رعایت اصول و نکات امنیتی در استفاده از سامانه گلستان

با توجه به اهمیت و حساسیت اطلاعات و دقت بیشتر درحفظ امنیت سامانه گلستان، رعایت برخی از نکات می تواند تاثیر بسزایی در افزایش امنیت آن داشته باشد. خواهشمند است کاربران محترم با سطح دسترسی بالا در سامانه گلستان به توصیه های امنیتی ذیل توجه نمایند:

۱. نام کاربری و کلمه عبور خود را با دقت انتخاب و به طور مداوم تغییر دهید.

توجه داشته باشید نام وکلمه عبور شما توانایی شما را در کار با برنامه تعریف می کند و داشتن این اطلاعات توسط شخصی دیگر بیانگر این است که آن شخص نیز معادل شما توانایی انجام کار خواهد داشت. کلمه عبور(رمز ساده)، کوتاه، قابل حدس و رمزهایی که به مدت طولانی (بیش از یک ماه) استفاده می شوند همواره شما را با خطرات امنیتی مواجه کرده یا ضریب امنیتی شما را پایین می آورند. پس ضروری است رمز خود را بطور مداوم تغییر داده و از بکار بردن کلمه عبور(رمزهای ساده) که بسادگی قابل حدس باشند، مانند(نام خودتان، سال تولد، شماره شناسنامه ،تلفن همراه و...) خودداری نمایید. پیشنهاد می شود کلمه عبور(رمز) بیش از ۶ کاراکتر و بصورت ترکیب حرف(بزرگ وکوچک)،کاراکتر و اعداد باشد. مثال یک رمز ضعیف کلمه" **saeed** " یا " ۱۲۳۶۵۴ " و مثال یک رمز قوی "**A@#93kd>** " یا " **s82%GL10** " می باشد.

۲. از کلمه عبور(رمز) خود بخوبی مراقبت کنید.

هیچگاه رمز خود را طوری یادداشت نکنید که در معرض دید یا دسترس دیگران باشد. بسیاری از مواقع مشاهده می شودکاربران رمز خود را به مانیتور می چسبانند و یا زیر شیشه میز قرارمیدهند. در این حالت رمز شما به راحتی در دسترس دیگران قرار گرفته و احتمال خطراتی که نهایتا به نام شما تمام خواهد شد بسیار بالا می رود. اگر برای جلوگیری از فراموشی رمز خود را یادداشت می کنید از مناسب و ایمن بودن محل نگهداری آن کاملا اطمینان حاصل نمایید و تا جاییکه که امکان دارد از یادداشت کد کاربری و رمز عبور خود جلوگیری نموده و تلاش کنید آن را حفظ نمایید. بهتر است برای اینکه رمز خود را به یاد داشته باشید از تکنیک های دیگری نیز استفاده نمایید. روشهایی مانند انتخاب کلمات اول یک جمله بطور مثال رمز" **msnir** " با استفاده از حروف اول عبارت **My son name is Reza** که می تواند با استفاده از حروف بزرگ و اضافه شدن اعداد و کاراکترها قوی تر شود " **mSniR8$**٪#". واضح است که جملات اینچنینی بسادگی در ذهن ماندگار هستند.حتی یک

جمله می تواند رمز شما باشد به شرطی که با گرفتن کلید Shift قسمت هایی از آن را با حروف بزرگ بنویسید تا از سادگی خارج شود. مثال: " It's a Good Idea! "

می توانید با استفاده از کاراکترهای مشابه رمز خود را پیچیده کنید در حالی که رمز همچنان قابلیت بیاد ماندن را دارد.بطور مثال رمز it is a good day را در نظربگیرید.می توانید آنرا اینگونه بنویسید " 1t 1$ @ g00d d@y " که بجای I از عدد ۱ و بجای a از @ و بجای S از $ بجای o از عدد صفر 0 استفاده شده است.

