاربران بیشتری از آن استفاده می‌کنند. البته باید گفت گزینه های دو و سه در کتاب رمزهای عبور رایج هم وجود دارند و این موضوع ضریب امنیتشان را کاهش می‌دهد.

الگوهای کیبوردی

هر چه پایین‌تر می‌آییم به منابعی می‌رسیم که کمترین کاربرد را میان کاربران دارند. اما در عین حال امنیت بسیار خوبی نسبت به روش‌های رایج‌تر دارند. استفاده از الگوهای خاص روی صفحه کلید نیز یکی دیگر از منابع کم
کاربرد اما امن است. دلیل امنیت آن نیز این است که کلماتی که بر اساس الگوی خاصی ساخته می‌شوند، در

فرهنگ لغت انگلیسی وجود ندارند. یعنی در واقع کلمه معنی دار و مشخصی نیستند که بتوان به راحتی آن را پیدا کرد.

شکل پایین میزان رواج استفاده از الگوهای خاص روی صفحه کلید را با دیگر منابع مقایسه می‌کند:



همان طور که در شکل بالا مشخص است، کمتر از یک درصد از کاربران از pattern یا همان الگوهای صفحه کلید برای ساخت رمز عبور استفاده می‌کنند. در پایین سه الگویی که بیش از همه استفاده می‌شوند را ذکر کرده‌ایم:

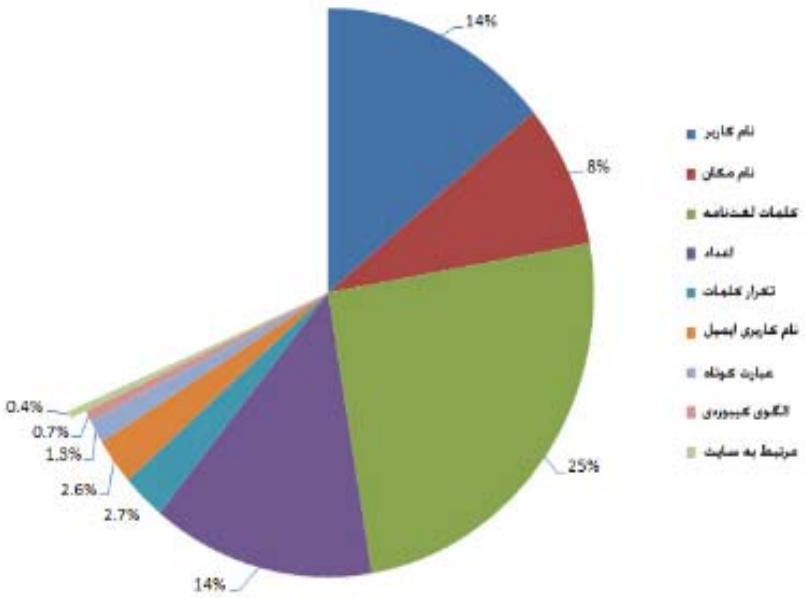
- qwerty
- asdfgh
- asdf1234

تعدادی از این رمزها بسیار خلاقانه و رندم انتخاب و تعدادی از آن‌ها نیز با اعداد ترکیب می‌شوند. در هر صورت باز هم تفاوت چندانی ندارد، چون به هر حال قابل پیش بینی هستند.

مرتبط با وب سایت

با آن که این منبع آمار بسیار کمی را میان کاربران به خود اختصاص داده است، اما ارزش معرفی شدن به عنوان روشی برای انتخاب رمز عبور را دارد .رمزهای عبور مرتبط به سایت، اصولاً مبنی بر لینک، نام یا موارد مرتبط به سایتی هستند که در آن ساخته می‌شوند.

در پایین نسبت استفاده این منبع را با دیگر منابع می‌بینید.



