کلیات دوره امنیت کاربری فناوری اطلاعات (اکفا)

- کلیات امنیت سایبری
- بهداشت سایبری
- امنیت سایبری در سازمان‌ها
- امنیت در شبکه‌های اجتماعی
- مهندسی اجتماعی
- آشنایی با نهادهای متولی امنیت سایبری
- مفاهیم حقوقی فضای سایبری

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

کلیات امنیت سایبری

- **فضای سایبری**
  - ✓ فضای سایبری به مجموعه ای اطلاق میگردد که شامل:

    زیر ساخت های فناوری اطلاعات، شبکه های ارتباطی آن، سامانه های رایانه ای باشد.
  - ✓ این فضا ممکن است به صورت مستقیم به اینترنت متصل باشد و یا تنها در محیط‌های خاص قابل دسترس باشند.

- **حمله سایبری**
  - ✓ به هر گونه اقدام غیر مجاز سایبری، که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دست یابی به اطلاعات سرمایه ملی سایبری مذکور انجام گیرد، حمله سایبری اطلاق می گردد.

- **سه مشخصه حملات سایبری**
  1. گستردگی
  2. نهفتگی
  3. تنوع
- **سرمایه‌های سایبری**
  - ✓ به تمامی داده‌ها و اجزای سامانه‌های سایبری که در یک ساختار وجود دارند سرمایه سایبری اطلاق می‌شود.
  - ✓ شامل زیرساخت‌ها و اطلاعات در شبکه‌های اطلاعاتی و نیز ساختارهای اداری در یک نظام اقتصادی می‌شود.

- **آسیب‌پذیری سایبری**
  - ✓ چنانچه ضعف موجود در داخل سامانه سایبری موجب از بین رفتن سرمایه سایبری و یا اختلال در روند اجرای آن شود.
- **منشاء آسیب‌پذیری‌های سایبری**
  - ✓ ضعف موجود در فناوری مورد استفاده در سامانه سایبری موردنظر، ضعف پیاده‌سازی (تولید) سامانه سایبری موردنظر،ضعف تنظیمات و بهره‌برداری از سامانه سایبری مورد نظر
- **مخاطره سایبری**
  - ✓ به احتمال بهره برداری یک تهدید سایبری از یک یا چند آسیب پذیری سایبری موجود به منظور تخریب، ایجاد اختلال، دسترسی غیر مجاز، افشای اطلاعات، دستکاری اطلاعات یا ممانعت از ارائه خدمات محسوب می شود.

- **شدت تهدید سایبری**

تهدیدات سایبری علیه سرمایه‌های ملی سایبری، در پنج سطح طبقه‌بندی می‌گردند:

خیلی زیاد(فاجعه)، زیاد (بحران)، متوسط (حادثه امنیتی عمده)، کم (حادثه امنیتی) و خیلی کم (رویداد امنیتی)

- دو قسم از تدابیر برای تامین امنیت در فضای سایبری را می‌توان در نظر گرفت:

1. **تدابیر مستقیم یا اصلی:** این تدابیر به کلیه ی تدابیر فنی و قانونی گفته می‌شود که برای تامین امنیت دو موضوع زیر به کار می‌آید:
   I. داده‌ها و اطلاعات رایانه‌ای
   II. سیستم‌ها و شبکه‌های رایانه‌ای و مخابراتی
2. **تدابیر واسطه‌ای:** این تدابیر در پی تنظیم مقررات مناسب برای فضای سایبری است تا به واسطه‌ی آن هدف اصلی یعنی امنیت فضای واقعی تامین شود.

