تاریخ : ۱۳۹۵/۰۹/۰۹

شماره : ۹۵/د/۲۹۱۸

پیوست : **ندارد**

بسمه تعالی

دانشگاه علوم پزشکی و خدمات بهداشتی درمانی تهران

مدیریت آمار و فناوری اطلاعات دانشگاه

جناب آقای/ سرکار خانم
معاون محترم / رئیس محترم / مدیر محترم

با سلام

احتراماً، با توجه به لزوم دقت پرسنل دانشگاه به مقوله امنیت اطلاعات در استفاده از امکانات رایانه‌ای موجود در مراکز مختلف و با توجه به حملات سایبری اخیر به برخی مراکز توسط بدافزارهای پیشرفته جدید از جمله بدافزار Remsec که توسط دو گروه جاسوسی سایبری حرفه‌ای با نام‌های "Strider" و "Project Sauron" که جهت حمله به اهدافی گزینش شده از بین نهادهای دولتی، مراکز تحقیقاتی و علمی، سازمان‌های نظامی، مخابراتی و مؤسسات مالی ۳۰ کشور از جمله ایران طراحی و منتشر گردیده است، خواهشمند ترتیبی اتخاذ فرمایید که کلیه کارکنان و دست اندرکاران احتیاط و هوشیاری بیشتری داشته و از مفاد این نامه مطلع گردند. برخی از مخاطرات و روش‌های مقابله با بد افزارهای فوق به شرح زیر است:

۱. این بدافزار بیشتر در شبکه‌های سازمانی فعالیت داشته و رایانه‌های فردی مورد هدف نیستند.
۲. از قابلیت‌های این بدافزار، در دست گرفتن کنترل کامل رایانه‌های قربانی و عدم کنترل اپراتور روی سیستم هدف است.
۳. ضبط اطلاعات صفحه کلید کاربر جهت دستیابی به رمزهای عبور از طریق گزارش صفحه کلید و حتی مکان‌یابی نشانگر جهت این هدف از دیگر مخاطرات این بدافزار است.
۴. سرقت فایل‌ها و اطلاعات رایانه‌های حاوی مطالب حساس نظامی، اقتصادی و علمی از دیگر اهداف این بدافزار است.
۵. این بدافزار از توان شناسائی راه‌های فرار و بررسی پروتکل‌های خروجی بهره برده و قادر است پس از جمع‌آوری اطلاعات مورد نیاز از طریق حتی یک دستگاه فلش مموری از شبکه‌های محلی فاقد اینترنت خارج شده و خود را جهت انتقال اطلاعات به اولین ترمینال اطلاعاتی در دسترس بین المللی (اینترنت) برساند.

لذا از این رو جهت امنیت هرچه بیشتر رایانه‌های مورد استفاده در آن مرکز توجه به نکات مشروحه زیر توسط کارکنان و همکاران کلیه واحدهای مستقر الزامی است:

۱. به همه همکاران یادآوری شود که رایانه های مرکز، اموال سازمانی بوده، و استفاده از آنها جز برای استفاده در فعالیتهای دانشگاه شرعاو قانونا مجاز نیست.
۲. عدم استفاده از ویندوز XP و لزوم استفاده از نسخه‌های به روز ویندوز ۷ ,SP1 و بالاتر (خیلی مهم).

آدرس : تهران ، بلوار کشاورز ، نبش خیابان قدس ، ساختمان ستاد مرکزی دانشگاه علوم پزشکی تهران ، ، طبقه دوم اتاق ۲۰۶ تلفن : ۸۱۶۳۳۱۰۲

آدرس پست الکترونیک:itcenter@tums.ac.ir آدرس الکترونیک: http://sit.tums.ac.ir

بسمه تعالی

دانشگاه علوم پزشکی
و خدمات بهداشتی درمانی تهران
مدیریت آمار و فناوری اطلاعات دانشگاه

۳. استفاده از نسخه ۱۰،۲،۴ و بالاتر آنتی ویروس کسپرسکی روی کلیه رایانه‌ها (خیلی مهم).

۴. عدم استفاده از هرگونه حافظه قابل حمل یا دیسک فشرده ناشناس یا غیر قابل اطمینان.

۵. عدم اتصال گوشی‌های تلفن همراه به رایانه‌های مرکز (خیلی مهم).

۶. عدم گشودن لینک‌های نا مطمئن در ایمیل‌ها و صفحات وب.

۷. عدم استفاده از شبکه‌های اجتماعی روی رایانه‌های مرکز.

۸. عدم گشودن ایمیل‌های ناشناس روی رایانه‌های مرکز.

۹. عدم نصب هرگونه نرم افزار متفرقه و غیر اداری روی سیستم‌ها.

۱۰.عدم استفاده از صفحات وب دارای محتوای غیر قانونی همانند سایت‌های ارائه کننده کرک و سریال برنامه‌ها و فیلم‌ها و سریال‌های دارای حق کپی رایت.

۱۱. از به روز بودن آنتی ویروس رایانه های مورد استفاده دانشجویان در کتابخانه ها، سالن های کامپیوتر و مانند آن اطمینان حاصل گردیده، و ترتیبی اتخاذ شود که این گروه از رایانه ها، از رایانه های سازمانی ایزوله گردد.

۱۲.به عدم اطمینان شبکه های بی سیم توجه نموده و حتی الامکان برای اتصال به سامانه های دانشگاهی از رایانه های رومیزی استفاده شود.

در خاتمه یادآور میشود، همه همکاران موظفند وقوع هر نوع مخاطراتی از این دست را سریعا به مسئولین مربوطه از جمله پست الکترونیک itcenter@tums.ac.ir گزارش نمایند.