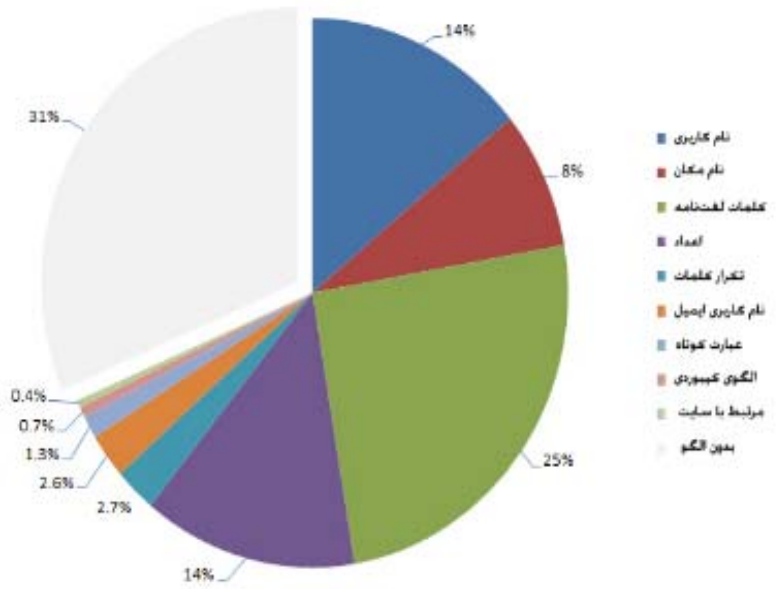
به طور مثال به گزینه پایین توجه کنید:

- نام سایت Gawker :رمز عبورGawker
- نام سایت Sony Pictures :رمز عبورsony123
- نام سایت pron.com : رمز عبورilovepron

همان طور که می‌بینید باز هم با رمزهای عبوری رو به رو هستیم که از کلمات به یادماندنی ساخته شده‌اند. منظور از به یاد ماندنی، کلماتی هستند که به طریقی به خود کاربر، نوع کار او یا حتی سایتی که در آن حساب دارد، مرتبط است. با این روش، احتمال فراموش کردن رمز عبور کاهش می‌یابد. البته رمز عبور مورد نظر به همان اندازه نیز قابل پیش بینی می‌شود. البته بعضی از این کدها همچون گزینه سوم رمزهای عبور بدی نیستند زیرا به نوعی گیج کننده‌اند.

منابع دیگر

آیا منبع دیگری نیز برای استخراج رمز عبور باقی مانده است؟ بله، دسته بزرگی از رمزهای عبور که به علایق شخصی کاربر مربوط هستند و هیچ گونه الگو و شکل ساختاری خاصی ندارند و نمی‌توان برای آن‌ها قالب خاصی تعریف کرد. همان طور که در شکل پایین می‌بینید، حدود ۳۱ درصد از رمزهای عبور حساب‌های کاربری بر اساس همین منبع ساخته شده‌اند. یعنی در واقع بیشترین آمار ساخت رمز عبور، بر اساس هیچ گونه قالب و ساختار خاصی نیست و به سلیقه و علاقه کاربر بر می‌گردد.



در پایین نمونه هایی از این منبع را می‌بینید که توضیحات آن‌ها نیز در جلوی هر کدام نوشته شده است.

- thx1138 نام فیلمی که چهل سال پیش ساخته شده است
- Gundam نام یک سریال کارتونی
- ncc1701 اسم رمز USS Enterprise در استارتِرک

این رمزها به هیچ کدام از دسته بندی‌های ذکر شده در بالا متعلق نیستند و بیشتر به فرهنگ و زندگی کاربر ارتباط دارند.

بیشتر این رمزها قابل پیش بینی نیستند. به طور مثال رمز mw818283 هیچ قاعده خاصی ندارد و پیدا کردن آن، کار زمان بر و خسته کننده ای است.

خلاصه کلام

در انتهای این توضیحات می‌توان به سه نتیجه گیری کلی اشاره کرد:

•رمزهای عبور یا به خود کاربر، شخصیت و نام و کار او بستگی دارند، یا به فرهنگ و علاقه‌اش

•تلاش برای ساختن رمزهای عبور عجیب و غیرقابل دستیابی، اصولاً منجر به استفاده از الگوهای معمول و قابل دسترس می‌شود.

•استفاده از رمزهای عبور رندم و بی قاعده بهترین روش برای امنیت حساب کاربری است. اما تقریباً هیچ کاربری از این روش استفاده نمی‌کند. آمار استفاده از این روش میان کاربران، کمتر از یک درصد است. عملاً یعنی هیچ!

امیدوارم با دانستن این موارد و آگاهی از آمار استفاده از منابع مختلف رمزهای عبور و میزان امنیت آن‌ها، رمز عبور قوی و غیرقابل دسترسی برای حساب کاربری خود بسازید.