دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سپرجند

حراست

امنیت پست الکترونیکی

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

ارتباطات رسمی و حتی غیر رسمی بسیاری از افراد از طریق ایمیل بر قرار می شود . نکاتی از جمله رمز عبور مناسب برای آدرس ایمیل ، از نکات اولیه محافظت از ایمیل و جلوگیری از دسترسی های غیر مجاز به صندوق پست الکترونیک به شمار می رود . لازم است رمز عبور ایمیل خود را حد اقل سالی دو بار عوض کنید . تعویض رمز عبور را با ترکیبی از حروف ، اعداد و علامت های خاص انجام دهید و هرگز از کلماتی که در فرهنگ های لغت موجود هستند ، برای رمز عبور خود استفاده نکنید . همچنین در کنار آن لازم است از عدم وجود نرم افزار های جاسوسی ، تروجان و سایر بد افزار های احتمالی که می توانند اطلاعات ما را به یغما ببرند ، مطمئن شوید. اسکن سیستم توسط نرم افزار های ضد جاسوس افزار و ضد ویروس ، برای اطمینان از این مورد توصیه می شود . افراد بسیاری از سرویس های رایگان ایمیل شرکت های بزرگی همچون یاهو و گوگل و م ایکروسافت استفاده می کنند . اما توصیه می شود جهت امنیت بیشتر پست الکترونیکی تان از سرویسی استفاده کنید که از SSL (secure sockets layer) بهره می برد و حتی الامکان سرویس دهنده آن در داخل کشور و یا کشورهایی که خصومتی با کشورمان ندار ند قرار داشته باشد ، مانند سرویس دهنده mail.iran.ir و یا سرویس دهنده چاپار به آدرس www.chmail.ir برای اینکه مطمئن شوید سرویسی که از آن استفاده می کنید از SSL برای برقراری ارتباطات رمزنگاری شده و امن ، بهره می برد هنگامی که صندوق پست الکترونیکی خود را باز می کنید به قسمت address Bar مرورگر خود توجه کنید . چنانچه آدرس صفحه مربوطه با https شروع شود ، سرویس مربوطه از ارتباط امن بهره می برد.

دقت کنید که لازم است صفحه ورود به صندوق پست الکترونیک شما نیز مبتنی بر https و رمز نگاری شده باشد . بدین ترتیب از رمز عبور شما نیز حفاظت می شود .

اسپم

اسپم ها ، ایمیل های نا خواسته ای هستند که اغلب با عناوین و متون تبلیغاتی و اغوا کننده در صندوق ورودی شما ظاهر می شوند . برای اینکه از شر اسپم ها در امان بمانید لازم است آدرس ایمیل خود را در هر فرم و لیستی قرار ندهید . همه لیست ها و فرم هایی که ایمیل شما را درخواست می کنند ، امنیت لازم را ندارند و ممکن است در واقع اسپمرهایی خودکار باشند . در صورت بی توجهی ، ایمیل خود را به اسپمر تحویل داده اید . برای ثبت نام در این فرم ها از ای میل هایی موقت استفاده کنید . همچنین می توانید ایمیلی را به همین منظور برای خود ایجاد نمایید و از آن استفاده کنید

با ایمیل های اسپم چگونه برخورد کنیم :

اگر ایمیلی دریافت کردید که مطمئن هستید اسپم است در مرحله اول ترجیحا به هیچ وجه آن را باز نکنید و چنانچه به اشتباه ایمیل را باز کردید ، به هیچ وجه به آن پاسخ ندهید. بهتر است با کلیک بر روی کلید Spam آن را به پوشه اسپم انتقال دهید و یا آن را پاک نمایید . در صورتی که اسپمی فایل ضمیمه ای را شامل می شد ، تحت هر شرایطی از دانلود آن اجتناب کنید .

فایل های ضمیمه و تصاویر

در مورد فایل های ضمیمه و تصاویر در ایمیل های دریافتی خود با احتیاط بر خورد کنید . در مرحله اول سیستم دانلود خودکار فایل های ضمیمه را در ایمیل خود غیر فعال نمایید . تا حد امکان از دانلود فایل های ضمیمه ای که منتظر دریافت آنها نیستید خودداری نمایید . حتی اگر دوستان یا همکاران تان در ایمیل شان فایلی را ضمیمه کرده و توضیحی در مورد آن نداده اند ، آن را تا حصول اطمینان دانلود نکنید . همچنین پس از دانلود فایل های ضمیمه شده به ایمیل های دریافتی ، آنها را قبل از باز کردن توسط آنتی ویروس اسکن کنید.

ضمنا نما یش تصاویری که در متن ایمیل ها وجود دارند را در حالت عادی غیر فعال کنید و ترجیحا اجاز نمایش تصاویری که در متن ایمیل قرار دارند را ندهید .

به روز رسانی سیستم عامل ، مرورگر و نرم افزار ها

برای اطمینان از امنیت ایمیل ، به روزرسانی مرتب و مکرر سیستم عامل ، مرورگر و نرم افزار های مورد استفاده در سیستم اهمیت ویژه ای دارند . بسته های به روز رسانی معمولا آخرین حفره های امنیتی نرم افزار ها را پوشش می دهند و از سوء استفاده هکر ها از این اشکالات پیش گیری می کند. به همین جهت لازم است در جهت افزایش امنیت ایمیل از به روز بودن کامپیوتر ، اطمینان حاصل کرد