Cybersecurity

مرکز تخصصی آپا
دانشگاه تخصصی تکمیلی
صنعت و فناوری پیشرفته

رمزنگاری

حذف ایمن فایل

امنیت فیزیکی

اصطلاحات رایج

Encryption Key

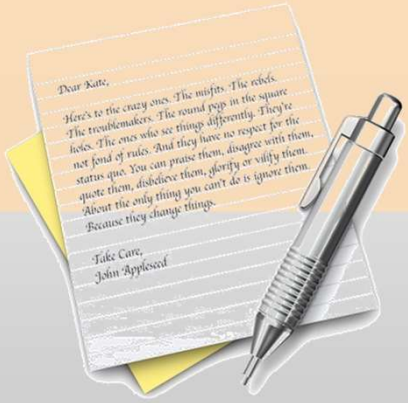
- کلید رمزگذاری، قسمتی از اطلاعات است که برای رمز نمودن و رمزگشایی داده مورد استفاده قرار می‌گیرد.

Cipher Text

- Cipher text یک متن رمزگذاری شده و غیرقابل خواندن است، تا زمانی که با یک کلید به Plaintext (متن ساده) رمزگشایی شود.

Plaintext

- Plaintext یا Cleartext یک متن ساده‌ی رمزگذاری نشده و قابل خواندن است.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

رمزگذاری چیست؟

- رمزگذاری، فرآیند تبدیل داه به یک cipher text است، به گونه‌ای که توسط افراد غیرمجاز قابل فهم نباشد.
- برای خواندن یک فایل رمز شده، باید به کلید محرمانه یا رمز عبوری که شما را قادر به رمزگشایی می‌کند دسترسی داشته باشید.
- رمزگذاری، به منظور حفاظت از اطلاعات حساس هنگام انتقال و ذخیره سازی داده مورد استفاده قرار می‌گیرد.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

اهداف رمزگذاری

تمامیت یا اصالت (Integrity) از پیام در برابر تغییر غیر مجاز محافظت می‌کند.

حفظ اسرار و محرمانگی (Confidentiality)، محرمانگی تضمین می کند تا افراد غیر مجاز قادر به دسترسی به اطلاعات حساس نباشند.

عدم انکار یا non-repudiation، فرستنده‌ی پیام نمی‌تواند منکر ارسال پیام شود.

احراز هویت یا (Authentication)، بسیاری از سیستم‌های تایید هویت کاربران تکیه بر رمزنگاری دارند.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

کاربردهای رمزگذاری

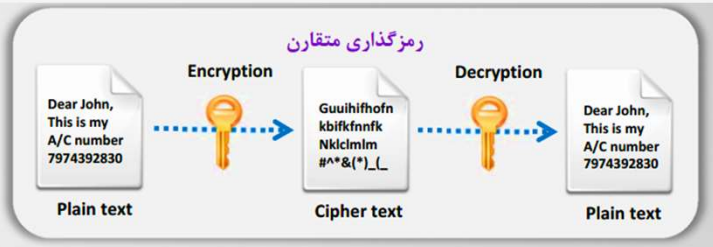
- رمزگذاری به عنوان یک منبع برای تبادل اطلاعات مبتنی‌بر وب، به منظور حفاظت از اطلاعات مهم مانند اطلاعات کارت اعتباری نیز مورد استفاده قرار می‌گیرد.
- رمزگذاری یک رسانه امن برای کاربران فراهم می‌نماید تا بتوانند خارج از محل کار یا منزل با خیال آسوده به شبکه دوستان یا سایر شبکه‌ها متصل شوند.
- رمزگذاری به منظور حفاظت از اطلاعات محرمانه کاربر مانند نام کاربری و رمز عبور مورد استفاده قرار می‌گیرد.
- رمزگذاری هویت فرستنده را تضمین می‌کند.
- رمزگذاری داده با دادن اطمینان به مخاطب مبنی‌بر قابل اعتماد بودن منبع و محتوای پیام میزان اعتماد بیشتری را فراهم می‌نماید.
- رمزگذاری داده کمک می‌کند تا با خیال آسوده اطلاعات حساس را بر روی کامپیوتر یا رسانه‌های ذخیره سازی خارجی ذخیره کنیم.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

انواع رمزگذاری

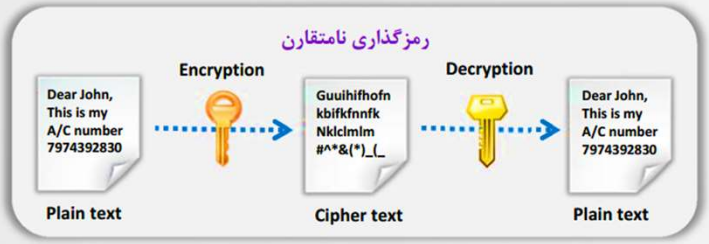
رمزگذاری متقارن

رمزگذاری متقارن (کلید محرمانه، کلید اشتراکی و کلید خصوصی) برای رمزگذاری و رمزگشایی از کلید یکسان استفاده می کند



رمزگذاری نامتقارن

رمزگذاری نامتقارن(کلید عمومی) از کلیدهای رمزگذاری متفاوت برای رمزگذاری و رمزگشایی استفاده می کند. این کلیدها تحت عنوان کلید خصوصی و کلید عمومی شناخته می شوند



تابع هش

تابع هش(رمزگذاری یک طرفه) از هیچ کلیدی برای رمزگذاری و رمزگشایی استفاده نمی کند

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

رمزگذاری متقارن در مقابل رمزگذاری نامتقارن

رمزگذاری متقارن

- رمزگذاری متقارن تنها از یک کلید برای رمزگذاری و رمزگشایی استفاده می‌کند.
- کلید نمی‌تواند به صورت آزادانه به اشتراک گذاشته شود.
- رمزگذاری متقارن مستلزم آن است که فرستنده و گیرنده هر دو کلید محرمانه را بدانند.
- با استفاده از رمزگذاری متقارن داده‌ها سریعتر رمز می‌شوند.
- الگوریتم رمزگذاری متقارن ساده‌تر و سریع‌تر است.
- رمزگذاری متقارن، محرمانگی و صحت داده را تضمین می‌کند.

رمزگذاری نامتقارن

- رمزگذاری نامتقارن از یک کلید عمومی برای رمزگذاری و از یک کلید خصوصی برای رمز گشایی استفاده می‌کند.
- در رمزگذاری نامتقارن، کلید عمومی می‌تواند آزادانه به اشتراک گذاشته شود که این موجب جلوگیری از به سرقت رفتن کلید محرمانه می‌شود.
- فرایند رمزگذاری با استفاده از رمزگذاری نامتقارن آهسته‌تر و پیچیده‌تر است.
- رمزگذاری نامتقارن، محرمانگی، صحت، تصدیق اصالت و عدم انکار را تضمین می‌نماید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

استانداردهای رمزنگاری

استاندارد رمزگذاری داده‌ها (DES)

- DES نام استاندارد پردازش اطلاعات فدرال (FIPS) است که الگوریتم رمزگذاری داده (DEA) را توصیف می‌کند.
- DEA یک سیستم رمزنگاری است که در اصل برای پیاده‌سازی در سخت‌افزار طراحی شده است.
- DEA برای رمزگذاری تک کاربره نیز مورد استفاده قرار می‌گیرد. به عنوان مثال برای ذخیره‌سازی فایل‌ها به فرم رمزگذاری شده در هارد دیسک می‌تواند استفاده شود.

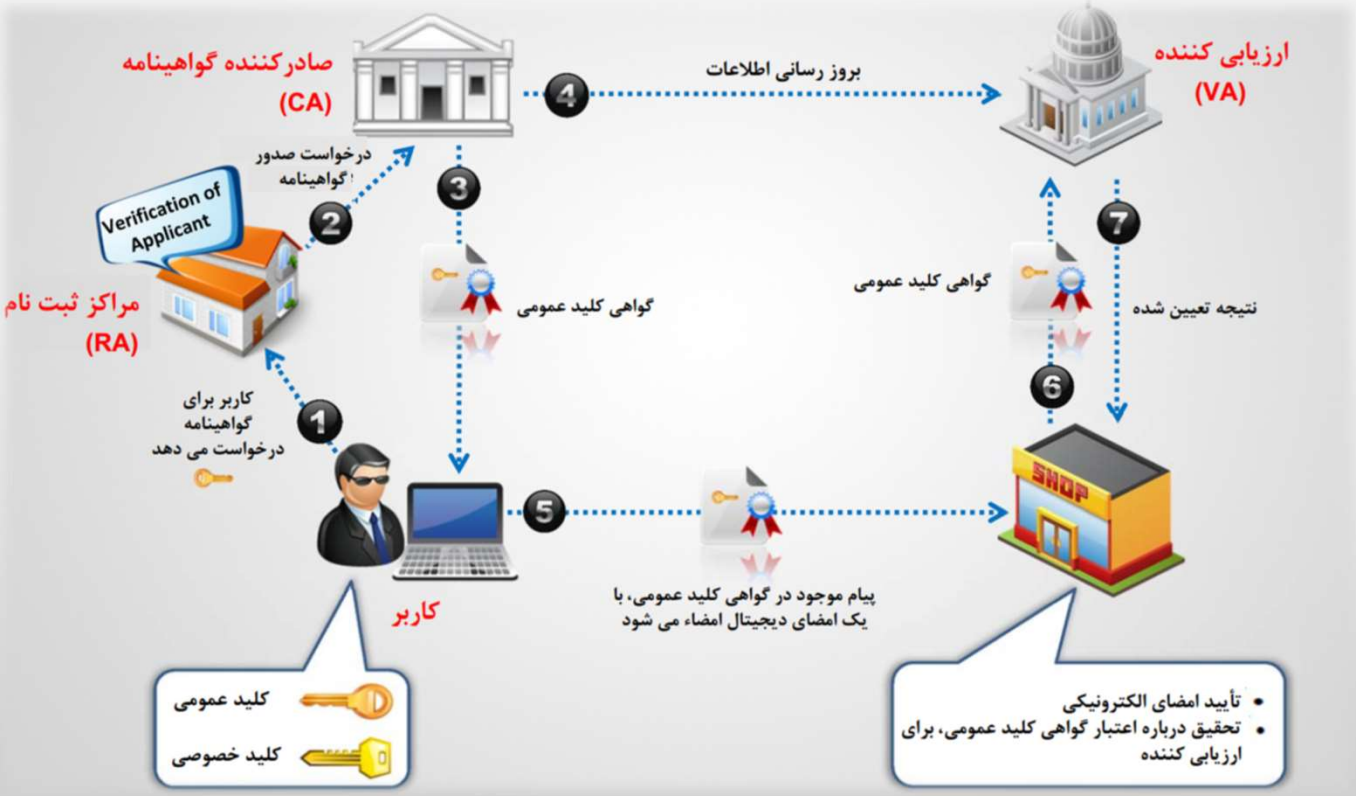
استاندارد رمزگذاری پیشرفته (AES)

