کاربران کامپیوتر و حداقل دانش لازم

- **راه اندازی مجدد قبل از تماس با واحد پشتیبانی** : با این که اعلام این موضوع به کاربران که در صورت بروز مشکل در ابتدا کامپیوتر خود را راه اندازی مجدد نمایند ، بنظر یک روش مناسب نمی باشد ولی این یک واقعیت اثبات شده است که با راه اندازی مجدد یک کامپیوتر ممکن است برخی از مسائل و مشکلات برطرف گردد. حتی در صورتی که با راه اندازی مجدد یک کامپیوتر مشکل برطرف نگردد ، این که پس از راه اندازی همچنان مشکل وجود دارد می تواند اطلاعات مفیدی را به منظور اشکال زدائی در اختیار کارشناسان واحد فنی قرار دهد .
- **نحوه گزارش یک مشکل** : علاوه بر این که لازم است کاربران آگاهی لازم در خصوص نحوه ارسال یک گزارش خطاء را داشته باشند (تماس تلفنی ، ارسال email و ...) ، می بایست بدانند که چه نوع اطلاعاتی می تواند به منظور سرعت در حل مشکل مفید واقع شود . در این رابطه می توان یک فرم خاص را به منظور جمع آوری اطلاعات مربوط به مشکل ایجاد شده طراحی و در آن به مواردی نظیر : پیام های خطاء ، برنامه های فعال در زمان بروز مشکل ، چه کاری انجام شده است که باعث بروز مشکل شده است و این که آیا امکان تولید مجدد همان خطاء و یا مشکل وجود دارد ، اشاره نمود . به منظور تکمیل صحیح و کامل این نوع فرم های اطلاعاتی ، می بایست به کاربران آموزش های لازم داده شود تا ضمن جلوگیری از ارسال اطلاعات ناقص و اندک ، آنان تشخیص خود را در خصوص مشکل ایجاد شده در مقابل علائم و دلایل بروز خطاء ارسال ننمایند .
- **نگهداری ایمن رمزهای عبور** : کاربران می بایست نسبت به عواقب نگهداری رمزهای عبور در یک مکان غیرایمن و یا اشتراک آنان با سایر همکاران ، آگاه گردند . بدفعات مشاهده شده است که کاربران رمزهای عبور خود را بر روی کاغذ نوشته و آن را به مانیتور و یا بر روی بدنه کیس خود می چسبانند و یا حتی از آنان به عنوان متن در screensaver استفاده می نمایند . آموزش کاربران به منظور تعریف و حفاظت از رمزهای عبور متناسب با سیاست های امنیتی یکی از ملزومات امنیتی اولیه در عصر حاضر محسوب می گردد .
- **ایجاد رمزهای عبور ایمن** : در زمان آموزش کاربران در خصوص نگهداری ایمن رمزهای عبور، از این فرصت می بایست استفاده و به آنان دستورالعمل های لازم در خصوص تعریف رمزهای عبور ایمن نیز گفته شود . ضوابط تعریف یک رمزعبور ایمن می بایست متناسب با سیاست های امنیتی تعریف شده در یک سازمان باشد .
- **حفاظت از کامپیوتر در زمان مسافرت** : استفاده از کامپیوترهای notebook و سایر دستگاه های الکترونیکی در مسافرت ، نیاز به هوشیاری بیشتری به منظور پیشگیری از دستیابی غیرمجاز دارد . به کاربران علاوه بر آموزش نحوه حفاظت از داده موجود بر روی کامپیوتر دفتر کار ، می بایست نحوه استفاده ایمن از کامپیوتر در زمان ترک دفتر کار نیز آموزش داده شود (دستیابی به کامپیوتر از راه دور و رعایت موارد امنیتی لازم) .

- **پیشگیری لازم در خصوص از دست دادن داده** : به کاربران می بایست آموزش داده شود که عملیات backup خود به خود انجام نمی شود و اگر آنان اقدام به حذف فایل و یا فایل هائی نمایند که قبلا" از آنان backup گرفته نشده است ، امکان بازیابی آنان وجود نخواهد داشت . در اکثر سازمان ها کاربران نسبت به گرفتن backup از داده های مهم موجود بر روی کامپیوتر توجیه نمی باشند و می بایست این موضوع و فرآیند انجام آن به درستی به کاربران آموزش داده شود .

- **رعایت سیاست های تعریف شده** : تمامی سازمان ها می بایست دارای یک سیاست امنیتی باشند که باید ها و نبایدها را مشخص می نماید . در واقع سیاست های امنیتی ، یک سطح امنیتی اولیه به منظور حفاظت از زیرساخت اطلاعاتی موجود در یک سازمان و منابع موجود بر روی آن را مشخص و تعریف می نماید. کاربران می بایست نسبت به مفاد سیاست های امنیتی و استفاده ایمن از منابع اطلاعاتی موجود در سازمان آگاه و معایب عدم رعایت مسائل مندرج در سیاست امنیتی به آنان آموزش داده شود .

- **دقت در ارسال email** : ارسال email با عناوین نادرست و محتویات غیرواقعی یکی از مشکلات اساسی در بسیاری از سازمان ها محسوب می گردد که قطعا" می تواند پیامدهای منفی را برای فرد ارسال کننده و یا سازمان مربوطه به دنبال داشته باشد . صرفنظر از محتویات و ماهیت سیاست استفاده از سرویس email در یک سازمان ، به کاربران می بایست آموزش های لازم در خصوص استفاده ایمن از email داده شود .

- **حفاظت در مقابل ویروس ها ، کرم ها و تروجان ها** : با این که معمولا" مسئولیت حفاظت از منابع اطلاعاتی در یک سازمان بر عهده کارشناسان فن آوری اطلاعات و ارتباطات است ولی نمی توان با تاکید بر این موضوع این تضمین را داد که هیچگونه مشکل امنیتی در سازمان ایجاد نخواهد نشد . قطعا" میزان هوشیاری و دقت کاربران در این خصوص بی تاثیر نخواهد بود . به کاربران می بایست آموزش داده شود که چگونه تهدیدات را شناسائی و با آنان برخورد نمایند . نحوه شناسائی phishing ، نامه های الکترونیکی مخرب ، عدم استفاده و یا مطالعه نامه های الکترونیکی از منابع ناشناخته ، عدم باز نمودن فایل های ضمیمه همراه نامه های الکترونیکی ، عدم استفاده از آدرس email سازمان در وب سایت ها ، غیر فعال کردن برنامه های حفاظتی نظیر آنتی ویروس ها و بهنگام سازی آنان از جمله مواردی می باشند که می بایست به کاربران آموزش داده شود .