منتشر شده در سایت *پلیس فتا* (https://www.cyberpolice.ir)

اجزای یک رمز عبور قوی برای حفظ حریم خصوصی خود

حتما این اصل ساده اما مهم را می دانید که یک رمزعبور باید به قدر کافی مشکل باشد تا یک برنامه کامپیوتری رمزشکن نتواند آن را به راحتی حدس بزند.

* رمزعبور باید طولانی باشد: رمزعبور هر چه طولانی تر باشد، احتمال اینکه یک برنامه کامپیوتری بتواند آن را حدس بزند کمتر می شود. سعی کنید رمز عبورتان حداقل ده حرف داشته باشد. البته بعضی افراد از رمزهایی شامل چند کلمه که با یا بدون فاصله پشت سر هم آورده می شوند، استفاده می کنند که اغلب به آنها عبارتِ رمز گفته می شود. ما نیز توصیه می کنیم تا آنجایی که برنامه یا سرویس مورد استفاده به شما اجازه می دهد، رمزعبور خود را طولانی انتخاب کنید.

* رمزعبور باید پیچیده باشد: علاوه بر طول، پیچیدگی نیز از کشف رمز توسط نرم افزارهای رمزشکن- که ترکیبی تصادفی از حروف را کنار یکدیگر قرار می دهند- جلوگیری می کند. پس در صورت امکان سعی کنید رمزعبور شما شامل حروف بزرگ انگلیسی، حروف کوچک انگلیسی، اعداد و علامت هایی مثل نقطه و کاما باشد. ضمنا یک رمزعبور می بایست به قدر کافی مشکل باشد تا افراد نتوانند آن را حدس بزنند.

* رمزعبور را باید بتوان به خاطر سپرد: اگر شما نتوانید رمزعبور خود را حفظ کنید و آن را جایی بنویسید، احتمالا آن را دو دستی به کسی که به خانه، کیف پول و یا حتی سطل آشغال دفتر شما دسترسی دارد، تقدیم کرده اید. راه های زیادی برای ایجاد و نگهداری رمزهای عبور طولانی که بتوان آنها را حفظ کرد وجود دارد. اما امکان استفاده از نرم افزارهایی مثل «LastPass» که این کار را برای شما به خوبی انجام می دهند، نیز وجود دارد. البته استفاده از نرم افزارهایی مانند Microsoft Word برای این کار مناسب نیست. رمزعبور این فایل ها توسط نرم افزارهای رایگانی که در اینترنت نیز پیدا می شوند قابل بازیابی است.

* رمزعبور نباید شخصی باشد: رمزعبور نباید هیچ ارتباطی با شخصیت شما داشته باشد، بنابراین از انتخاب کلمات یا عباراتی که قسمتی از اطلاعات شخصی شما هستند مانند نام، شماره کارت ملی، شماره تلفن ها، اسم فرزندان، روز تولد یا هر چیزی که ممکن است افراد دیگر درباره شما بدانند، پرهیز کنید.

* رمزعبورتان را مخفی نگه دارید: همیشه هنگام وارد کردن رمزعبور به افرادی که ممکن است آن را از روی شانه شما بخوانند توجه کنید. همچنین به جز در موارد کاملا ضروری رمزعبور خود را به هیچ کس نگویید. اگر هم مجبور بودید که آن را به دوست، هم کلاسی یا یکی از اعضای خانواده بگویید، ابتدا آن را به یک رمزعبور موقتی تغییر دهید و به شخص مورد نظر بدهید. پس از اتمام کار، آن را به حالت قبل بازگردانید. البته، اغلب اوقات راه های دیگری مانند ایجاد یک رمز عبور جداگانه در حساب خود وجود دارد که در صورت امکان بهتر است از این روش ها استفاده کنید. یک رمزعبور می بایست به گونه ای انتخاب گردد که اگر کسی آن را دانست، حداقل ضرر را برایتان به همراه داشته باشد.

