توصیه‌های حفاظتی در استفاده از رایانه‌های اداری دانشگاه رازی

حوزه فناوری اطلاعات و امنیت فضای مجازی

دی ماه ۱۴۰۲

۱. **ایجاد کلمه عبور (پسورد) برای ورود به سیستم متصل به شبکه دانشگاه**

برای سیستم کلمه عبور تعیین کرده و آن را طوری تنظیم نمائید که در صورت عدم استفاده از آن به مدت (حداکثر) پنج دقیقه از شما کلمه عبور درخواست نماید. این کار مانعی برای دسترسی دیگران به سیستم شما خواهد بود و تا حدودی امنیت را افزایش می‌دهد.

۲. **از رمز عبور ساده و مشخص استفاده نکنید.**

سعی کنید رمز عبورهای سیستم خود را پیچیده و غیرقابل پیش‌بینی انتخاب کنید. انتخاب رمز عبور با کاراکترهای زیاد، با حروف و اعداد، حروف کوچک و بزرگ و یا انتخاب آن به زبان دیگر، می‌تواند امنیت سیستم شما را افزایش دهد.

۳. **در صورت ترک محل کار (حتی برای بازه زمانی کوتاه) حتماً سیستم خود را قفل نمایید.**

در صورت باز گذاشتن سیستم پس از ترک محل کار، امکان دسترسی ارباب رجوع‌ها و یا افراد سوءاستفاده‌گر به سیستم شما فراهم خواهد شد و در بازه‌ای که شما حضور ندارید می‌توانند اطلاعات سیستم شما را به سرقت ببرند و یا اقدام به خراب‌کاری نمایند.

٤. **بلاک شدن رایانه اداری در صورت استفاده از یوزر اینترنت سایر همکاران.**

استفاده از نام کاربری اینترنت متعلق به شخص دیگر، سبب بلاک شدن اتصال رایانه به شبکه اینترنت دانشگاه بمدت یک هفته می شود.

۵. **در مواقع غیرضروری سیستم خود را به شبکه اینترنت متصل ننمائید.**

در مواقعی که نیازی به ارتباط با اینترنت ندارید، آن را قطع نمائید تا از گزند هکرها و جاسوسان اینترنتی و عوامل بیگانه در امان باشید. هکرها توانائی فعال‌سازی میکروفون و دوربین (وب‌کم) شما را بدون توافق با شما دارند. لذا با توجه به متصل بودن بی‌مورد و طولانی مدت سیستم شما به اینترنت این‌گونه خطرات همواره متصور است.

٦. **از رایانه‌ای که دارای اطلاعات محرمانه و یا اطلاعات خصوصی است، برای متصل شدن به اینترنت استفاده نکنید.**

همیشه در هنگام متصل شدن به اینترنت خطر سرقت اطلاعات و تخریب اطلاعات به‌صورت جدی وجود داشته و در صورت بی تفاوتی به این مطلب خطرات جبران‌ناپذیری سیستم و اطلاعات شما را تهدید می‌کند.

۷. **رایانه خود را که حاوی اطلاعات اداری، محرمانه یا خصوصی است، جهت تعمیر به افراد متفرقه و ناشناس ندهید.**

حتماً تعمیر رایانه خود را به نماینده حوزه فناوری اطلاعات مستقر در محل بسپارید.

۸. **هرگز قطعات آسیب‌دیده رایانه (مانند: هارد، سی دی و ...) را دور نیاندازید.**

حتماً این‌گونه لوازم از کار افتاده را منهدم کرده و امکان بهره‌برداری مجدد را از آن‌ها بگیرید. اغلب رایانه‌های مستعمل و از رده خارج شده دارای اطلاعات ارزشمندی است که در هنگام تعویض یا فروش، بر اثر سهل‌انگاری در سیستم‌ها باقی مانده است. هم‌چنین امکان بازیافت اطلاعات از حافظه‌های پاک شده سیستم وجود داشته و صرف پاک کردن یا فرمت کردن سیستم نمی‌توان از پاک شدن صد در صد آن‌ها اطمینان داشت. بنابراین بعضی از افراد تصور می‌کنند با پاک کردن هاردهای مستعمل تمام اطلاعات آن‌ها از بین رفته و می‌توانند آن‌ها را دور ریخته یا به فروش برسانند.

