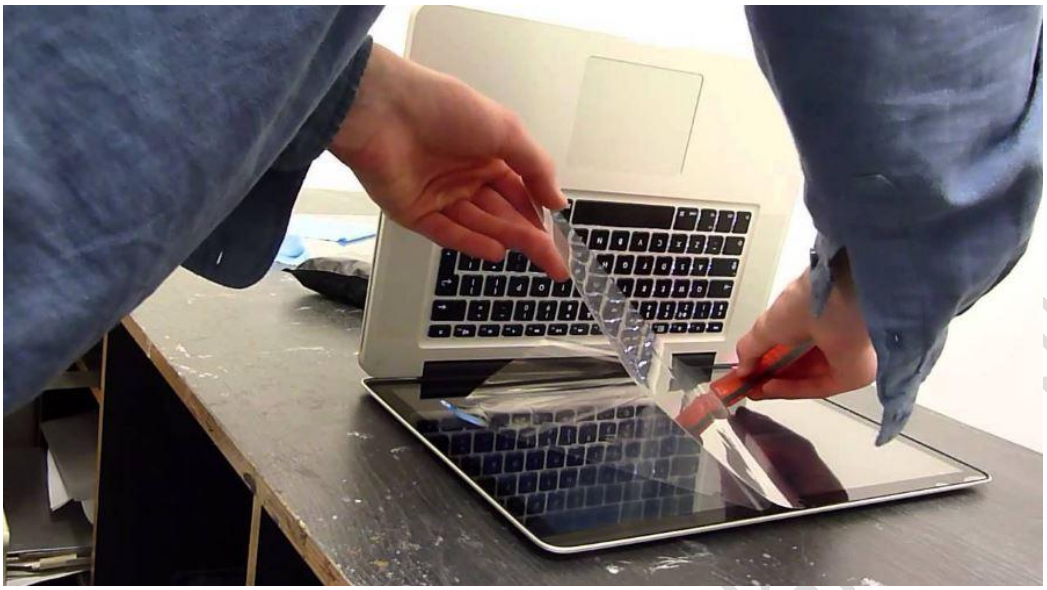


درخشش بیش از اندازه دیوارها و استفاده از رنگ‌های روغنی براق هم می‌تواند با انعکاس برروی صفحه مانیتور سبب ایجاد خستگی چشم‌ها شود به همین دلیل توصیه می‌شود درمحیط‌های اداری از رنگ‌های غیر روغنی، کاغذ دیواری و یا ترکیبی از چوب و سایر مواد استفاده شود تا کارمندان دچار خستگی چشم در زمان کاربا رایانه نشوند.

دقت درانتخاب عینک مناسب برای کار با مانیتور رایانه

در صورتی که از عینک طبی در زمان کار و مطالعه استفاده می‌کنید، حتماً عینک انتخابی شما دارای پوشش ضد انعکاسی AR باشد. این پوشش به کاهش میزان نور منعکس شده از صفحه نمایش مانیتور کمک می‌کند.

وقت خود را صرف بازی‌های رایانه نکنید

ارزش سلامت شما چشمان شما بیش از این است که افزون برکار روزانه مدت زمان طولانی را صرف انجام بازی‌های رایانه‌های یا سرگرم شدن درشبکه‌های اجتماعی نصب شده برروی گوشی‌های تلفن همراه هوشمند کنید. در بازه‌های زمانی غیرکاری به ورزش، استراحت، قدم زدن یا مطالعه کتاب‌های کاغذی بپردازید تا اعصاب چشم هایتان سالم بمانند.

پژوهش‌ها نشان می‌دهند نور آبی HEV منتشرشده از وسایل دیجیتال می‌تواند سبب آسیب به بافت شبکیه چشم افراد و ابتلا به بیماری‌های چشمی، چون دژنراسیون ماکولا شود.