- ✓ جهانی و فرامرزی بودن
- ✓ دستیابی آسان به آخرین اطلاعات
- ✓ جذابیت
- ✓ آزادی اطلاعات و ارتباطات
- ✓ چند وجهی و متنوع بودن
- ✓ سهولت انجام جرم
- ✓ عدم شناسایی آسان مجرمان
- ✓ تأثیر گذاری شگرف

Cybersecurity

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

- ✓ نبود الزام روشن برای طراحی
- ✓ کاهش عملکرد سیستم‌های قدیمی در صورت ارتقا ایمنی آنها
- ✓ افزایش ابزارهای پیچیده‌ی هکرها
- ✓ اشتراک گذاری ناکافی اطلاعات
- ✓ هماهنگی ضعیف دولت و صنعت
- ✓ درک ضعیف از خطرات سایبری
- ✓ سرمایه گذاری کم در امنیت سایبری

- ✓ توانایی محدود برای اندازه‌گیری و ارزیابی وضعیت امنیتی سایبری
- ✓ نداشتن معیارهای امنیت سایبری
- ✓ دشواری اثبات و اندازه‌گیری تهدیدات
- ✓ رشد تهدیدات با افزایش سیستم‌های متصل به هم
- ✓ ارتباطات طراحی شده نامناسب بین سیستم‌های کنترلی و شبکه‌های سامانی

Cybersecurity

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

حوزه های تهدید

- ✓ تهدیدات فرهنگی جامعه از قبیل رواج بی بندوباری، ایجاد بی اعتقادی، سست کردن باورهای مذهبی، تهاجم فرهنگی
- ✓ تهدیدات اجتماعی جامعه از قبیل بسیج و سازماندهی اغتشاشات و ناآرامی‌های مختلف در کشور و یا تشکیل و هدایت گروه‌های منحرف
- ✓ تهدیدات سیاسی از قبیل انجام اقدامات هماهنگ علیه یک کشور
- ✓ تهدیدات اقتصادی و مالی از قبیل اعمال تحریم‌های اقتصادی از طریق فضای مجازی از قبیل ممانعت از خرید و فروش اینترنتی کالا و خدمات یا جلوگیری از نقل و انتقالات پولی و بانکی
- ✓ تهدیدات امنیتی از قبیل تروریسم سایبری

منابع تهدید

منبع تهدید	توصیف
کشورهای خارجی	در سطح جهان موارد متعددی از این دست برای سوء استفاده و تخریب زیرساخت‌های اطلاعاتی کشورها شامل اینترنت، شبکه‌های اطلاعاتی، سامانه های رایانه ای و پردازشگرها و کنترل‌کننده های نهفته در صنایع حیاتی مشاهده شده است.
گروه های خرابکار	به طور روزافزون تهاجمات سایبری این گروه ها که به منظور کسب درآمد به سامانه های سایبری حمله می برند رو به افزایش است.
هکرها	هکرها گاهی اوقات برای اظهار وجود خود وارد شبکه می‌شوند.
هکرهای سازمان یافته	این افراد معمولاً میزبان‌های پست الکترونیک را با افزایش بار مواجه نموده و با نفوذ به سایت‌های شبکه وب پیام‌های سیاسی خود را اعلام می‌نمایند.
عوامل ناراضی داخلی	این دسته از عوامل لازم نیست دانش قابل توجهی در خصوص تهاجمات رایانه‌ای داشته باشند زیرا اطلاع آنها از سیستم مورد هدف غالباً امکان دسترسی نامحدود برای وارد کردن ضربه به سامانه و یا سرقت اطلاعات سازمان را فراهم می سازد.
تروریست‌ها	تروریست‌ها به دنبال تخریب، ناتوان‌سازی و یا بهره‌برداری بدخواهانه از زیرساخت‌های حیاتی به منظور تهدید کردن امنیت ملی، وارد آوردن خسارات سنگین، تضعیف اقتصاد کشور و تخریب روحیه و اعتماد عمومی می‌باشد.

