راهنمای رفتار امن در مواجهه با مسائل امنیتی و تهدیدات سایبری

مخاطرات سایبری

شماره نهم

مدیریت آمار، فناوری اطلاعات و ارتباطات

رمزنگاری

توصیه می‌شود از رمزنگاری برای حفاظت از اطلاعات حساس استفاده شود

همیشه از اتصال امن به سامانه‌ها، (پروتکل HTTPS) استفاده نمایید.

HTTPS://mis.ajums.ac.ir

به‌روزرسانی نرم‌افزار

الزام بروزرسانی نرم‌افزارها و سیستم‌عامل‌ها بطور مداوم

رایانه را به سامانه مرکزی بروزرسانی‌های
سیستم عامل ویندوز (WSUS Server)
در مرکز داده دانشگاه متصل نمایید.
(از کارشناس رایانه محل خدمت خود
درخواست کمک کنید)

ایمیل‌های مشکوک

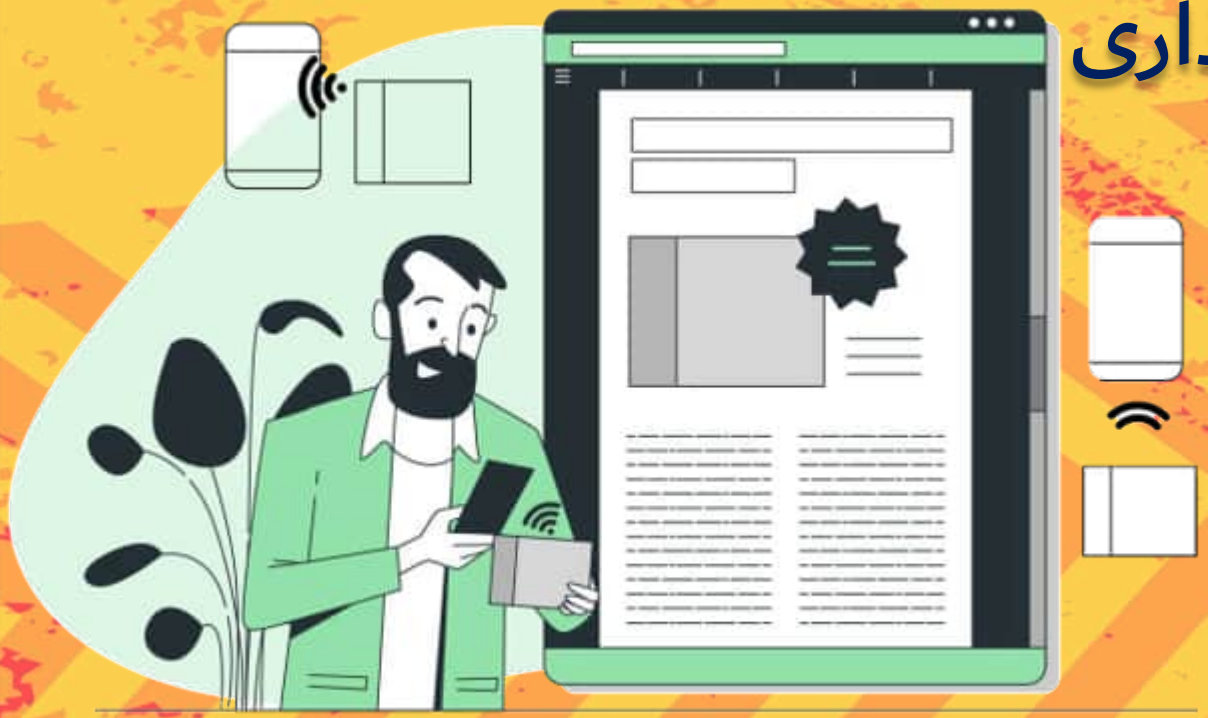
ایمیل‌های مشکوک از آدرس‌های ناشناخته را باز نکنید و اطلاعات شخصی به آنها ارسال نکنید

اگر ایمیلی ناشناخته یا مشکوک دریافت کردید، آن را حذف کنید و به هیچ عنوان آدرس های موجود در آن باز ننمایید.

حفظ داده‌ها

داده‌ها را با دقت حفظ کنید و به اشتباه با دیگران منتشر نکنید

حفظ اسناد و اطلاعات حساس در محل های ایمن و مطمئن و عدم به اشتراک گذاری اطلاعات حساس از قبیل نامه های اداری در شبکه های مجازی



تلفن‌های همراه

برای تلفن همراه رمز عبور مناسب در نظر بگیرید

تلفن همراه خود را همیشه قفل کنید و از

تأیید رمز دو مرحله برای ورود به

برنامه های حساس(مثلاً نرم افزارهای

بانکداری) استفاده نمایید

گزارش تهدیدات

تهدیدات و حوادث امنیتی را به واحد امنیت سایبری گزارش دهید

هرگونه تهدید و یا موارد امنیتی اعم از مشاهده فایل‌های مشکوک در رایانه، دریافت ایمیل‌های مشکوک، دریافت پیام‌های مشکوک بواسطه فعالیت در اینترنت و ... را به گروه زیرساخت و امنیت در مدیریت آمار و فناوری اطلاعات با شماره داخلی 1001 و یا خط مستقیم 33111001 گزارش نمایید.