قانوان ۲۰-۲۰-۲۰ را فراموش نکنید

بنابراین قانون که چشم پزشکان آن را توصیه می‌کنند پس از هر ۲۰ دقیقه کاربا رایانه حداقل به مدت ۲۰ ثانیه به فضای ۲۰ فوتی (۶ متر بیشتر) نگاه کنید تا دچارخشکی چشم نشوید.

درخرید وسایل الکترونیکی جدید دست و دلبازباشید

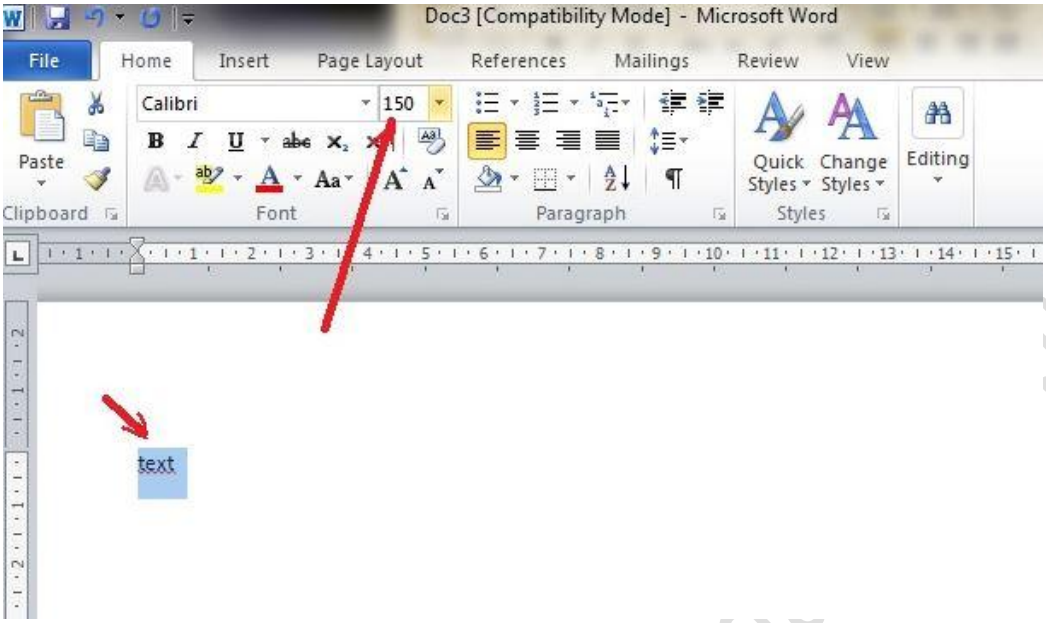
اگر با مانیتور قدیمی کار می‌کنید به ویژه از نوع CRT حتماً آن را تعویض و از مدل‌های جدید مانند LCD استفاده کنید. فناوری‌های جدید دارای استانداردهای بهتری برای محافظت ازچشم هاهستند و به این ترتیب آسیب کمتری به چشم‌های شما می‌رسد.

همچنین با بررسی دفترچه راهنمای مانیتور یا مطالعه درسایت‌های اینترنتی می‌توانید بهترین تنظیمات برای میزان نور دهی مانیتور را پیدا کنید و به این ترتیب به سلامت چشمان خود کمک کنید.

اندازه صفحه مانتیور از ۱۹ اینچ به بالا برای **سلامت چشم‌ها** توصیه می‌شود، زیرا ابعاد کوچک‌تر ازاین مقدار می‌تواند سبب فشار به چشم برای مشاهده اطلاعات و به تدریج بالا رفتن فشارخون چشم و بیماری‌های ناشی ازآن شود.

اندازه متن‌ها را بزرگ کنید

اگر مشغول به تایپ یا خواندن مطالب هستید با استفاده ازقابلیت بزرگنمایی داخل برنامه‌های رایانه، ابعاد فونت‌ها را بزرگ کنید به این ترتیب چشم شما کمتر دچار خستگی، قرمزی واشک ریزی می‌شود.