- AES یک استاندارد رمزگذاری کلید متقارن است که توسط دولت ایالات متحده آمریکا ایجاد شده است.
- این استاندارد اندازه بلاک ثابت ۱۲۸ بیتی و اندازه کلید ۱۲۸، ۱۹۲، ۲۵۶ بیتی دارد.

گواهینامه‌های دیجیتال

- گواهینامه دیجیتال یک کارت الکترونیکی است که اطلاعات مربوط به اعتبارنامه را به هنگام انجام تراکنش‌های آنلاین ارائه می‌نماید.
- گواهینامه دیجیتال به عنوان یک همتای الکترونیکی برای گواهینامه رانندگی، گذرنامه یا کارت عضویت عمل کرده و هویت تمام کاربران درگیر در تراکنش آنلاین را تایید می‌کند.

گواهینامه‌های دیجیتال چگونه کار می‌کنند؟



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

امضای دیجیتال

استانداردهای دیجیتال از استانداردهای باز پیروی می‌کنند، چرا که به یک فرد یا سازمان وابسته نیستند

شمای امضای دیجیتال شامل دو کلید رمزگذاری است: یک کلید خصوصی برای امضای پیام و یک کلید عمومی برای تایید امضا

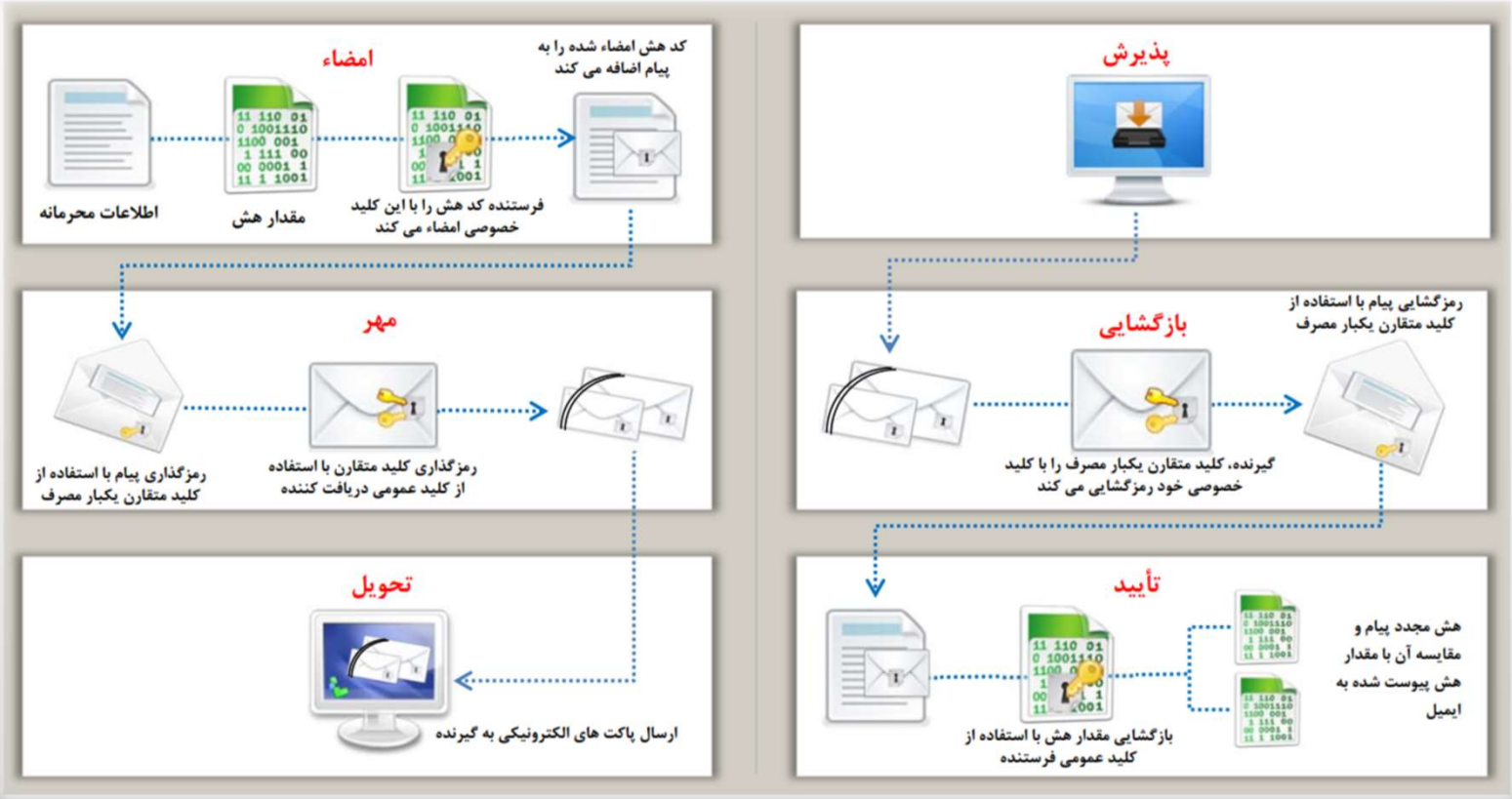
امضای دیجیتال به جای امضای روی کاغذ، با پیاده‌سازی رمزنگاری نامتقارن ویژگی‌های امنیتی امضا را به فرم دیجیتال شبیه‌سازی می‌کند.

امضای دیجیتال مستقل از تایید امضا بین فرستنده و گیرنده است.

امضای دیجیتال اغلب برای پیاده‌سازی امضاهای الکترونیکی به کار می‌رود و توسط هر نوع پیامی می‌تواندمورد استفاده قرار گیرد.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

امضای دیجیتال چگونه کار می‌کند؟



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

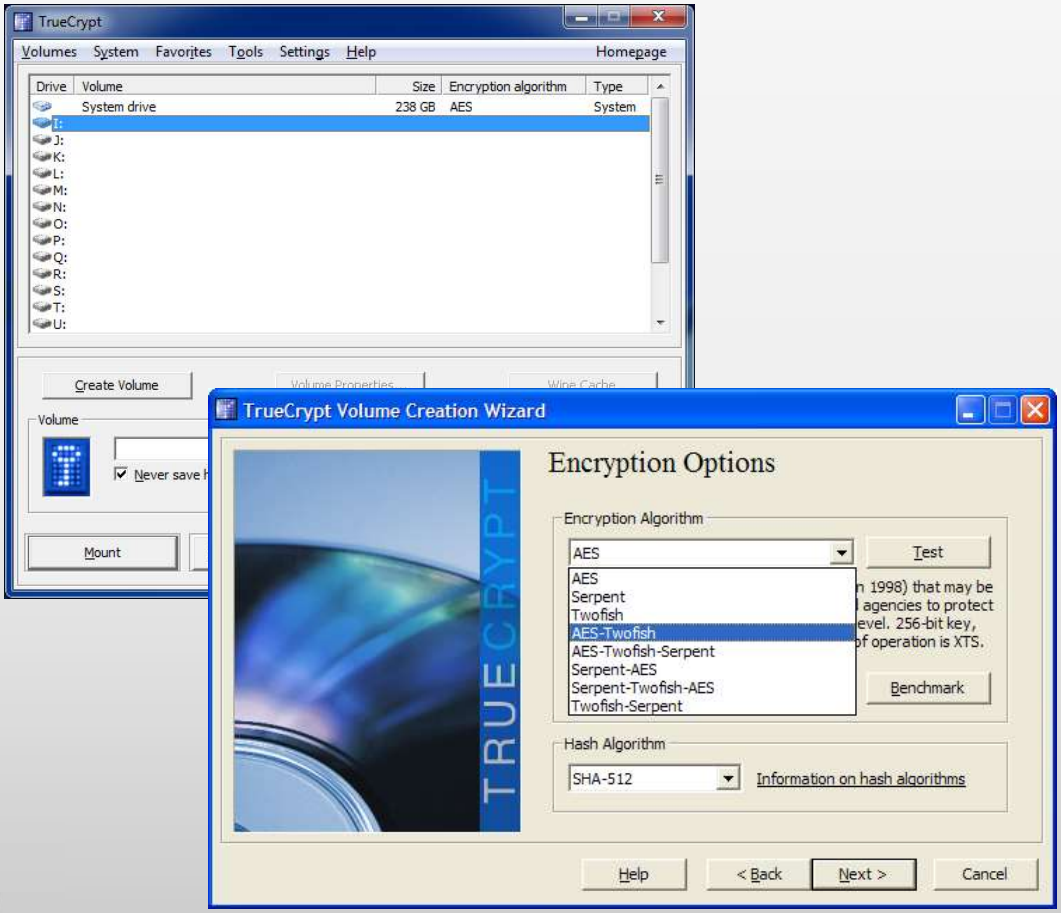
ابزارهای رمزنگاری

TrueCrypt یک دیسک رمز شده مجازی داخل یک فایل ایجاد نموده و آن را به عنوان یک دیسک واقعی لود می‌کند.