۹. **هرگز از رایانه اداری متصل به شبکه و اینترنت دانشگاه، برای کارهای متفرقه استفاده ننمائید.**

استفاده از نرم‌افزارهای متفرقه غیراداری خطر آسیب‌پذیری رایانه و نفوذ به شبکه دانشگاه را افزایش داده و متصدی رایانه باید پاسخگوی مخاطرات باشد.

در نظر داشته باشید که مودم، پرینتر، اسکنر و بعضی از اجزای داخلی رایانه «آی- پی» پذیر بوده و می‌توانند اطلاعات خود را به آدرس برنامه‌ریزی شده از طریق اینترنت ارسال کنند. بنابراین ممکن است نامه‌ای که تایپ کرده و پرینت گرفته‌اید و حتی از رایانه خود پاک کرده‌اید، بعد از آن‌که به اینترنت متصل می‌شوید، به آدرس برنامه‌ریزی شده ارسال گشته بدون آن‌که شما از آن مطلع گردید.

۱۰. **نسبت به محافظت و نگهداری نسخه ذخیره اطلاعات (backup) بی‌تفاوت نباشید.**

به منظور محافظت از اطلاعات و پیش‌گیری از تخریب آن‌ها، اقدام به تهیه نسخه‌های ذخیره (پشتیبان) ضروری است. حفاظت و نگهداری این نسخه‌ها حتی از اطلاعاتی که در سیستم‌ها نگهداری می‌شوند با اهمیت‌تر می‌باشد. زیرا این اطلاعات به‌صورت آماده و بدون دردسر بوده و سهل‌انگاری در نگهداری از این نسخه‌های ذخیره بعضاً معضلات جبران‌ناپذیری در بر خواهد داشت.

۱۱. **هرگز نسبت به تهیه نسخه ذخیره از اطلاعات درون رایانه خود مسامحه نکنید.**

رایانه‌ها ابزار قابل اطمینانی نیستند و همواره احتمال صدمه دیدن آن‌ها متصور است لذا همیشه سعی کنید از اطلاعات داخل سیستم خود یک نسخه ذخیره (روی فلش یا حافظه کلاد) داشته باشید تا در صورت بروز هرگونه اختلالی اطلاعات شما در اختیارتان باشد.

۱۲. **آنتی‌ویروس مطمئن نصب کنید.**

ویروس‌ها و بدافزارهای کامپیوتری همه‌جا حضور دارند. برنامه‌های آنتی‌ویروس از رایانه شما در برابر کدهای مخرب یا نرم‌افزارهای غیرمجازی که ممکن است سیستم‌عامل شما را تهدید کنند، محافظت می‌کنند. همچنین ویروس‌ها ممکن است پیامدهای مخربی برای شما داشته باشند. نرم‌افزار آنتی‌ویروس با شناسایی تهدیدات مختلف، نقش مهمی در محافظت از امنیت کامپیوتر شما ایفا می‌کند. برخی از برنامه‌های آنتی‌ویروس پیشرفته به‌روزرسانی‌های خودکار را ارائه می‌کنند و از دستگاه شما در برابر ویروس‌های جدیدی که همه روزه ظاهر می‌شوند محافظت می‌کنند. خط مقدم محافظت از امنیت کامپیوتر شما، استفاده از آنتی ویروسی است که قابلیت اطمینان بالایی داشته باشد و مدام به‌روزرسانی شود.

۱۳. تلفن همراه خود و حافظه‌های فلش مشکوک را حتی‌المقدور به رایانه‌های اداری متصل نکنید.

گاهی اوقات در حافظه فلش یا گوشی همراه شما فایل‌هایی به‌صورت مخفی وجود دارند که در صورت اتصال به رایانه و باز کردن آن‌ها، به‌صورت خودکار اجرا شده و باعث آلودگی رایانه محل کار می‌شوند. پس تا جای ممکن از اتصال این قبیل دستگاه‌ها خصوصاً حافظه فلش خودداری کنید.

۱۴. از اجرای فایل‌های مشکوکی که از اینترنت دریافت کرده‌اید، خودداری کنید.

فضای اینترنت مملو است از فایل‌های آلوده‌ای که می‌توانند در قالب نرم‌افزار یا حتی تصاویر عادی قرار داده شوند و در صورت اجرای آن‌ها، ویروس یا بد افزاری که پشت این فایل‌ها پنهان شده است اجرا شود و صدمات جبران‌ناپذیری به رایانه شما وارد کند. ترجیحاً این قبیل فایل‌ها را باز نکنید یا در صورت ضرورت برای باز کردن، ابتدا توسط آنتی ویروس آن‌ها را اسکن کنید. معمولاً این کار را می‌توانید از طریق راست کلیک کردن روی فایل، سپس پیدا کردن گزینه‌ای مانند scan انجام دهید.