استفاده از قطره اشک مصنوعی فقط با اجازه پزشک

بسیاری از افراد که دچارخشکی چشم می‌شوند بلافاصله با مراجعه به داروخانه با تهیه قطره اشک مصنوعی سعی در مقابله با این مشکل می‌کنند .کارشناسان هشدار می‌دهند استفاده از **قطره اشک مصنوعی** تنها در موارد خاص، باتجویز پزشک و برای بازه زمانی محدود امکان پذیر است و استفاده بی رویه از این دارو خود می‌تواند سبب عارضه‌های سلامت درافراد شود.

محققان اعتقاد دارند یکی از دلایل **خشکی چشم** افراد پلک زدن بیش از اندازه آن‌ها در زمان کار با رایانه است. پلک زدن واکنش طبیعی بدن درزمان خشک شدن لایه بیرونی چشم برای مرطوب نگه داشتن آن و جلوگیری از برخورد ذرات مختلف با چشم است. اما زمانی که پلک زدن بیش از اندازه روی دهد دیگر غدد اشکی چشم توانایی مرطوب کردن بخش بیرونی چشم را ندارد. کارشناسان توصیه می‌کنند افراد درمحل کار از دستگاه‌های تهویه هوا استفاده کنند که سبب افزایش رطوبت نسبی می‌شود.

آرایش چشم‌ها عاملی جدی برای خستگی چشم‌ها

برخی ازبانوان درتمام طول روز آرایش چشم مانند خط چشم، ریمل یا حتی مژه کاشت دارند که این سبب سنگین شدن پلک و احساس خستگی و قرمز شدن چشم‌ها می‌شود.

ورزش و تغذیه مکمل‌های کمکی برای سلامت چشم‌ها

با انجام ورزش منظم، قدم زدن هردو ساعت یک بار درمحل کار پس از کار با رایانه و مصرف مواد غذایی سالم حاوی کاروتنوئید می‌توانید به سلامت چشمان خود کمک کنید.

روش های حفاظت از داده

به اعتقاد بسیاری از کارشناسان ، مهمترین و یا بهتر بگوئیم با ارزش ترین چیز بر روی یک کامپیوتر ، داده ایجاد شده توسط کاربر است و شاید وجود همین اطلاعات است که ضرورت استفاده از کامپیوتر و یا شبکه را توجیه می نماید . سیستم های عامل و نرم افزارها را در بسیاری از موارد و همزمان با بروز مشکل در سیستم ، می توان مجددا" نصب نمود ولی داده ایجاد شده توسط کاربر در نوع خود منحصربفرد بوده و در صورت از دست دادن ، امکان استفاده مجدد از آنها با مشکل اساسی مواجه و در برخی موارد عملا" غیرممکن خواهد بود.

برخی از داده های ذخیره شده بر روی کامپیوتر ممکن است دارای اهمیت بیشتری نسبت به سایر اطلاعات باشند و ضمن این که هرگز علاقه مند به از دست دادن آنها نمی باشیم ، نمی بایست امکان استفاده از آنها توسط کاربران غیرمجاز نیز وجود داشته باشد . دستیابی به برخی از داده های مهم نظیر شماره کارت اعتباری و یا حساب بانکی می تواند در نهایت منجر به سرقت هویت کاربران گردد . مسائل اشاره شده ، صرفا" محدود به کاربران شخصی نبوده و سازمان ها و موسسات را نیز شامل می شود . هر سازمان دارای داده های مهم و حساسی است که از دست دادن آنها می تواند خسارات جبران ناپذیری را برای یک سازمان به دنبال داشته باشد .

برای حفاظت از اطلاعات می بایست از یک استراتژی خاص تبعیت نمود که ضمن کاهش احتمال از دست دادن داده ها ، امکان استفاده از آنها توسط افراد غیرمجاز نیز وجود نداشته باشد .

