باسمه تعالی

امنیت اطلاعات دیجیتال – قسمت اول

امروزه کمتر سیستمی پیدا می شود که مواردی از قبیل اطلاعات دیجیتال محرمانه، اسناد مالی، پیام های خصوصی و ... روی آن ذخیره نشده باشد.این اطلاعات نیازمند حفاظت هستند تا از دستبرد و سوء استفاده در امان بمانند.

در این مختصر قصد آگاهی بخشی درباره امنیت اطلاعات روی PC/Laptop را داریم و در ذیل به آن می پردازیم:

س . کلمه عبوری که در قسمت BIOS SETUP کامپیوتر گذاشته می شود چقدر امنیت و اهمیت دارد؟

ج . گذاشتن آن توصیه می شود ولی این کلمه عبور را می توان به صورت سخت افزاری(ریست تنظیمات CMOS) و برای برخی مادربوردها به صورت میان افزاری برداشت.

س . ایجاد کلمه عبور برای کاربران ویندوز چه اهمیتی دارد؟

ج . همانطور که می دانید کاربران ویندوز معمولا به دو دسته مدیر و محدود شده تقسیم می شوند؛ پیشنهاد می شود که بجز در موارد ضروری از کاربر مدیر استفاده نکنید چون دارای دسترسی کامل است و ویروس ها و هکر ها هم از این دسترسی استفاده می کنند و اینرا نیز بدانید که نداشتن کلمه عبور بهتر از کلمه عبور ضعیف است زیرا مایکروسافت بطور پیش فرض اجازه اتصال راه دور به کاربر بدون کلمه عبور را نمی دهد! همچنین اگر کاربر ، وارد شده باشد می توان با دستور خط فرمان یا برنامه معادل آن در ویندوز پسورد را بدون دانستن آن، برداشت و یا تغییر داد!.

س . آیا راهکاری برای رفع آن وجود دارد؟

ج . بله! از یک کلمه عبور قوی حداقل هشت کارکتری که شامل حروف، ارقام و علائم باشد استفاده کنید و محافظ صفحه نمایش را به صورت زیر تنظیم نمایید:

Wait : 5minutes

- ✓ On resume, Display Logon Screen

س . آیا این کار صد در صد مطمئن است؟

ج . خیر اولا این کلمه عبور را هم با دسترسی به خط فرمان در Logon Screen می توان پاک کرد، ثانیا نرم افزاری مانند WinPasswordRemover وجود دارد که از روی لوح فشرده، بوت شده و امکان پاک کردن کلمه عبور را فراهم می کند. می توانید برای افزایش امنیت SysKey را فعال کنید.

س . SysKey چیست؟

ج. نوعی کلمه عبور است؛ مسیر زیر را دنبال کنید:

Run>Syskey>Update>Password Startup>Type your Password

س . آیا تمامی این موارد به من اطمینان خاطر می دهد؟

ج . خیر با استفاده سیستم عامل زنده که از روی لوح فشرده، بوت می شود و یا با جداکردن دیسک سخت و اتصال آن به کامپیوتر دیگر، می توان به اطلاعات شما دسترسی داشت. لذا باید علاوه بر موارد فوق، از پنهان سازی و رمزگذاری **روی خود فایل ها** استفاده کنید.در پنهان سازی وقت هکر صرف پیداکردن مکان فایل ها می شود و در رمزگذاری صرف پیدا کردن کلمه عبور، و بهتر است از ترکیب این دو روش استفاده کنید؛ این دو راهکار را در آینده توضیح خواهیم داد.

س . از Win RAR و Zip می توانم استفاده کنم؟

ج . بله، مسیر زیر را دنبال کنید:

راست کلیک روی پوشه مورد نظر>Add to archive>Advanced>Set Password>نوشتن کلمه عبور>OK>OK.

توجه داشته باشید اگر تعداد فایل ها زیاد و یا حجم آنها بالاست این کار زمانبر خواهد بود و همچنین کلمات عبور دو یا سه حرفی براحتی توسط WinRARPasswordFinder/Remover کشف می شوند.

س . پس چه باید کرد؟

ج . از کلمات عبور قوی استفاده کنید!، پشتیبان گیری از اطلاعات را فراموش نکنید و همچنین می توانید از نرم افزاری مانند**Folder Guard Pro** که آموزش تصویری آن همراه این ارجاع است استفاده نمایید.(حتما مشاهده کنید).

در پایان خواهشمند است نظرات و پیشنهادهای ارزشمند خود را از طریق اتوماسیون و یا رایانامه زیر برای حفاظت فناوری اطلاعات بفرستید.

herasat@birjand.ac.ir