کل یک پارتیشن یا دستگاه ذخیره‌سازی، مانند USB فلش درایو یا هارد دیسک را رمزگذاری می‌کند.

پارتیشن یا درایوی که ویندوز در آن نصب شده است را رمزگذاری می‌کند.

رمزگذاری خودکار، بلادرنگ و شفاف است.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

ابزارهای رمزنگاری

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

رمزنگاری فایل ها و پوشه ها

- همیشه از NTFS استفاده کنید.
- فایل سیستم NTFS نسبت به فایل سیستم FAT عملکرد بهتر و امنیت بیشتری را برای داده‌های موجود بر روی هارد دیسک و پارتیشن‌ها فراهم می‌نماید.
- پارتیشن‌هایی که از فایل سیستم FAT16 یا FAT32 قدیمی استفاده می‌کنند را با استفاده از دستور تبدیل، به فایل سیستم NTFS تبدیل کنید.
- نکته: تبدیل یک پارتیشن از FAT به NTFS تاثیری بر روی داده‌ها ندارد. اگر پارتیشن حاوی فایل‌های سیستمی باشد، برای تبدیل به NTFS سیستم شما باید ریستارت شود.

تمام برنامه‌های باز را که در حال اجرا بر روی پارتیشن یا درایو منطقی در نظر گرفته شده برای تبدیل هستند، ببندید.

بر روی START کلیک نموده و CMD را درحالت RUN AS ADMINISTRATOR بازکنید.

در CMD دستور زیر را وارد کنید:

CONVERT DRIVE_LETTER: /FS:NTFS

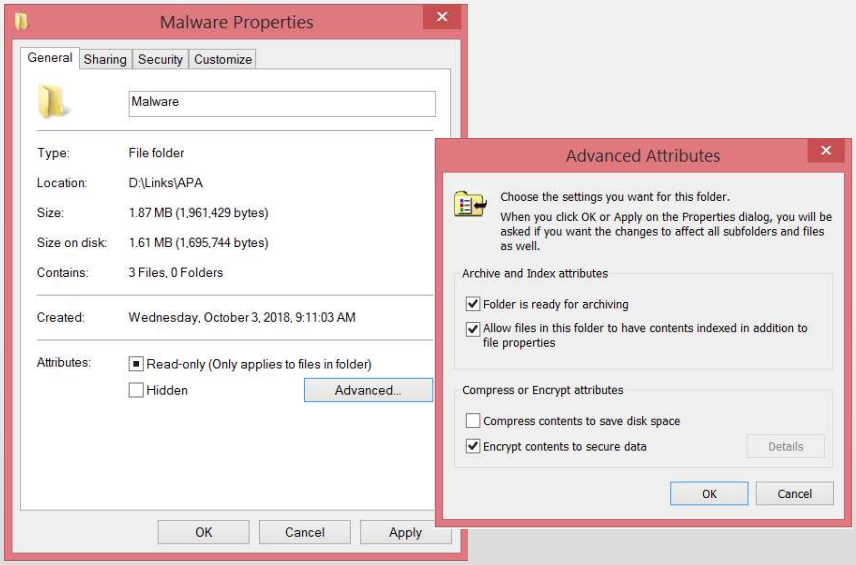
در دستور فوق DRIVE_LETTER نام درایو NTFS است که برای تبدیل در نظر گرفته شده است.

نام درایوی که برای تبدیل در نظر گرفته شده است را وارد نموده و ENTER بزنید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

چگونه یک فایل را با استفاده از EFS در ویندوز رمزگشایی کنیم؟

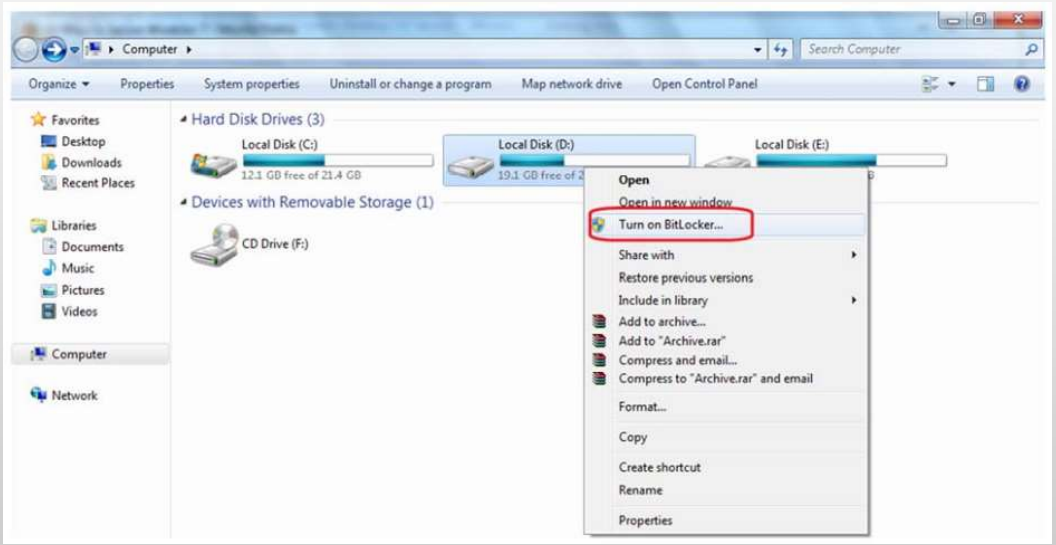
- رمزگذاری فایل سیستم (EFS) برای کاربران این امکان را فراهم می‌آورد که بتوانند فایل‌ها و پوشه‌های خود را در فرمت NTFS رمزگذاری کنند، مراحل رمزگذاری در ویندوز به شرح ذیل می‌باشد:.
- بر روی فایلی که می‌خواهید رمز شود، کلیک راست نموده Properties را انتخاب کنید و سپس بر روی تب General کلیک کرده و دکمه Advance را بزنید.
- در پنجره باز شده، در قسمت Compress or Encrypt attributes دو گزینه وجود دارد.
- تیک گزینه Encrypt contents to secure data، را بردارید.
- بر روی OK کلیک نمایید تا دیالوگ باکس Compress or Encrypt Attributes بسته شود.



فعال‌سازی BitLocker در ویندوز ۷

- BitLocker Drive Encryption با رمزگذاری کل درایو سیستم عامل، امکان محافظت بهتر از داده‌ها را فراهم می‌آورد.
- هر یک از درایوهای هارد دیسک، یا هر رسانه قابل حملی بر روی کامپیوتر می‌تواند رمزگذاری شود.
- هر رسانه قابل حمل رمز شده‌ای در ویندوز ۷ می‌تواند رمزگذاری شود.

Start -> my computer -> Right click on any drive -> select the option Turn on BitLocker