* رمزهای عبور نباید یکسان باشند: از یک رمز عبور برای بیش از یک حساب استفاده نکنید، زیرا اگر کسی آن را بفهمد به تمام اطلاعات شما دسترسی پیدا خواهد کرد. فرض کنید رمزعبور کامپیوتر و ایمیل شما یکسان است، حال اگر کسی بتواند کامپیوتر شما را «هک» کند یا به طریقی رمز آن را بدست آورد، به ایمیل شما نیز دسترسی خواهد داشت.

* رمزهای عبور را به صورت دوره ای عوض کنید: توصیه می شود رمز عبور خود را به طور منظم حداقل هر 3 ماه یک بار عوض کنید. زیرا به مرور زمان احتمال اینکه دیگران رمز عبور شما را بفهمند، افزایش می یابد . همچنین اگر کسی بدون اطلاع شما رمزعبورتان را دزدیده باشد تا زمانی که آن را عوض نکنید، از رمزعبور استفاده می کند.

چند راه خوب برای ساختن رمزهای عبور مطمئن

برای ساختن رمزعبور، بهتر است از کاراکترهای متنوع و روش های مختلف استفاده کنید. برای مثال:

* حروف بزرگ و کوچک
* حروف و اعداد
* مخلوط کردن بعضی علامت ها
* استفاده از چند زبان

استفاده از این روش ها پیچیدگی و امنیت رمزعبور را بالا می برد، اما آن را کاملا بی معنی و غیر قابل حفظ کردن نمی کند. حتی استفاده از بعضی از راه های شایع مثل بکار بردن 0 (صفر) به جای حرف O یا علامت @ به جای حرف a هم ایده خوبی است، زیرا این کار حداقل، زمان پیدا شدن رمز عبور توسط نرم افزار رمزشکن را افزایش می دهد یا آن را برای افراد معمولی غیر قابل حدس زدن می کند.

رمزهای عبور را می توان با علامت های جایگزین رایج (مثل مخفف ها) به عبارات پیچیده و عجیب تبدیل کرد.

برای ما راحت تر است که ابتدا جملات خود را به صورت فینگلیش بنویسیم و بعد روی آن تغییراتی را انجام بدهیم.
کار یک نرم افزار رمزشکن این است که حروف مختلف را با هم ترکیب کرده و آنها را در محل رمز عبور قرار می دهد تا از طریق آزمون و خطا، رمزعبور را بیابد. نویسندگان این برنامه ها می دانند که اکثر افراد از یک کلمه معنی دار برای رمزعبور خود استفاده می‌کنند، به همین دلیل برنامه خود را به گونه ای آماده می کنند تا ابتدا کلماتی را که در لغت نامه قرار دارد، امتحان کند. خب، نکته مثبت برای ما فارسی زبانان این است که اکثر این نرم افزارها برای زبان انگلیسی و لغات آن طراحی می شوند، پس توصیه می شود برای رمز عبور خود، به جای انگلیسی از فینگلیش استفاده کنید. البته راه عالی دیگری نیز وجود دارد. فرض کنید در حین وارد کردن رمز، کسی مخفیانه به کیبورد (صفحه کلید) شما نگاه می کند. اگر کلمه ای که شما می زنید یک کلمه‌ی انگلیسی یا فینگلیش باشد او به راحتی آن را متوجه می شود، چون معمولا افراد به حروف انگلیسی کیبورد توجه می کنند. اما انتخاب دیگری نیز پیش روی شماست، کلمه خود را فارسی تایپ کنید! احتمالا برای همه ما پیش آمده که می خواهیم در محلی یک کلمه فارسی بنویسم و بعد از اینکه آن را می نویسیم متوجه می شویم که زبان نوشته انگلیسی بوده و ما انگلیسی تایپ کرده ایم.

