تاریخ : ۱۳۹۵/۰۵/۲۴.....

شماره : د/۲/۸۳۹۲.....

پیوست: دارد.....

بسمه تعالی

اداره فناوری اطلاعات و ارتباطات دانشگاه

کلیه واحدهای تابعه دانشگاه

با سلام و احترام

پس از حمد خدا و درود و صلوات بر محمد و آل محمد (ص)، اخیرا گونه های مختلفی از بدافزارهای مخرب موسوم به ویروس گروگانگیر با هدف رمزنگاری و تخریب اطلاعات رایانه و همچنین محدودسازی دسترسی کاربر به اطلاعات در ادارات و مراکز مختلف استان دیده شده که منجر به تخریب اطلاعات آن مرکز گردیده است و امکان بازگردانی این اطلاعات در مواردی وجود نداشته است.لذا نظر به رویکرد مشابه و نحوه انتشار و عملکرد این بدافزارها و جلوگیری از مخاطرات و سوء استفاده، دستورالعمل ذیل برای مقابله با تهدیدات احتمالی اعلام می گردد.

تذکر: اجرای این دستورالعمل برای تحویل گیرندگان کامپیوترهای شخصی و کلیه سرورهای مستقر در دانشگاه و مراکز لازم الاجراست.

۱- تهیه نسخه پشتیبان از اطلاعات ذخیره شده در مکانی خارج از رایانه یا شبکه

۲- عدم استفاده از افزونه های(add-on) غیرضروی یا ناشناس برروی مرورگرها

۳- نظارت و محدود کردن سطوح دسترسی کاربران به سیستم عامل و منابع شبکه

۴- حذف نرم افزارهای غیرضروری و بلااستفاده از رایانه ها

۵- بررسی فعال بودن گزینه پیش فرض ماکرو در نرم افزارهای آفیس و عدم تایید پیغام امنیتی فعال سازی ماکرو در فایل های ناشناس

۶- نصب و به روزرسانی آنتی ویروس به همراه فایروال (Internet Security)

۷- درصورت امکان از آخرین نسخه مربوط به سیستم عامل و برنامه های کاربردی استفاده شده یا آنها را به روزرسانی نمایید.

۸- به هیچ عنوان ایمل های ناشناس را باز نکنید و اجرای کردن لینک های مشکوک به طور جدی اجتناب کنید.

۹- حتی الامکان از نرم افزارهای قفل شکسته استفاده نکنید.

۱۰-از غیر فعال کردن موقت سرویس های انتی ویروس یا فایروال جدا اجتناب کنید.

در صورت الوده شدن سیستم و فراهم شدن فرصت کافی برای بدافزار، فایل های موجود در رایانه توسط بدافزار رمزنگاری می شود که در بسیاری از موارد کشف کلید یا بازگردانی اطلاعات وجود ندارد(ممکن است حالت یکی از راه ها باج گیری باشد اما هیچ تضمینی برای بازگشت فایل ها وجود ندارد و در مواردی مشاهده شده که از قربانی پس از دریافت باج مجددا پول بیشتری درخواست شده است.بنابراین ضمن جدی گرفتن این بدافزار، پیش بینی های لازم برای مقابله با آن در نظر گرفته شود.

مهندس محمدباقر محبی
سرپرست اداره فناوری
اطلاعات و ارتباطات