سازوکارها و روش‌های تهدید

نوع حمله	توصیف
انکار خدمات	در این روش دسترسی سامانه به کاربران مجاز و بالعکس از دست می‌رود. در واقع حمله کننده از یک نقطه شروع به غوطه ور کردن کامپیوترهای هدف در پیام های مختلف و انسداد آمد و شد قانونی داده ها می نماید.
انکار توزیع شده خدمات	در این روش به جای شروع حمله از یک منبع، همزمان از تعداد زیادی سامانه توزیع شده اقدام به حمله می‌کنند. غالباً این کار با استفاده از کرم‌ها و تکثیر آنها در رایانه‌های متعدد برای حمله به هدف صورت می‌گیرد.
ابزارهای سوء استفاده	این ابزار ها در دسترس عموم قرار دارد که می‌توانند با برخورداری از سطوح مهارتی مختلف آسیب‌پذیری‌های موجود در شبکه‌ها را کشف و از آن طریق وارد شوند.
بمب منطقی	نوعی خرابکاری که در آن برنامه نویس کدی وارد برنامه می‌کند که در صورت بروز اتفاقی خاص برنامه خود به خود یک فعالیت تخریبی را صورت می‌دهد.
اسنیفر	برنامه‌ای است که داده‌های مسیریابی شده را شنود نموده و با بررسی هر بسته در جریان داده‌ها به دنبال اطلاعات خاصی مانند کلمه‌های عبور می‌گردد.

سازوکارها و روش‌های تهدید

نوع حمله	توصیف
ارسال هرزنامه	ارسال نامه‌های پست الکترونیک تجاری ناخواسته که می‌تواند حاوی سازوکار تحویل نرم افزار های مخرب و سایر تهدیدات سایبری باشد.
سرقت کلمه های عبور و اطلاعات مالی	با استفاده از هرزنامه افراد را فریب می‌دهد تا اطلاعات حساس خود را افشا نمایند.
ساخت وب سایت جعلی	ایجاد یک وب سایت فریب برای تقلید از یک سایت واقعی و مشروع.
فریب	روشی که دزدان کلمه عبور برای فریب کاربران و متقاعد کردن آنها از ارتباط با وب سایت معتبر بکار می‌برند.
بات نت	بات‌ها معمولاً به صورت مخفیانه در سامانه هدف نصب می‌شوند و امکان کنترل از راه دور رایانه مورد هدف را به کاربر غیر مجاز می‌دهند تا اهداف خرابکارانه خود را محقق کنند.

انواع نفوذ گران و بازیگران تهدید

گروه نفوذگران کلاه صورتی

- این افراد آدم‌های کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کنند.

گروه نفوذگران کلاه خاکستری

- اشخاصی هستند که حد وسط دو تعریف کلاه سفید و سیاه می‌باشند.

گروه نفوذگران کلاه سیاه

- اشخاصی هستند که وارد رایانه قربانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن بدافزار و غیره می‌پردازند.

گروه نفوذگران کلاه سفید

- هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند که در حقیقت متخصصین شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا کرده و به مسئولان گزارش می‌دهند.

انگیزه‌های تهدید

- تجاری
- مالی
- تلافی جویانه
- تفننی

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

Cybersecurity

Computer Emergency Response Team (CERT)

- اهداف CERT عبارتند از:
  - محافظت از سرمایه‌های حساس اطلاعاتی
  - ایجاد چارچوبی برای ساخت قابلیت اطمینان و پاسخ مناسب به حوادث
  - تمرکز مدیریت تداوم کسب و کار به تعریف تأثیر بالقوه تهدیدات متوجه تداوم فعالیت‌های کسب و کار
  - پاسخ مناسب به ریسک‌های در حال تغییر به‌طور مداوم
  - ایجاد ساختار پاسخ و بازیابی از حوادث و خرابی‌ها
  - ایجاد آمادگی برای پاسخ به حادثه قبل از آنکه منجر به توقف سرویس گردد
  - ایجاد اطمینان از تداوم فعالیت‌های حیاتی کسب و کار که توسط خدمات فناوری اطلاعات پشتیبانی می‌شوند.