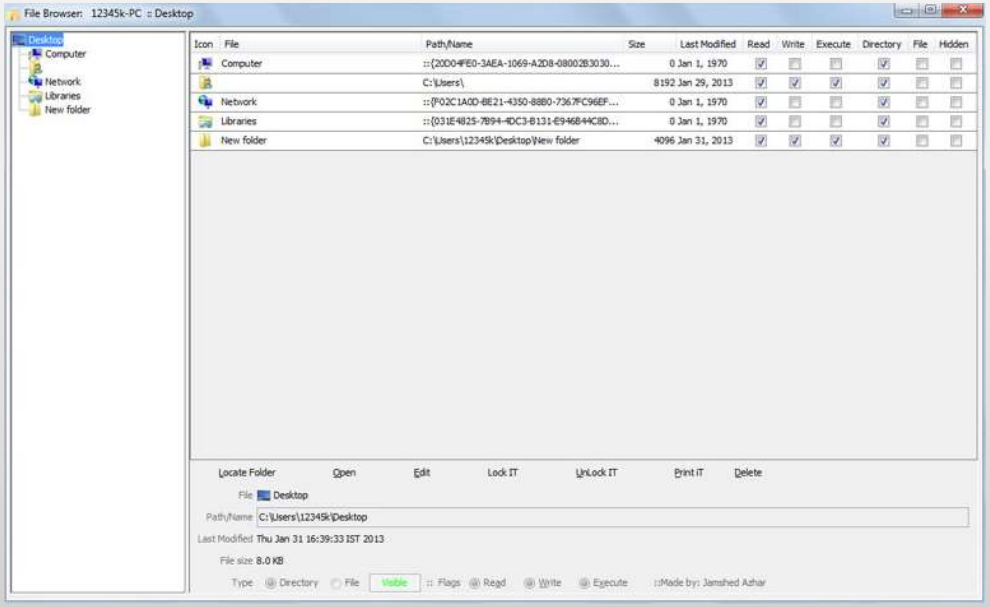


مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

رمز گذاری روی پوشه‌های ویندوز

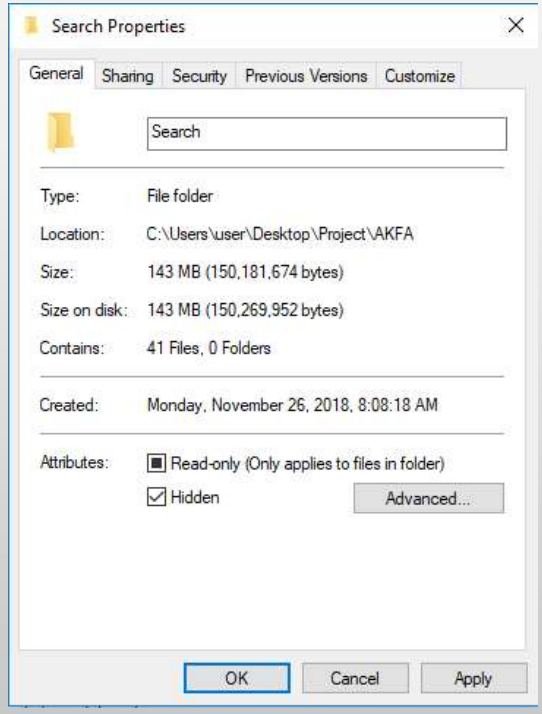
رمزگذاری روی فایل ها و فولدرها از طریق نرم افزار NEO- Easy Folder LOCKER

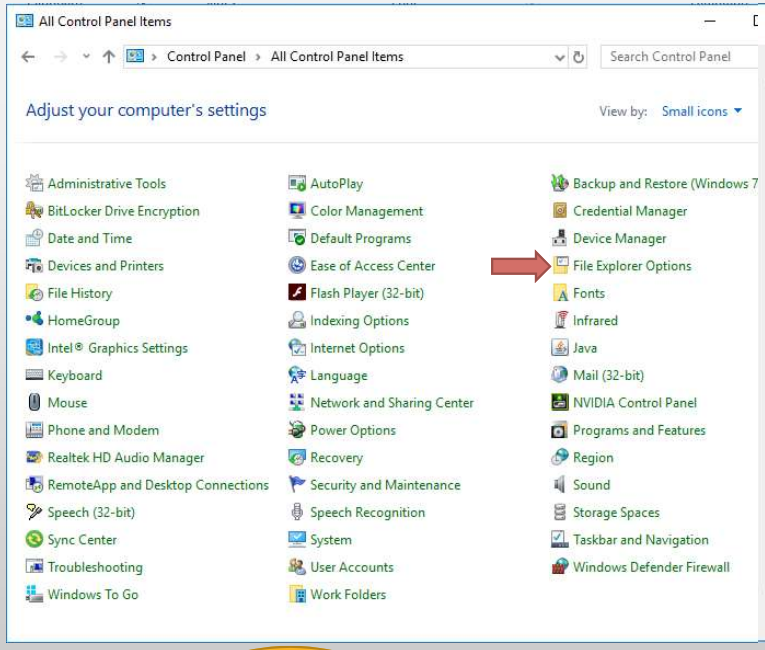


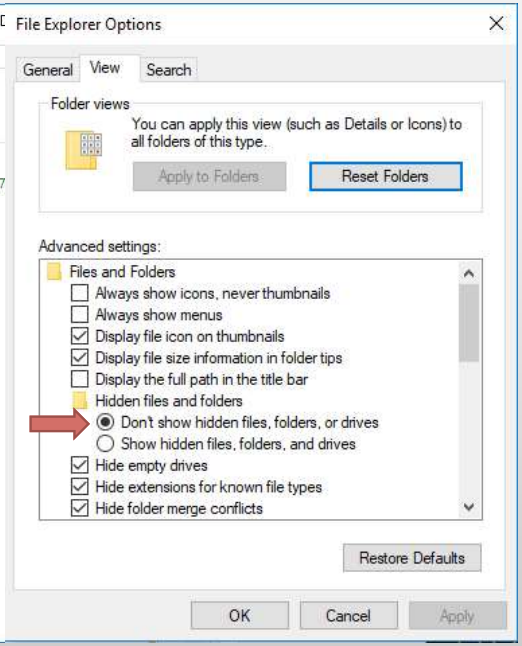
- ✓ NEO- Easy Folder LOCKER یک نرم افزار رایگان است که برای گذاشتن پسورد و قفل کردن آسان فایل ها و فولدرها در ویندوز می‌توانید از آن بهره ببرید.

- ✓ رابط کاربری نرم افزار بسیار ساده است و پس از تنظیم رمز در تنظیمات کافیست فولدر مورد نظر را برای قفل کردن از لیست بالا برنامه انتخاب و گزینه Lock it را بزنید ، برای باز کردن پوشه نیز پوشه را انتخاب و سپس بر روی گزینه Unlock it کلیک کنید.

- بر روی فایل یا پوشه‌ای که می‌خواهید مخفی شود کلیک راست نموده و Properties را انتخاب کنید، در قسمت پایین دیالوگ باکس باز شده زیر قسمت Attributes تیک گزینه Hidden را زده و سپس OK کنید.
- در control panel، File Explorer Options را انتخاب نمایید.
- سپس به تب View رفته و گزینه Do not show hidden files and folders option را تیک بزنید.







مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

پنهان کردن پوشه ها در مک از طریق نرم افزار Hide Folders for macOS

- ✓ Hide Folders for macOS نرم افزاری است رایگان برای کابران سیستم عامل مک که می خواهند از اطلاعات شخصی خود محافظت کنند.
- ✓ این برنامه بسیار ساده و طبیعی است و با یک کلیک فایل ها و پوشه ها و محتویاتشان را مخفی می کند. شما می توانید با استفاده از این برنامه، فایل های خود را از دیده شدن، حذف شدن و ادیت شدن محافظت کنید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

نرم افزارهایی برای پاک کردن ایمن فایل ها از سیستم

- Wise Disk Cleaner پاکسازی کامل هارد دیسک
- Glary Disk Cleaner پاکسازی فایل های بیهوده هارد دیسک
- Glary Tracks Eraserپاکسازی ردپا در ویندوز
- O&O SafeErase All Edition نرم افزار پاکسازی اطلاعات
- Macrorit Data Wiper حذف کامل اطلاعات
- Wipe Pro نرم افزار پاکسازی اطلاعات در ویندوز
- و ...

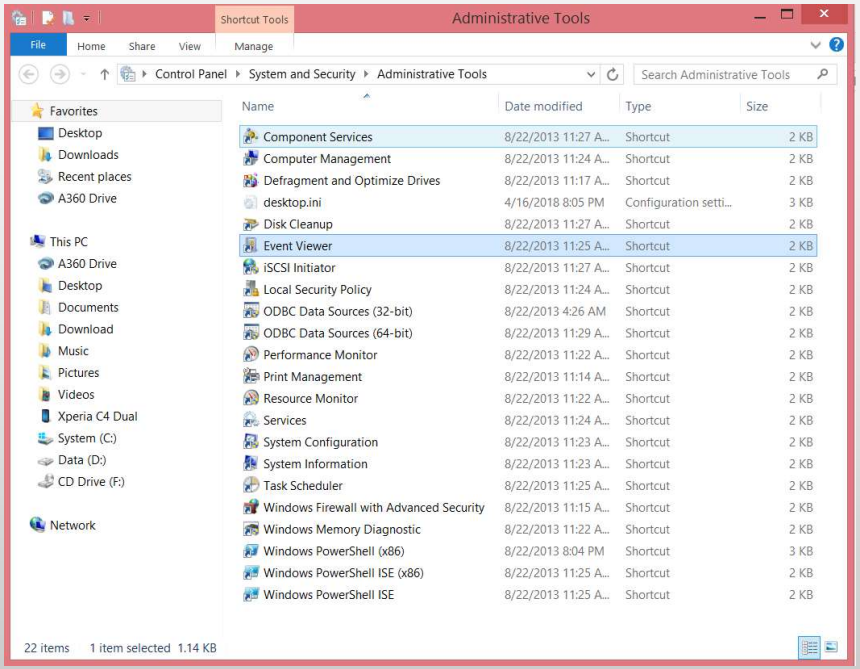
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

راه اندازی Event Viewer در ویندوز

- Event Viewer یک قابلیت درون ساخت در ویندوز است که به کاربر اجازه می‌دهد لاگ‌های سیستم، اطلاعات مربوط به مشکلات سخت‌افزاری و نرم‌افزای و نیز رویدادهای امنیتی ویندوز را مشاهده و مدیریت نمایید.

