امنیت سایبری کاربران نهایی سازمانی

تهدیدات فیزیکی:

۱- دسترسی فیزیکی مهاجم به سیستم قربانی
۲- به دست آوردن کلمات عبور
۳- آلوده نمودن سیستم (آلودگی با یو اس بی بسیار ساده تر از آلوده نمودن از طریق شبکه)
۴- تخریب و از بین بردن اطلاعات
۵- دسترسی به شبکه و کنترل کامپیوتر به سادگی

مقابله با تهدیدات فیزیکی :

۱- جلوگیری از سرقت اطلاعات (- قفل کردن درب اتاق - نگهداری اطلاعات مهم در مکان های امن - حفاظت از کارت شناسایی - ننوشتن کلمات عبور روی کاغذ و رها نکردن کاغذ)
۲- قفل نمودن کامپیوتر (- زمانی که پشت سیستم نیستید کامپیوتر را قفل نمایید)
۳- جعل هویت (به هیچ فرد ناشناسی اجازه استفاده از سیستم خود و حتی اتصال ذخیره سازبه کامپیوتر خود را ندهید .)
۴- گیت های امنیتی (شناسایی افرادی که به سازمان وارد می شوند)
۵- اتیکت های مشخصات فردی (برای شناسایی افراد در سازمان)

حملات کلمه‌عبور :

کلمات عبور ضعیف آسیب پذیر تر هستند .
کلمات عبور یکسان برای حساب های متفاوت خطر افشای آن ها را بیشتر میکند .

کلمه‌عبور قدرتمند :

۱- کلمات عبور با طول بالا (طول بیشتر یعنی امکان کمتر پیدا کردن کلمه عبور)
۲- کلمات عبور پیچیده (استفاده از حروف بزرگ و کوچک، اعداد و نشانه ها)
۳- کلمات عبور تصادفی (استفاده نکردن از قالب های پر کاربرد - استفاده نکردن از ساختار های قابل پیش بینی)
۴- کلمات عبور به روز! (کلمات عبور متفاوت برای حساب های مختلف - تغییر کلمات عبور به صورت دوره ای)

امنیت داده‌های موردمبادله :

۱- اطمینان از ارسال اطلاعات به وب سایت های امن (ترجیحا از سایت های Httpsاستفاده نمایید)

۲- مراقب استفاده از شبکه های عمومی باشید (در شبکه های عمومی فقط از سایت های امن Httpsاستفاده نمایید)
۳- مراقب فیشینگ (وب سایت های مشابه سایت اصلی) باشید

قوانین امنیت سایبری سازمانها :

۱- برای ذخیره سازی فایل ها از شبکه داخلی واحد مربوطه استفاده کنید.
۲- هنگام ترک میز کار، سیستم خود را باز نگذارید.
۳- دستگاه های ناشناس را به کامپیوتر خود متصل نکنید
۴- هیچ نرم افزاری را بدون اجازه دانلود یا نصب نکنید
۵- ایمیل های ناخواسته و ناآشنا پاسخ ندهید. پشتیبانی افراد ناآشنایی که تماس می گیرند را نپذیرید