# اقدامات امنیتی کاربران شبکه اینترنت دانشگاه

۱- مرکز فناوری اطلاعات تحت هیچ عنوان نیازی به اطلاعات کاربری پست الکترونیک شامل نام کاربری و کلمه عبور و سایر اطلاعات دیگر ندارد، لذا به اینگونه ایمیلها پاسخ نداده و بر روی لینکهای موجود در نامه کلیک نکنید بلکه آنها را تحت عنوان اسپم یا جانک به سیستم معرفی نمایید.

۲- از باز کردن فایلهای ضمیمه مشکوک در ایمیل خودداری نمایید.

۳- بصورت مرتب کلمات عبور خود در کلیه سامانه های الکترونیکی دانشگاه و دیگر سامانه های موجود در شبکه اینترنت را تغییر دهید.

۴- تحت هیچ عنوان کلمات عبور خود را در اختیار سایر کاربران قرار ندهید.

۵- هیچگاه از عبارات ساده و اعدادی مانند ۱۲۳۴۵۶ جهت رمز عبور استفاده ننمایید.

۶- هیچگاه از شماره موبایل، تلفن، کد ملی، شماره شناسنامه، سال تولد، نام، نام خانوادگی و امثال آن به عنوان کلمه عبور استفاده ننمایید.

۷- به هیچ عنوان رمز عبور خود را نام کاربری قرار ندهید. رمز عبور با نام کاربری یکسان نباشد.

۸- رمز عبور خود را از عبارات پیچیده شامل ترکیبی از اعداد، حروف بزرگ، کوچک و کاراکترهای ویژه مانند $, ٪ و ... انتخاب نمایید.

۹- پس از اتمام کار با هر سامانه ای، حتما بر روی گزینه خروج آن سامانه کلیک نمایید.

۱۰- بر روی کامپیوتر خود از یک آنتی ویروس استفاده نموده و مرتب آن را به روز نمایید. نباید تصور شود که کامپیوتری که ویندوز به تازگی روی آن نصب شده آلوده به ویروس نیست و یا آلوده نخواهد شد.

۱۱- فایروال ویندوز و سیستم عاملهای موجود بر روی کامپیوتر خود را فعال نمایید.

۱۲- گزینه Remote desktop بر روی ویندوز و سایر سیستم عاملهای موجود بر روی کامپیوتر خود را غیر فعال نمایید.

۱۳- نرم افزارهای TeamViewer و AnyDesk و مشابه آن باعث نفوذ هکرها و دستیابی به اطلاعات موجود بر روی آن می شوند تا حد ممکن از اینگونه نرم افزارها استفاده ننمایید.

۱۴- در مکانهای عمومی نظیر کافی نت ها از ورود به سامانه های اینترنت بانک خودداری نمایید.

۱۵- همیشه از فایلهای حیاتی و مهم موجود بر روی کامپیوتر خود یک نسخه پشتیبان تهیه نمایید. این امکان وجود دارد که فایلهای سیستمی ویندوز خراب شده و دستیابی به ویندوز و فایلهای حیاتی با مشکل جدی مواجه شود.

۱۶- از Windows update برای بررسی و به روز رسانی سیستم عامل استفاده نمایید. همچنین سایر نرم افزارهای روی کامپیوتر خود را به روز رسانی نمایید.

۱۷- در مورد گوشی های هوشمند علاوه بر استفاده از نرم افزارهای ضد ویروس از دانلود هر برنامه ناشناس و ورود به هر لینکی خودداری نمایید.

۱۸- پس از اتمام کار با کامپیوتر و استفاده از اینترنت حتما کامپیوتر را خاموش نمایید. کامپیوتر های روشن و متصل به شبکه ابزاری برای نفوذ و حمله به دیگر کامپیوترهای موجود در شبکه می باشد.

**مرکز فناوری اطلاعات و امنیت فضای مجازی دانشگاه**