در اینجا ما با توجه به حروف فارسی روی کلیدهای کیبورد کلمه فارسی مورد نظرمان را تایپ می کنیم، اما چون زبان سیستم عامل روی انگلیسی است، حروفی که در محل وارد کردن رمزعبور تایپ می شوند نیز انگلیسی خواهند بود. البته هنگامی که قرار بر استفاده از یک صفحه کلید بدون برچسب فارسی باشد (!) مساله بسیار سخت می شود.

این ها فقط چند راه ساده برای پیچیده کردن و در عین حال قابل حفظ ماندن رمزهای عبور هستند، بدیهی است که شما می توانید از روش‌های ابداعی خود برای این کار استفاده کنید.

سوالات امنیتی
در موارد زیادی در زمان ایجاد حساب کاربری مانند ثبت نام یک ایمیل جدید، شما امکان تعریف یک سوال امنیتی را دارید که در موارد خاص با پاسخ دادن به این سوال هویت خود را برای سرویس دهنده اثبات می کنید. این سوالات امنیتی اگر چه معمولا به چشم نمی آیند و برای انتخابشان وسواسی خرج نمی شود، اما از اهمیت بسیار بالایی برخوردارند. حتی زمانی که شما درون گوگل به دنبال سوالات امنیتی مناسب می گردید در موارد زیادی با نمونه های بسیار ضعیفی روبرو می شوید که استفاده از آن ها و موارد مشابه آن بسیار خطرناک است.

یک سوال امنیتی خوب باید این خصوصیات را داشته باشد:

1. به راحتی به خاطر سپرده شود و یادآوری آن هم ساده باشد، به طوری که حتی طی ۱۰ تا ۱۵ سال آینده آن را فراموش نکنید.
2. سوالی باشد که بتوان جواب های مختلفی را برای آن تصور کرد. سوالی با ۱۰۰۰ جواب ممکن که فقط یکی از آن ها درست باشد چطور است؟
3. سوالی نباشد که در مصاحبه یا نظر سنجی به آن پاسخ داده باشید.
4. جوابش در یک یا دو کلمه خلاصه شود.
5. هرگز تغییر نکند

مواردی که به هیچ وجه انتخاب مناسبی نیستند:

1. غذاهای مورد علاقه یا رنگ یا هر چیزی از علایق شخصی که در طول زمان تغییر می کنند.
2. مدل و یا زمان ساخت اتومبیل تان، زیرا برای یک خوره ماشین، تشخیص مدل و سال ساخت آن از روی عکس اش چندان سخت نخواهد بود.
3. تاریخ تولد: سوالات در این رابطه به دلیل سادگی یافتن جواب و وجود شبکه های اجتماعی مختلف که مرتبا تاریخ تولد شما را به همه یاد آوری می کنند غیر قابل استفاده اند.
4. اسم و یا تاریخ تولد افراد خانواده: وقتی که افراد خانواده تان هم در شبکه های اجتماعی عضو هستند و در لیست دوستان تان هم قرار دارند،

تنها کسی که مشخصات شناسنامه ای آنها را نمی داند خواجه حافظ شیرازی است.

5. نام مدرسه و یا محل زندگی: پیدا کردن محل زندگی افراد و طبیعتا محل تحصیل آنها کار چندان دشواری نیست و به راحتی می‌توان چند احتمال قوی را مشخص و امتحان کرد.

6. نام اولین شغل و یا نام موسسه ای که در آن مشغول شده اید: با کمی پرس و جو در خصوص محل تولد و زندگی تان، تنها تعداد محدودی شغل در لیست هکر محترم باقی می مانند که یک فرد می تواند به عنوان اولین کار انتخاب کند.

7. سوالاتی از قبیل، چه رنگی است؟ رنگ های بسیار زیادی وجود دارد اما شما حتما یک رنگ مشخص از آن وسیله را دارید. به عنوان مثال: عکس ماشین تان در فیس بوک وجود دارد و همه از رنگِ آن مطلع هستند.

امنیت کسب و کار | سواد رسانه‌ای | امنیت رمز عبور | رمز عبور | حري

منبع آدرس https://www.cyberpolice.ir/learning/3261 **URL:**