۱۵. رمزهای عبور خود در سامانه‌های مختلف را در مرورگر ذخیره نکنید.

اگر رمزهای عبور خود را برای ورود به سامانه‌های مختلف ذخیره کرده باشید، هر شخصی به راحتی می‌تواند بعد از دسترسی به رایانه شما، با حساب کاربری شما وارد سامانه‌ها شود و به نام و با مسئولیت شما اقدام به خراب‌کاری نماید. پس همیشه سعی کنید با به خاطر سپردن رمزهای عبور خود، در هر بار ورود به سامانه‌های دانشگاه، آن را وارد کنید و از ذخیره کردن آن خودداری کنید.

۱۶. از انتخاب رمز عبورهای یکسان برای سامانه‌های مختلف خودداری نمایید.

در صورت انتخاب رمز عبور یکسان برای سامانه‌های مختلف، در صورت لو رفتن یکی از رمزهای عبور، امکان دسترسی به سایر سامانه‌ها نیز فراهم خواهد شد و فرد غیرمجاز (هکر) می‌تواند به همه‌ی سامانه‌ها و اطلاعات شما دسترسی پیدا کند.

۱۷. در صورت دیدن هرگونه رفتار مشکوک در رایانه خود، آن را سریعاً به واحد IT نزدیک به خود گزارش دهید.

رفتارهایی مانند کندی سیستم، ری‌استارت شدن ناگهانی، پاک شدن یا غیب شدن فایل‌ها، بسته شدن خودکار برنامه‌ها، به هم ریختن برخی تنظیمات سیستم و مواردی از این دست می‌توانند نشانه‌ی آلوده بودن رایانه به بدافزار یا ویروس باشند. در صورت مواجهه با هریک از این موارد سریعاً به نزدیک‌ترین واحد IT محل کار خود گزارش دهید.

۱۸. از دانلود برنامه‌های با نام مشابه برنامه اصلی اکیداً خودداری نمایید.

اغلب ویروس‌ها و بدافزارها خود را در قالب برنامه‌های به ظاهر مجاز پنهان می‌کنند و از این طریق وارد سیستم می‌شوند. توصیه می‌شود هنگام نصب نرم‌افزارها حتماً به نام آن دقت نموده و ترجیحاً نرم‌افزار را از مرجع اصلی آن دانلود نمایید. (به عنوان مثال ممکن است هنگام دانلود مرورگر Google chrome با برنامه‌ای به نام Google chrone مواجه شوید و با نصب آن به راحتی ویروس و بدافزار را به سیستم خود دعوت نمایید!)

۱۹. از مخرب نبودن فایل‌ها یا برنامه‌ها اطمینان حاصل کنید.

در صورت نیاز به نصب برنامه جدید، پس از دانلود فایل نصبی برنامه از سایت‌هایی که از معتبر بودن آن‌ها مطمئن نیستید، حتما فایل نصبی برنامه را در سایت https://www.virustotal.com آپلود کرده و از مخرب نبودن آن اطمینان حاصل کنید. (در سایت virus total، فایل شما توسط تعداد زیادی آنتی‌ویروس به صورت آنلاین بررسی می‌شود و در صورت مشاهده مورد مشکوک به شما هشدار داده می‌شود، اگر کامل سبز شود یعنی فایل مخرب نیست و احتمال خرابکاری آن بسیار کم است).

۲۰. در صورت مواجهه با علائم مشکوک در سیستم یا تغییر نام فایل‌ها و رمز شدن آن‌ها، سریعاً کابل شبکه را از پشت سیستم جدا کنید.

برخی از بدافزارها هنگام ورود به سیستم و آلوده کردن سیستم قربانی، خود را در شبکه پخش می‌کنند و سعی دارند سیستم‌های دیگر را نیز آلوده نمایند، در این شرایط برای جلوگیری از انتشار آلودگی در شبکه بهترین راه، جدا کردن کابل شبکه است. برخی از کاربران در اثر دستپاچگی ناشی از این اتفاق سیستم را خاموش می‌کنند، این کار اشتباه است! چرا که ممکن است اطلاعات مفیدی از ردپای هکر داخل حافظه کامپیوتر وجود داشته باشد که با خاموش شدن سیستم از بین برود، لذا بهترین راه همان قطع ارتباط سیستم با شبکه و مطلع ساختن مسئولین IT است.