Start -> Control Panel -> System and Security -> Administrative Tools -> EventViewer



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

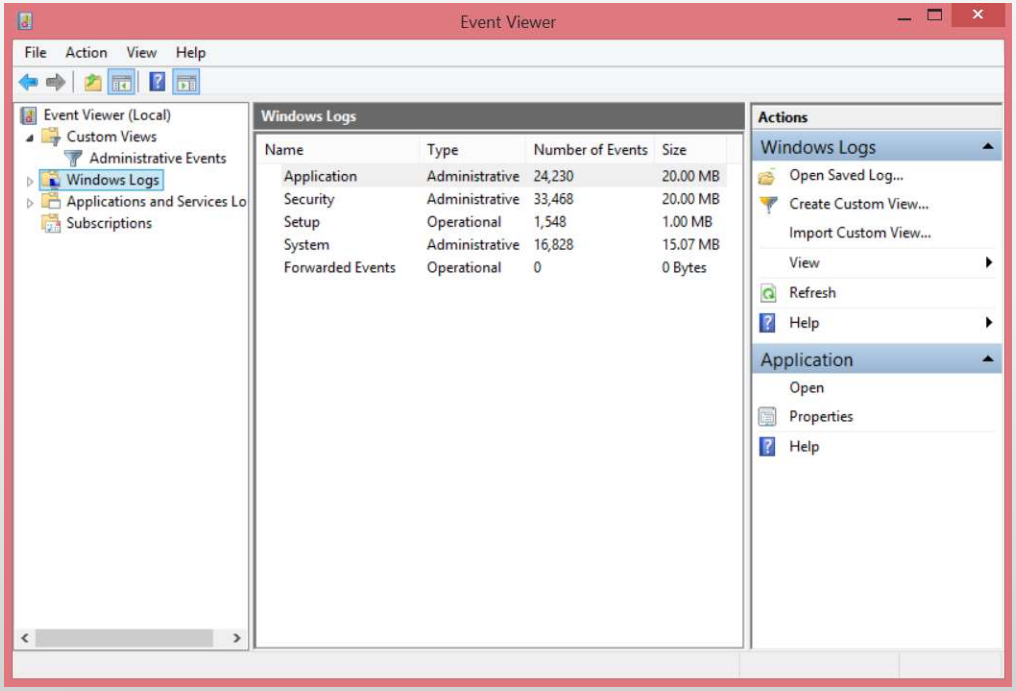
Cybersecurity

رویدادها و نحوه خواندن گزارش‌ها در سیستم

1. Event Viewer رویدادها را به ۵ دسته تقسیم می‌کند:

Error, Warning, Information, Audit Success, Audit Failure

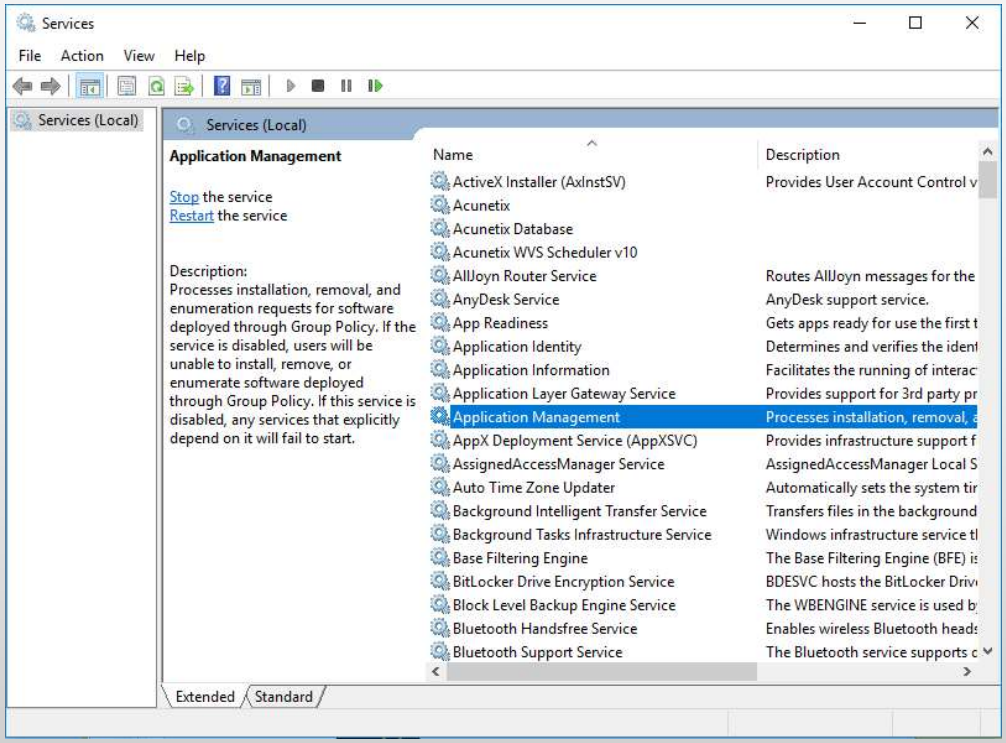
2. هر لاگ رویداد به واسطه سطح، محتویات اطلاعات هدر و شرح آن از سایرین متمایز می‌گردد.
3. هدر هر رویداد حاوی شرح مفصلی از سطح آن، تاریخ، ساعت، منبع، شناسه رویداد و نوع دسته آن می‌باشد.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

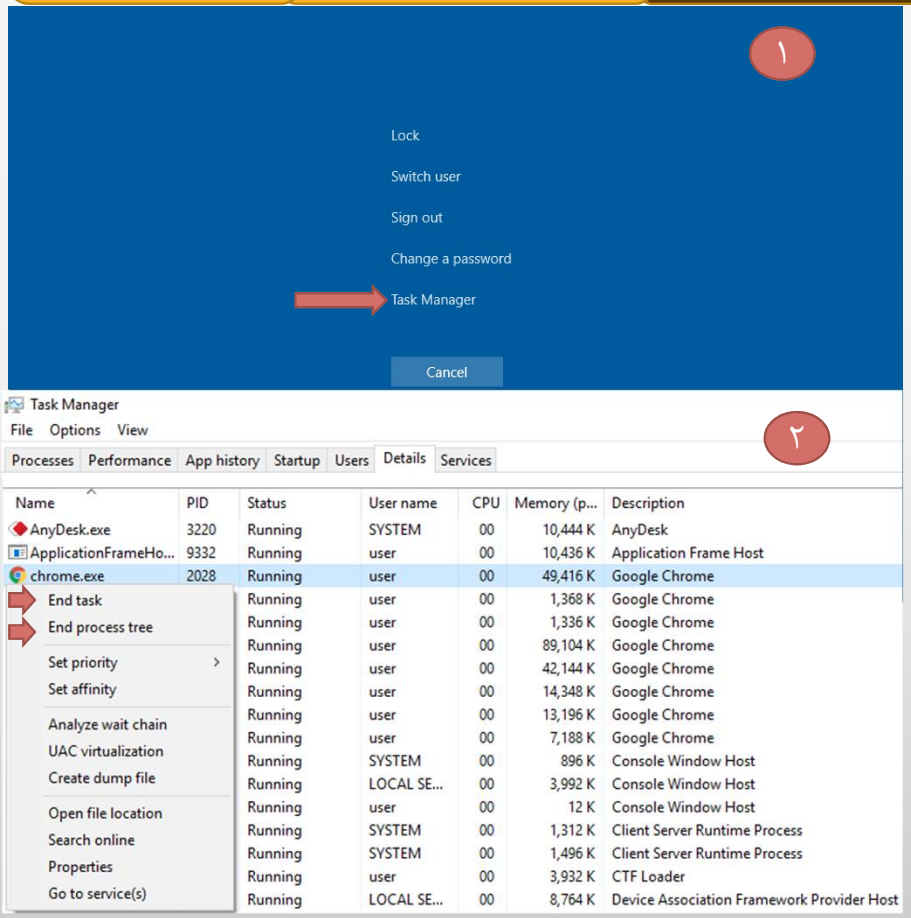
غیرفعال نمودن سرویس‌های غیرضروری در ویندوز



- سرویس، یک برنامه اجرایی است که به طور مداوم در حال اجرا می‌باشد و بدون نیاز به دخالت کاربر کارهای خاصی را انجام می‌دهد.
- سرویس‌ها معمولا با بالا آمدن سیستم یا بوت شدن آن شروع به کار می‌کنند.
- برخی از سرویس‌ها به طور خودکار اجرا می‌شوند، در حالیکه بقیه سرویس‌ها هنگام استفاده از یک برنامه فراخوانی می‌گردند.
- سرویس‌های در حال اجرا را از مسیر زیر می‌توان مشاهده نمود:
- Start -> Control Panel -> Administrator Tools -> double_click Services
- برای مشاهده سرویس‌های در حال اجرا می‌توان از مسیر زیر نیز اقدام نمود:
- بر روی start کلیک نموده و services.msc را در نوار جستجو وارد نمایید و Enter را بزنید تا پنجره سرویس‌های در جال اجرا به شما نشان داده شود.
- در پنجره سرویس‌های در حال اجرا، کاربر می‌تواند سرویس‌های غیرضروری را غیر فعال نماید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity



متوقف نمودن پردازش‌های ناخواسته

- متوقف یا منقضی کردن پردازش‌های غیرضروری یا مشکوک، به منظور بهبود عملکرد سیستم و محافظت از سیستم در مقابل بدافزارها صورت می‌گیرد.

متوقف نمودن یک پردازش

- کلیدهای [alt] + [ctrl] + [del] را همزمان بگیرید.
- بر روی Task Manager کلیک نمایید.
- در پنجره Task Manager بر روی تب Process کلیک نمایید.
- در نهایت بر روی پردازش مورد نظر کلیک راست نموده و گزینه End Process را انتخاب کنید.