در ادامه به برخی از متداولترین روش های حفاظت از اطلاعات اشاره می گردد:

تهیه Backup در اولین فرصت و به صورت مرتب : تهیه backup بطور مرتب و بر اساس یک استراتژی خاص ، یکی از اقدامات اساسی در جهت حفاظت از اطلاعات می باشد . اطلاعاتی که ممکن است به هر دلیلی با مشکل مواجه و امکان استفاده از آنان وجود نداشته باشد . برای تهیه backup ، می توان از امکانات موجود در ویندوز نظیر برنامه ntbackup استفاده نمود . با استفاده از ویزارد ارائه شده در برنامه فوق ، می توان به سرعت و به سادگی عملیات لازم به منظور تهیه backup و یا برگرداندن اطلاعات backup گرفته شده را انجام داد . در صورت ضرورت ، می توان تهیه backup از داده های مهم موجود بر روی سیستم را به صورت یک job تعریف و برای آن یک برنامه زمانبندی خاص را در نظر گرفت .

برای تهیه backup ، می توان از نرم افزارهای متعدد دیگری نیز استفاده نمود که امکانات بمراتب بیشتری را در مقایسه با برنامه ارائه شده در ویندوز

در اختیار کاربران قرار می دهند . صرفنظر از این که از چه برنامه ای برای تهیه backup استفاده می گردد ، می بایست از اطلاعات backup گرفته شده به دقت حفاظت و آنها را در مکان هائی با ضریب ایمنی و حفاظتی بالا نگهداری کرد .

استفاده از مجوزهای امنیتی file-level و share-level : به منظور حفاظت از داده در مقابل دستیابی افراد غیرمجاز ، اولین مرحله تنظیم مجوزها بر روی فایل ها و فولدرهای حاوی داده می باشد .در صورتی که می بایست داده به صورت مشترک در شبکه استفاده گردد ، می توان با تنظیم share permissions نحوه استفاده از آنها را قانونمند نمود . بدین منظور می توان در ویندوز ۲۰۰۰ و یا XP پس از انتخاب فایل و یا فولدر ، از طریق صفحه Properties گزینه Sharing و در نهایت دکمه permission را انتخاب نمود . تنظیمات امنیتی اشاره شده در رابطه با کاربرانی که به صورت محلی از سیستم حاوی اطلاعات حساس استفاده می نمایند ، اعمال نخواهد شد .

در صورتی که کامپیوتر با کاربر دیگری به اشتراک گذاشته شده است ، می بایست از مجوزهای file-level استفاده نمود . به این نوع از مجوزها ، مجوزهای NTFS نیز گفته می شود چراکه استفاده از آنها صرفا" برای فایل ها و فولدرهای ذخیره شده بر روی پارتیشن هائی که با سیستم فایل

NTFS فرمت شده اند ، امکان پذیر می باشد . برای استفاده از مجوزهای فوق ، پس از انتخاب فایل و یا فولدر مورد نظر می توان از طریق صفحه properties ، گزینه Security tab را انتخاب و مجوزها را بر اساس سیاست مورد نظر تنظیم نمود .

در هر دو مورد (مجوزهای file-level و share-level) می توان مجوزها را برای user account و groups تعریف نمود . مجوزها را می توان از "فقط خواندنی" تا " کنترل کامل " در نظر گرفت .

حفاظت از فایل ها و سایر مستندات توسط رمز عبور : تعداد زیادی از نرم افزارها (نظیر نرم افزارهای آفیس و Adobe Acrobat) ، امکان تعریف رمزعبور برای استفاده از مستندات را در اختیار کاربران قرار می دهند . پس از در نظر گرفتن یک رمز عبور ، در صورت فعال کردن (بازنمودن) یک مستند در ابتدا از کاربر درخواست رمز عبور خواهد شد . به منظور انجام این کار در برنامه ای نظیر Microsoft word ۲۰۰۳ ، از طریق منوی Tools گزینه options و در ادامه Security tab را انتخاب می نمائیم . با استفاده از امکانات فوق ، می توان یک رمز عبور و نحوه رمزنگاری را مشخص نمود .

