" انتخاب و محافظت از کلمات عبور "

کلمات عبور بخش مهمی از امنیت کامپیوتر هستند و در حقیقت در خط مقدم حفاظت از Account 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 می شود. در حقیقت مخاطب این گزارش تمام افرادی هستند که مسئول Account 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.

۱. تمام کلمات عبور سطح کاربر (مانند e-Mail یا کامپیوتر) باید هر شش ماه تغییر کنند که البته تغییر چهار ماهه توصیه می شود.
۲. Account های کاربری که مجوزهای سطح سیستم دارند باید کلمات عبوری داشته باشند که با کلمات عبور دیگر Account های آن کاربر متفاوت باشد.
۳. کلمات عبور نباید در e-Mail یا سایر شکلهای ارتباطات الکترونیکی درج شوند.
۴. باید رهنمونهای زیر در تمام کلمات عبور سطح سیستم و سطح کاربر رعایت شود.

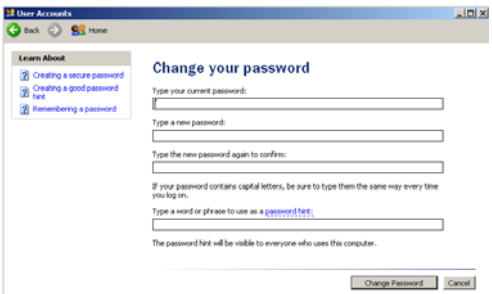
راهنمائیها :

۱. راهنمایی کلی ساخت کلمه عبور

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

- ✓ Account های سطح کاربر
- ✓ Account های دسترسی به وب
- ✓ e-Mail Account
- ✓ حفاظت از مونیتور
- ✓ کلمه عبور Mail Box
- ✓ ورود به Router محلی

چون سیستمهای بسیار کمی از نشانه های یکبار مصرف استفاده می کنند (مانند کلمات عبور Dynamic که فقط یکبار استفاده می شوند)، هر کسی باید از نحوه انتخاب کلمات عبور مناسب آگاه باشد.



کلمات عبور ضعیف معمولا مشخصات زیر را دارند:

۱. کلمه عبور شامل کمتر از هشت حرف است.

۲. کلمه عبور کلمه ای است که در یک فرهنگ لغت یافت می شود.

۳. کلمه عبور کلمه ای است که کاربرد عمومی دارد مانند:

- ✓ نام خانوادگی، حیوانات اهلی، دوستان، همکاران، شخصیت های خیالی و غیره
- ✓ نامها و اصطلاحات کامپیوتری، فرمانها، سایتها، شرکتها، سخت افزار و نرم افزار.
- ✓ نام شرکت یا کلمات مشتق شده از این نام.
- ✓ تاریخ های تولد و سایر اطلاعات شخصی مانند آدرس ها و شماره های تلفن.
- ✓ الگوهای کلمات یا شماره ها مانند aaabbb، qwerty، zyxwvuts، 123321 و غیره.
- ✓ هرکدام از عبارات فوق بطور برعکس.
- ✓ هرکدام از عبارات فوق که تنها با یک رقم شروع یا به آن ختم می شود.

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 استفاده‌می‌شود مانند 0-9 و !@#$%^&*()_+|~=’{}[];<>?./
- ✓ حداقل هشت حرف دارند.
- ✓ کلمه ای در هیچ زبان، گویش یا صنف خاص نیستند.
- ✓ برپایه اطلاعات شخصی، اسم یا فامیل نیستند.
- ✓ کلمات عبور هرگز نباید نوشته یا جایی ذخیره شوند. سعی کنید کلمات عبوری انتخاب کنید که بتوانید براحتی 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.

۲. استانداردهای حفاظت از کلمه عبور:

از کلمات عبور مشترک برایAccount های شرکت و دسترسی های 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 Account های NT و UNIX کلمات عبور متفاوت انتخاب کنید.

کلمات عبور شرکت با هیچ کس از جمله دستیاران و منشی ها در میان نگذارید. باید با تمام کلمات عبور بصورت اطلاعات حساس و محرمانه برخورد شوند.

در اینجا به لیستی از "انجام ندهید" ها اشاره می شود.

- ✓ 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 (مثلا نام خانوادگی)
- ✓ کلمه عبور را روی فهرست سوالات 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.

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

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

اگر هر Account 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 نمایندگی های آن رخ دهد. اگر کلمه عبور در طول یکی از این پیمایش ها 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.