متوقف نمودن درخت پردازش

- Task Manager را اجرا نموده، بر روی پردازش مورد نظر کلیک راست کنید و گزینه End Process Tree را انتخاب نمایید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

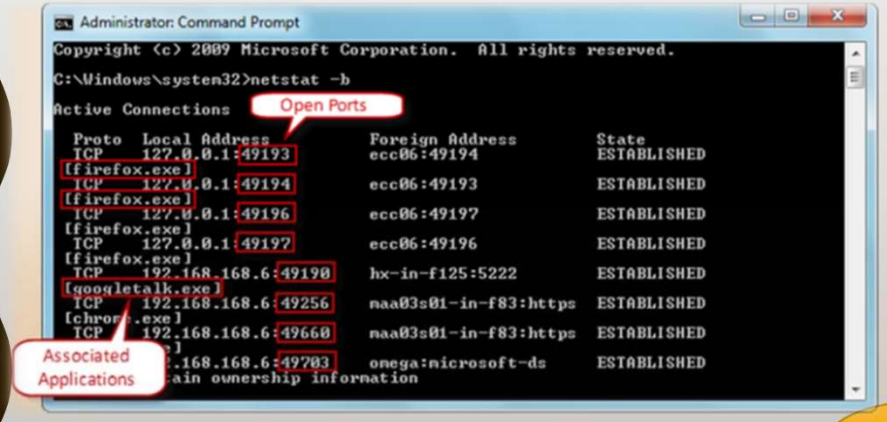
Cybersecurity

یافتن پورت‌های باز با استفاده از Netstat

- آگاهی از پورتهای باز، سرویس‌ها و برنامه‌های مرتبط با پورت‌ها در تشخیص وجود بدافزار در سیستم، مانند ویروس، کرم، تروجان و غیره کمک می‌کند.
- بدافزار معمولا پورت‌ها را برای دریافت یا ارسال بسته‌های داده به مهاجم باز می‌کند.
- Netstate یک قابلیت درون ساخت در ویندوز است که می‌تواند برای تعیین پورت‌های باز در سیستم و برنامه‌های مرتبط با آنها در سیستم مورد استفاده قرار گیرد.
- از مسیر زیر Command Promt را باز کنید:

Start -> type cmd in search bar -> Right click on cmd -> Run as administrator

- دستور netstate -b را در cmd وارد نمایید تا لیست پورت‌های باز و برنامه‌های مرتبط با آن‌ها نشان داده شود.



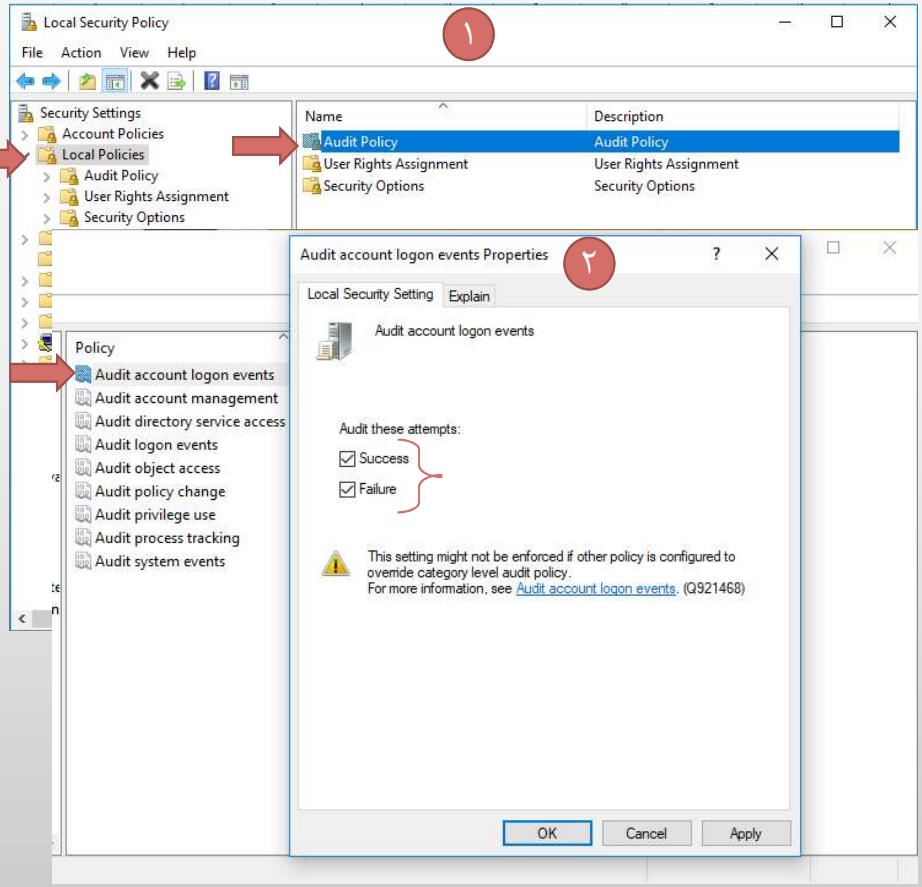
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

پیکربندی سیاست‌های ممیزی

- سیاست‌های ممیزی باید به منظور شناسایی حملات انجام شده و نیز حملات موفقیت آمیز بر روی سیستم و شبکه پیکربندی شوند.

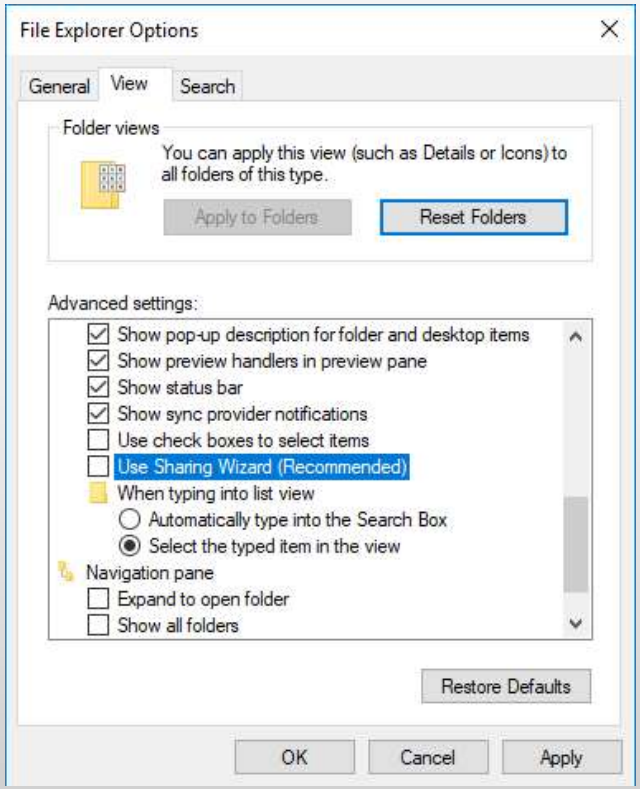
1. بر روی start کلیک نموده و در نوار جستجو secpol.msc را وارد کنید، سپس Enter را بزنید.
2. بر روی Local policies کلیک نموده و Audit policy را انتخاب کنید، سپس بر روی Audit account logon events دابل کلیک نموده و تیک گزینه‌های Success و Failure را بزنید و در نهایت بر روی Apply و OK کلیک نمایید.
3. به طور مشابه تنظیمات امنیتی را برای تمام سیاست‌های لیست شده در سمت راست پنجره Local Security Policy تغییر دهید.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

غیرفعال نمودن به اشتراک گذاری فایل در ویندوز



- به مسیر start -> control panel -> File Explorer Options بروید.
- به تب View بروید.
- در قسمت Advance Settings به بخش انتهایی تنظیمات بروید.
- تیک گزینه Using sharing wizard را برداشته و بر روی OK کلیک نمایید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

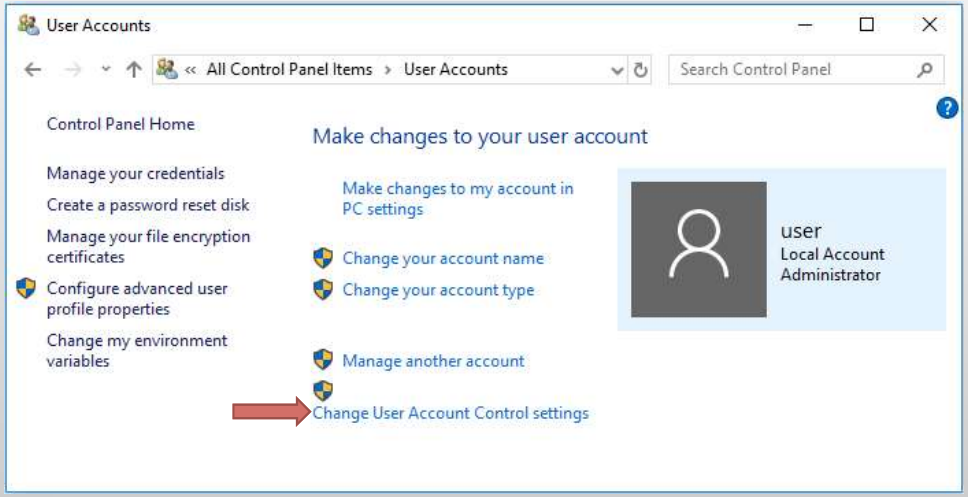
Cybersecurity

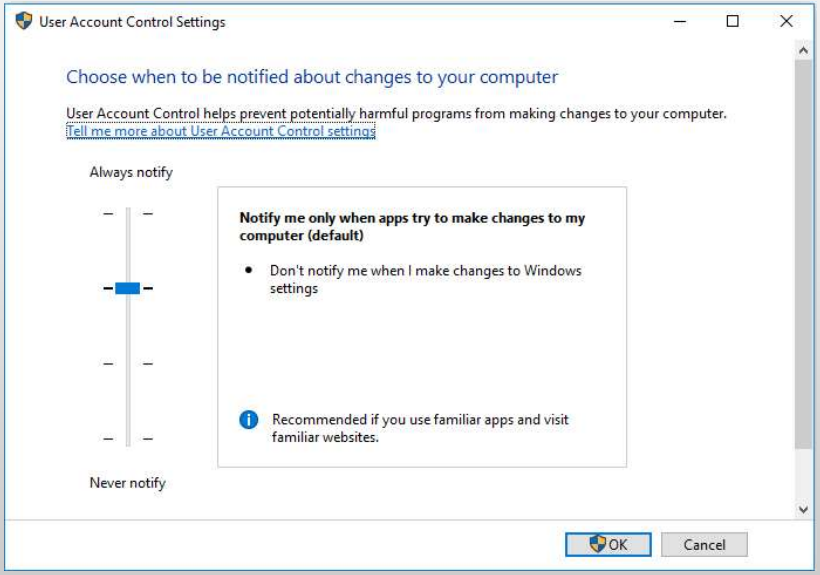
استفاده از کنترل حساب کاربری در ویندوز (UAC)