متاسفانه، سیستم رمز استفاده شده در محصولات مایکروسافت ، به سادگی شکسته می گردد و کاربران غیرمجاز می توانند از برنامه های متعددی به

منظور رمزگشائی مستندات استفاده نمایند. برنامه AOPR (برگرفته از Advanced Office Password Recovery) نمونه ای در این زمینه می باشد .

در صورت لزوم می توان از نرم افزارهائی نظیر WinZip و PKZip به منظور فشرده سازی و رمزنگاری اسناد و یا فایل ها استفاده نمود .

استفاده از رمزنگاری EFS : ویندوز ۲۰۰۰ ، XP و ۲۰۰۳ از رمزنگاری سیستم فایل موسوم به EFS (برگرفته از Encrypting File System) حمایت می نمایند . از سیستم رمزنگاری فوق می توان به منظور رمزنگاری فایل ها و فولدرهای ذخیره شده بر روی پارتیشنی که با NTFS فرمت شده است ،استفاده نمود . بدین منظور می توان پس از انتخاب صفحه properties ، از طریق General tab گزینه Advanced button را انتخاب نمود (بطور همزمان نمی توان از رمزنگاری EFS و مجوزهای NTFS استفاده نمود) .

سیستم رمزنگاری EFS به منظور افزایش امنیت و کارآئی از ترکیب رمزنگاری متقارن و نامتقارن استفاده می نماید . سیستم فوق برای حفاظت از داده های ذخیره شده بر روی دیسک استفاده می گردد و در صورتی که یک فایل رمز شده در طول شبکه حرکت کند و کاربران از یک sniffer به منظور

capture بسته های اطلاعاتی استفاده نمایند ، می توانند اطلاعات موجود در فایل را مشاهده نمایند .

استفاده از رمزنگاری دیسک : با استفاده از نرم افزارهای متعددی می توان تمامی محتویات یک دیسک را رمز نمود . بدین ترتیب ، کاربران غیرمجاز قادر به مشاهده محتویات ذخیره شده بر روی دیسک نخواهند بود . داده بطور اتومانیک و در زمان نوشتن بر روی هارد دیسک رمز و قبل از استقرار درون حافظه ، رمزگشائی می گردد . از اینگونه محصولات می توان به منظور رمزنگاری درایوهای USB ، فلش درایوها و ... استفاده نمود . PGP Whole Disk Encryption و DriveCrypt نمونه هائی از اینگونه برنامه ها می باشند .

استفاده از زیرساخت کلید عمومی : PKI (برگرفته از public key infrastructure) ، سیستمی برای مدیریت زوج کلید خصوصی و عمومی و گواهینامه های دیجیتال است . با توجه به این که کلید ها و گواهینامه ها توسط یک مرکز تائید شده صادر می شوند از استحکام امنیتی بیشتری برخوردار می باشند . (سرویس دهندگان گواهینامه دیجیتال ممکن است به صورت داخلی و در یک شبکه خصوصی نصب و یا در یک شبکه عمومی ، نظیر

Versign ، نصب شده باشند) . در چنین مواردی ، می توان داده را با استفاده از کلید عمومی کاربر مورد نظر رمز نمود . در ادامه، صرفا" کاربری قادر به رمزگشائی اطلاعات است که دارای کلید خصوصی مرتبط با کلید عمومی باشد .

مخفی کردن داده درون داده دیگر : با استفاده از یک برنامه steganography می توان داده مورد نظر را درون سایر داده ها مخفی نمود . به عنوان نمونه ، می توان یک پیام متن را درون یک فایل گرافیکی JPG . و یا فایل موزیک ۳mp . ، مخفی نمود . اینگونه ها برنامه ها پیام ها را رمز نمی نمایند و اغلب از آنان به همراه نرم افزارهای رمزنگاری استفاده می گردد . در چنین مواردی ، در ابتدا داده رمز و در ادامه با استفاده از نرم افزارهای steganography مخفی می گردد . برنامه StegoMagic یک نمونه از برنامه های steganography است که با استفاده از آن می توان متن مورد نظر را رمز و درون فایل هائی از نوع WAV، TXT . . و یا BMP . ذخیره نمود .