هرگز از بکارگیری یک رمز در چند جا استفاده نکنید.توجه داشته باشید که برای برنامه های مختلف رمزهای متفاوتی داشته باشید.چرا که اگر رمز شما لو برود شما چیزهای زیادی برای ازدست دادن دارید.

۳. کامپیوتر خود را در هنگام باز بودن برنامه، رها نکنید.

هیچگاه درحالی که برنامه روی کامپیوتر شما اجرا شده و باز است کامپیوتر خود را رها نکنید.این کار خطرات امنیتی زیادی بهمراه دارد. در فاصله زمانی که شما در پشت کامپیوتر خود نیستید ممکن است شخص دیگری با برنامه کار کند و تغییراتی را انجام داده و یا مسیر را برای سوء استفاده های بعدی خود فراهم نماید. درجه این خطرات با توجه به میزان دسترسی شما از متوسط تا خیلی زیاد خواهد بود. کاربرانی که از دسترسی بالا برخوردارند در این خصوص دقت بیشتری نمایند.علاوه بر حضور دانشجویان و افراد ناشناس در محل کار توجه نمایید که اگر چه همه همکاران محترم هستند ولی ممکن است در این زمان کاری را انجام دهند که بنام شما ثبت شود و عواقب این کار با مسئولیت شما تمام شود. بنابراین هنگام ترک کامپیوتر از برنامه خارج شده و ویندوز کامپیوتر خود را با انتخاب گزینه های Ctrl+delete و کلید Lock Computer قفل (Lock Computer) نمایید.(یا دکمه "ویندوز+L " را بزنید)

۴. بعد از اتمام کار از برنامه خارج شوید.

حتما پس از پایان کار از برنامه خارج شوید(لازم به ذکر است جهت حفظ امنیت در سامانه مدت زمان بیکاری معینی، در این خصوص تعریف شده که بلافاصله و به طور خودکارپیام "بعلت عدم کار کردن با سیستم قادر به انجام کار نخواهید بود" صادر می شود). به این ترتیب ارتباط شما با سرور قطع شده احتمال سوء استفاده از طریق شبکه گرفته شده و احتمال سوء استفاده از کد کاربری شما در غیاب شما کاهش می یابد. دقت نمایید همیشه بزرگترین مشکلات امنیتی از طریق کوچکترین سهل انگاری ها رخ می دهند.

۵. نام و کلمه عبور خود را در اختیار دیگران قرارندهید و از روی کامپیوترهای ناشناس وارد برنامه نشوید.

به هیچ وجه رمز خود را در اختیار دیگران قرارندهید. این کار مشکلات امنیتی زیادی را بهمراه خواهد داشت.

۶. از اجرای فایل های نامطمئن در سیستم خود، خودداری نمایید.

هیچ فایل و نرم افزار نامطمئنی را در سیستم خود دانلود واجرا نکنید.در این شرایط احتمال دانلود یک کد مخرب و سپس اجرای مستقیم آن در رایانه توسط خود شما بسیار بالاست.

۷. بررسی منظم امنیت کامپیوتر و استفاده از آنتی ویرو سها

نحوه استفاده از آنتی ویروس ها و به روز رسانی آنها و همچنین بررسی پیکر بندی امنیتی مرور گرها و حصول اطمینان از تنظیمات سطوح امنیتی از جمله موارد ضروری و با اهمیت در حفظ امنیت کامپیوتراست.

۸. استفاده از سخت افزارهای امنیتی در صورت نیاز (مانند توکن)

توکن امنیتی، سخت افزاری کوچک است که برای ورود کاربر به یک سرویس رایانه ای به سامانه بکار می رود. به عبارت دیگر این دستگاه یک دستگاه فیزیکی است که در اختیار کاربران مجاز قرار می گیرد تا به راحتی بتوانند برای استفاده از یک سیستم کامپیوتری هویت آنها بصورت الکترونیکی تشخیص داده شود و سوء استفاده های احتمالی جلوگیری بعمل آید.