- کنترل حساب کاربری به کاربر کمک می‌کند تا در هنگام نصب نرم‌افزار تصمیمات مهمی را اتخاذ نماید.
- در مسیر زیر:

Start -> Control Panel -> User Account Control -> Change User Account Control Settings

نوار لغزنده را در بالاترین سطح خود یعنی Always notify me قرار دهید.





مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

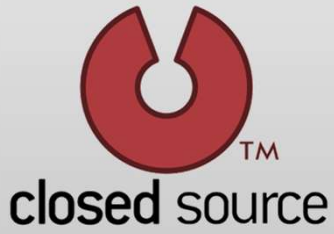
Cybersecurity

Open Source Software یا نرم افزارهای متن باز

- نرم افزار متن باز را می توان نرم افزاری معرفی کرد که تحت یک مجوز (Licence) دارای موافقتنامه انتشار یافته، که اجازه ی به اشتراک گذاری کد منبع (کد کامپیوتری) را جهت مشاهده و انجام تغییرات در آن توسط کاربران و سازمانهای دیگر میدهد.
- مثالهایی از این نوع نرم افزارها می توان به مرورگر موزیلا، لینوکس، جوملا، وردپرس و غیره اشاره کرد.

Closed Source Software یا نرم افزارهای اختصاصی (متن بسته)

- اینگونه نرم افزارها، نرم افزارهایی اختصاصی هستند که تحت یک مجوز دارای موافقتنامه برای انجام تغییرات، توزیع، کپی و انتشار محدود و کنترل شده در اختیار کاربران و سازمانها قرار می گیرند. یا به صورت ساده تر نرم افزارهایی که برای دریافت آنها باید پول پرداخت کنید و اجازه دسترسی به کد منبع برنامه را ندارید.
- مثالهایی از این نوع نرم افزارها می توان به محصولات میکروسافت مانند Office یا شرکت Adobe مانند Photoshop و غیره اشاره کرد.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

مقایسه دو پلتفرم Open source و Closed source

❑ **هزینه**

Open source:

- نرم افزارهای متن باز رایگان هستند.
- کاربر باید سطح تخصص معینی جهت مدیریت محتوای آنها داشته باشد.
- ممکن است هزینه های آموزش کاربران، پیاده سازی، مسائل مربوط به خدمات و پشتیبانی و رشد و توسعه سازمان و بدست آوردن تخصص کار با نرم افزار متن باز از هزینه ی خرید یک نرم افزار Closed Source بیشتر شود.
- ارائه دهندگان نرم افزارهای متن باز به طور فزاینده ای در حال قدرت بخشیدن به نرم افزار های خود بوسیله ی اضافه کردن افزونه ها و خدمات جدید هستند.

Closed source:

- هزینه خرید نرم افزارهای اختصاصی (متن بسته) بسته به پیچیدگی نرم افزار از چند دلار تا چند میلیون دلار متغیر است.
- دارای مجموعه ای از مزایا شامل استفاده از یک نام تجاری معتبر و قابل اعتماد، سطوح بالاتری از امنیت و عملکرد، نوآوری مستمر، آموزش مستمر، پشتیبانی قابل اعتماد و نیاز کمتر به مهارتهای فنی می باشد.
- این موارد می تواند در بلند مدت علاوه بر جبران هزینه های پرداخت شده، ارزش افزوده ای نیز برای سازمان ایجاد کند.

مقایسه دو پلتفرم Open source و Closed source

❑ خدمات و پشتیبانی

Open source:

- این نرم افزارها جهت پشتیبانی و ارائه خدمات به کاربران خود متکی به شبکه های اجتماعی آنلاین مانند انجمن ها و وبلاگها هستند.
- امروزه با توجه به کمبود زمان، مصرف کنندگان نیاز به خدمات و پشتیبانی فوری دارند تا مشکلاتشان در اسرع وقت حل و فصل شود.
- این جوامع آنلاین نمی تواند به اندازه کارشناسان آماده به پاسخگویی نرم افزارهای اختصاصی، پشتیبانی به موقع و سریع را تضمین نماید.

Closed source:

- حمایت مداوم از کاربرانی است که بدون داشتن مهارت فنی می توانند بدون دلهره از نرم افزارهای آنها استفاده کنند.
- قابلیت برقرای تماس فوری و در لحظه با سازنده ی نرم افزار جهت حمایت و پشتیبانی است.
- خدمات و پشتیبانی سریع و به موقع یکی از دلایل اصلی کاربران برای انتخاب این نرم افزارها است.

مقایسه دو پلتفرم Open source و Closed source

❑ ابداع و نوآوری

Open source:

- نرم افزارهای متن باز با ایجاد آزادی عمل و انعطاف پذیری فراوان این امکان را به کاربران می دهند تا بتوانند بدون محدودیت به نوآری و ابداع های جدید دست بزنند.
- نوآوری و ابداع در این دسته از نرم افزارها(متن باز) وابستگی شدیدی به میزان فعال بودن کاربران آنها در جوامع آنلاین دارد.
- شخصی سازی های انجام شده بر روی کد منبع اصلی ممکن است آینده پشتیبانی و توسعه نرم افزار را محدود کند. که بستگی مستقیم به تلاش ارائه دهندگان نرم افزارهای متن باز برای بزرگ کردن مقیاس R&D تشکیلاتشان دارد.

Closed source:

- اجازه ی تغییر کد منبع را به کاربران خود نمی دهند.
- عدم تغییر کدها باعث تضمین امنیت و قابل اطمینان بودن نرم افزار می شود.
- در جوامع آنلاین متمرکز ایده های کاربران به اشتراک گذاشته می شود.
- ابداعات بصورت کامل مورد آزمایش قرارگرفته و ثانیا در اختیار تمام کاربران نرم افزار قرار می گیرد.
- در نرم افزارهای متن باز نوآوری بیشتر تکنیک محور است امادر نرم افزارهای اختصاصی(متن بسته) تجارت محور.

مقایسه دو پلتفرم Open source و Closed source

❑ قابلیت استفاده

Open source:

- ازنرم افزارهای متن باز به علت عدم قابلیت استفاده پذیری بسیار انتقاد شده است.
- این نوع نرم افزارها اکثرا برای کسانی بوجود می آیند که تخصص رفع خطا و یا تغییر کد ودستکاری آنها را داشته باشند.
- علاوه بر اینها، اینگونه نرم افزارها بصورت قانونی موظف به داشتن راهنمای کاربری نیستند.
- زمانی که مستنداتی ارائه می شود اغلب شامل یکسری اصطلاحات مخصوص برای متخصصان خواهد بود.
- بدون مستندات کافی، کاربر باید بر جایگزین هایی مانند جوامع آنلاین تکیه کند با این فرض که یک نفر قبلا این مشکل را داشته و به او پاسخ داده شده است.

Closed source:

- زیر نظر کارشناسان متخصص جهت قابل استفاده بودن مورد تست و بررسی تخصصی قرار می گیرند و هدف نهایی کاربران هستند.
- طراحی نرم افزار بگونه ای خواهد بود که کاربر را بیشتر راضی کرده و استفاده پذیری آن بسیار بالا می رود.
- کتابچه راهنمای جامع و خدمات حمایتی شامل سمینارها، دوره های آموزشی هدفمند و پشتیبانی گسترده نیز جهت به حداکثر رساندن استفاده پذیری نرم افزار وجود دارد.
- درحالی که بسیاری از مردم این نرم افزارها را بسته می بینند، ارائه دهندگان این نرم افزار ها ، مکانیزم وسیعی را جهت بهبود آنها توسط توسعه دهندگان و سیستم‌های third party در اختیار گذاشته اند.

مقایسه دو پلتفرم Open source و Closed source

❑ امنیت

Open source:

- نرم افزارهای متن باز اغلب به داشتن مشکلات و مسائل امنیتی مشهور هستند.
- اینگونه نرم افزارها لزوما در یک محیط کنترل شده توسعه نیافته اند.
- این نرم افزارها اغلب بصورت کامل بازبینی و تصحیح نمی شوند پس امکان اینکه یک برنامه نویس که در توسعه نرم افزار مشارکت داشته و کدی را در نرم افزار گنجانده باشد تا بوسیله ی آن بتواند از اطلاعات شما سوء استفاده نماید، وجود دارد.
- اتخاذ یک نام تجاری معتبر با یک تیم توسعه متمرکز و پشتیبانی شده توسط جامعه آنلاین می تواند این خطر بالقوه را کاهش دهد.