حفاظت داده در حال حمل : داده ارسالی در یک شبکه می تواند در زمان حرکت توسط مهاجمان شنود گردد . مهاجمان در این رابطه از نرم افزارهائی

موسوم به sniffer استفاده می نمایند که امکان آنالیز پروتکل و یا مانیتورینگ شبکه را در اختیار آنان قرار می دهد. برای حفاظت داده در زمان حرکت در شبکه ، می توان از IPSec (برگرفته از Internet Protocol Security) استفاده نمود . در چنین مواردی ، سیستم ارسال کننده و سیستم دریافت کننده می بایست قادر به حمایت از ویژگی فوق باشند . از ویندوز ۲۰۰۰ به بعد ، امکانات لازم به منظور حمایت از IPSec در سایر نسخه ها تعبیه شده است.

ایمن سازی مبادله داده در محیط های wireless : داده ئی که از طریق یک شبکه wireless ارسال می گردد ، دارای استعداد بیشتری به منظور بررسی و شنود توسط مهاجمان نسبت به سایر داده های ارسال شده بر روی یک شبکه اترنت است ، چراکه ضرورتی ندارد مهاجمان به محیط فیزیکی شبکه و یا دستگاه های مربوطه دستیابی داشته باشند . در صورت عدم پیکربندی صحیح و ایمن access point ، مهاجمان با استفاده از یک کامپیوتر قابل حمل که دارای امکانات wireless است ، می توانند به داده ذخیره شده در شبکه دستیابی داشته باشد . کاربران می بایست صرفا" اقدام به ارسال و دریافت داده بر روی شبکه هائی نمایند که از رمزنگاری WPA (برگرفته از Wi-Fi Protected Access) در مقابل WEP (برگرفته از

Wired Equivalent Protocol) استفاده می نمایند (WPA ، بمرابت دارای امنیت بیشتری نسبت به WEP است) .

استفاده از مدیریت حقوق به منظور حفظ کنترل : در برخی موارد ، لازم است که داده برای سایر کاربران ارسال گردد ولی نگران نحوه برخورد آنان با داده ارسالی می باشیم (مثلا" آیا آنان می توانند داده ارسالی را حذف و یا تغییر دهند) . در چنین مواردی می توان از RMS (برگرفته از Rights Management Services) در ویندوز استفاده نمود . سیستم فوق ، مشخص می نماید که دریافت کننده پس از دریافت اطلاعات قادر به انجام چه کاری خواهد بود . به عنوان نمونه ، می توان حقوق مورد نظر را بگونه ای تنظیم نمود که صرفا" دریافت کننده قادر به مطالعه فایل ارسالی باشد و نتواند در آن تغییراتی را اعمال نماید . همچنین ، با استفاده از سیستم فوق می توان مدت زمان استفاده از مستندات و یا پیام ها را مشخص نمود . بدین ترتیب پس از گذشت مدت زمان مشخص شده ، اعتبار آنها به اتمام رسیده و عملا" امکان دستیابی و استفاده از آنها وجود نخواهد داشت .

برای استفاده از RMS ، به ویندوز ۲۰۰۳ که به عنوان یک سرویس دهنده RMS پیکربندی شده است نیاز می باشد . در چنین مواردی ، کاربران نیز به یک نرم افزار خاص و یا یک add-in همراه مرورگر نیاز خواهند داشت تا

بتوانند به مستندات حفاظت شده توسط RMS دستیابی داشته باشند . کاربران مجاز یک گواهینامه را از سرویس دهنده RMS دریافت می نمایند .