Closed source:

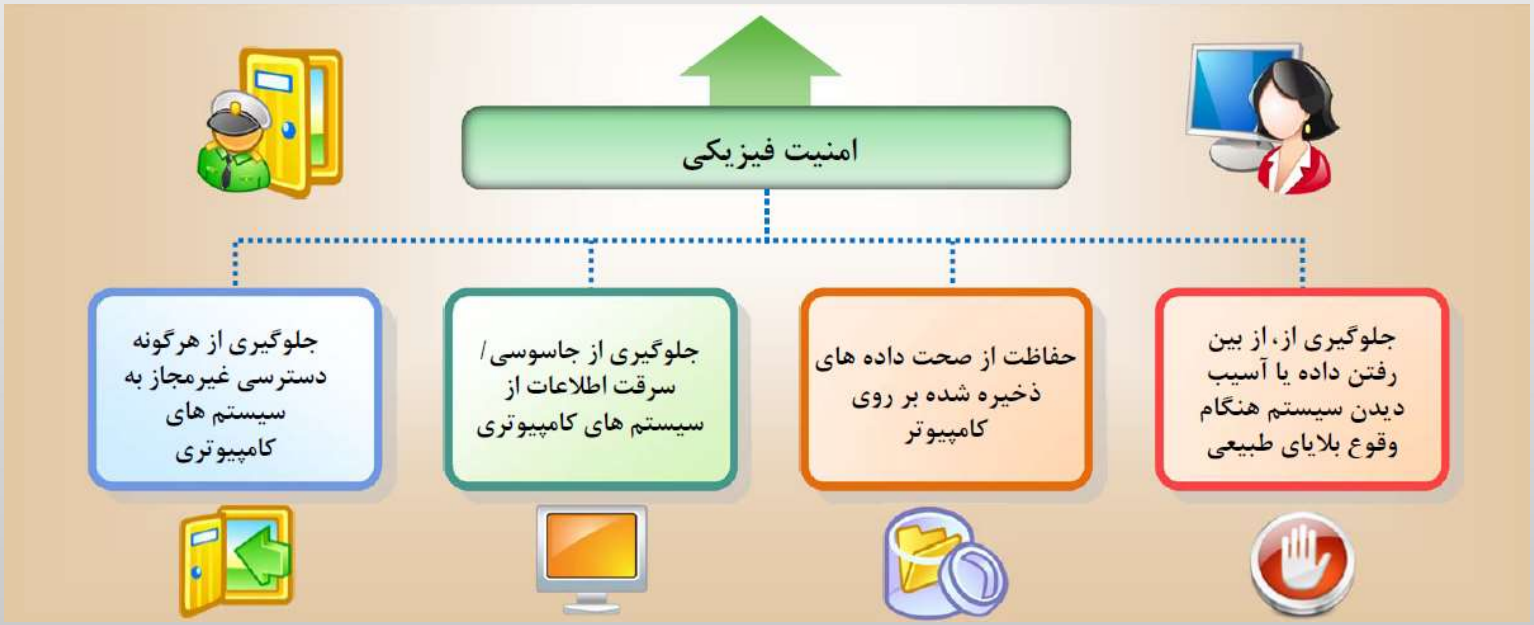
- نرم افزارهای اختصاصی امن تر است به این دلیل که در یک محیط کنترل شده توسط یک تیم متمرکز با مسیر مشترک توسعه یافته است.
- علاوه بر این بازبینی و تست کد منبع توسط این تیم خطر وجود back doorها و هرگونه اشکالات را بشدت کاهش می دهد.

مقایسه دو پلتفرم Open source و Closed source

❑ نتیجه گیری

- به نظر می‌رسد استفاده از هریک از این دو پلتفرم در جای مناسب می تواند بسیار مفید باشد.
- نرم افزارهای متن باز (open source) را می‌توان در جایی که فاکتورهایی همچون امنیت و پشتیبانی دارای اهمیت کمتر و هزینه کم دارای اهمیت بیشتر باشد، بکار برد.
- اما در مکانهایی همچون سازمانها نمی‌توان این ریسک را انجام داد و بهتر است بیشتر روی نرم افزارهای اختصاصی (closed source) تکیه کرد که دارای قابلیت اطمینان بیشتری هستند.

- امنیت فیزیکی، اولین لایه حفاظتی برای کامپیوتر و داده‌هاست.
- امنیت فیزیکی شامل حفاظت از دارایی‌هایی مانند سخت افزار، شبکه و داده در مقابل حملاتی است که موجب از بین رفتن یا آسیب دیدن آن‌ها می‌شوند
- عوامل مختلفی وجود دارند که می‌توانند امنیت فیزیکی را تحت تاثیر قرار دهند، مانند خرابی، سرقت، گرد و غبار، آتش سوزی، سیل، زلزله و غیره



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

اقدامات لازم جهت برقراری امنیت فیزیکی: قفل

- قفل‌ها به عنوان اولین روش کنترل دسترسی فیزیکی برای سیستم‌های اطلاعاتی و سایر دستگاه‌های ذخیره‌سازی قابل جابه‌جایی در نظر گرفته می‌شوند.
- قفل‌ها با توجه به نحوه‌ی طراحی و پیاده‌سازی، سطوح امنیتی مختلفی ارائه می‌کنند.

قفل‌ها استفاده می‌شوند برای:

- محدود نمودن افراد غیرمجاز برای استفاده از اتاق کامپیوتر
- جلوگیری از دسترسی غیرمجاز به کامپیوتر، توسط قفل نمودن درها و پنجره‌های محلی که کامپیوتر در آنجا قرار دارد
- قفل کردن CPU و مانیتور به منظور جلوگیری از به سرقت رفتن آنها

Lock Computer (WIN-L)

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

اقدامات لازم جهت برقراری امنیت فیزیکی: بیومتریک

بیومتریک به شناسایی و تشخیص هویت افراد براساس خصوصیات آنها اشاره دارد.

تکنیک‌های تشخیص بیومتریک

- اثر انگشت
- اسکن شبکیه
- اسکن عنبیه
- تشخیص براساس ساختار رگ
- تشخیص چهره
- تشخیص صدا

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

اقدامات لازم جهت برقراری امنیت فیزیکی:جلوگیری از آتش سوزی

آتش‌سوزی ممکن است به علت یک اتصال کوتاه رخ دهد و موجب به بار آمدن خسارات سنگین و جبران‌ناپذیر گردد.

اقدامات لازم جهت پیشگیری از آتش‌سوزی

- اتاق را عاری از گرد و غبار نگه داشته و در اسرع وقت وسایل اضافی و اوراقی را دور بیندازید.
- از تجهیزاتی که موجب شوک الکتریکی می‌شوند استفاده نکنید.
- از سیم‌کشی درست و ابزار و تجهیزات خوب استفاده کنید.
- اطمینان حاصل کنید که تمام درب‌ها و راه‌روهای اضطراری مشخص شده باشند.
- باید نحوه‌ی استفاده از کپسول آتش‌نشانی را بدانید.
- کاربران باید بدانند که در شرایط اضطراری با چه کسی باید تماس بگیرند.
- در انتهای روز حتما لوازم برقی را از برق بکشید.
- اطمینان حاصل کنید که سطل زباله به طور مرتب خالی می‌شود.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

امن‌سازی لپ‌تاپ‌ها برای جلوگیری از سرقت

سرقت لپ‌تاپ‌ها منجر به افشای اطلاعاتی مانند نام‌های کاربری، پسوردها، داده‌های محرمانه و نیز جزئیات شبکه‌ی شرکت با محیطی که لپ‌تاپ به آن متصل شده است می‌گردد.

امنیت لپ‌تاپ

نبایدها

- ✓ لپ‌تاپ را بدون مراقبت در اتومبیل، خارج از محل کار/ منزل رها نکنید.
- ✓ رمز عبور را فراموش نکنید و از به اشتراک گذاشتن آن با دیگران جدا اجتناب نمایید.

بایدها

- ✓ شماره سریال لپ‌تاپ را به خاطر سپرده و آن را ایمن نگه دارید.
- ✓ یک پوشش برای لپ‌تاپ در نظر بگیرید تا بتوانید آن را به راحتی تشخیص دهید.
- ✓ در صورت به سرقت رفتن لپ‌تاپ سریعا سرقت را گزارش نمایید.

اقدامات مقابله با سرقت لپ‌تاپ

- بر روی لپ‌تاپ خود ابزارهای ردیابی نصب کنید تا در زمان به سرقت رفتن لپ‌تاپ بتوانید مکان آن را ردیابی کنید.
- از امنیت مبتنی‌بر سخت‌افزار قوی استفاده کنید.
- برای لپ‌تاپ خود بیمه کامپیوتر تهیه کنید.
- برای داده‌های بسیار حساس یک third-party privacy protection در نظر بگیرید.
- برای تنظیمات بایوس لپ‌تاپ خود یک رمز عبور در نظر بگیرید.
- داده‌های حساس را رمزگذاری نموده و از هر آنچه که در لپ‌تاپ وجود دارد پشتیبان تهیه کنید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

با تشکر از توجه شما

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508