Cybersecurity

مرکز تخصصی آپا
دانشگاه تحصیلات تکمیلی
صنعتی و فناوری پیشرفته

بهداشت سایبری

هر سیستم عامل و برنامه کاربردی در معرض خطر نقص های امنیتی است

عرضه کنندگان نرم افزار معمولاً برای رفع نقص های امنیتی وصله ارائه می کنند

با نصب به موقع وصله های امنیتی می توان از تسخیر سیستم جلوگیری نمود

کاربران باید وصله های امنیتی را نصب نموده و نرم افزار را پیکربندی نمایند

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

Cybersecurity

راه‌های ایجاد امنیت در سیستم‌های خانگی و اداری

- نصب نسخه اصلی:
  - آنتی ویروس
  - نرم افزار ضد جاسوسی
- به روز رسانی مستمر نرم افزارها
- امنیت رمز عبور
- ذخیره‌سازی فایل های مهم و حساس در رسانه‌های قابل حمل مثل کول دیسک‌ها و سی دی و ...
- رمز نگاری پیشرفته پوشه ها و فایل‌ها

راه‌های ایجاد امنیت در سیستم‌های اداری

- ✓ راه اندازی شبکه داخلی یا اینترانت
- ✓ ذخیره سازی اطلاعات حساس و مهم کاری بر روی حافظه های جانبی
- ✓ حفاظت فیزیکی از حافظه های جانبی
- ✓ بخش بزرگی از امنیت اطلاعات مهم و محرمانه در محیط کار مثل شبکه های کامپیوتری، امنیت نرم افزار و بانک اطلاعاتی و... بر عهده مسئولین IT است.
- ✓ حفاظت فیزیکی سیستم های اداری با حراست ادارات می باشد.
- ✓ باز نکردن نامه ها و ایمیل های دریافتی از منابع ناشناس
- ✓ خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه
- ✓ قطع اتصال به اینترنت در مواقع عدم استفاده
- ✓ گرفتن منظم وصله های امنیتی Patches
- ✓ حصول اطمینان از آگاهی کاربران از نحوه برخورد با کامپیوترهای آلوده
- ✓ بررسی مرتب میزان دریافت و ارسال اطلاعات

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

Backdoor

یک شیوه غیرمجاز برای دسترسی به سیستم و دور زدن مکانیزم های امنیتی آن

Worm

یک ویروس خود تکثیر که فایل ها را تغییر نمی دهد اما در حافظه کامپیوتر مستقر شده و خود را تکثیر می نماید

Virus

برنامه ای که با کپی کردن خود در برنامه های دیگر، سکتورهای بوت سیستم یا داکیومنت ها تکثیر شده و فایل های کامپیوتر و نیز اپلیکیشن ها را تغییر می دهد و یا به آن ها آسیب می رساند

Logic Bomb

برنامه ای که یک ویروس یا کرم را منتشر می کند

Trojan

برنامه ای که مجاز به نظر می رسد اما پس از اجرا اقدامات مخرب انجام می دهد

Rootkit

مجموعه ای از برنامه ها یا ابزارها که دسترسی به سطح روت را در سیستم فراهم می کنند

Cybersecurity

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

جاسوس افزار

جاسوس افزارها شامل تروجان‌ها و سایر نرم‌افزارهای مخرب هستند که بدون اطلاع کاربر اطلاعات شخصی وی را از سیستم سرقت می‌نمایند. مانند: کی لاگر

کی لاگر

کی لاگر یک دستگاه سخت افزاری یا یک برنامه نرم افزاری کوچک است که هر کلیدی را که بر روی صفحه کلید کاربر فشرده می‌شود ثبت می‌کند.

کرک پسورد

کرک پسورد فرآیند شناسایی یا بازیابی یک پسور ناشناخته یا فراموش شده است.

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

کرک پسورد

Guessing

حدس زدن

تست کردن پسوردهای مختلف تاازمانی که یکی از آن ها درست باشد

5

Brute Forcing

بروت فورس

تلاش برای ترکیب کاراکترهای مختلف تا زمانی که پسورد صحیح پیدا شود

4

Dictionary Attack

حمله دیکشنری

از لیستی از کلمات از پیش تعریف شده برای یافتن پسورد استفاده می کند

3

Shoulder Surfing

مخفیانه نگاه کردن

مخفیانه نگاه کردن به کسی که در حال وارد نمودن پسورد است

2

Social Engineering

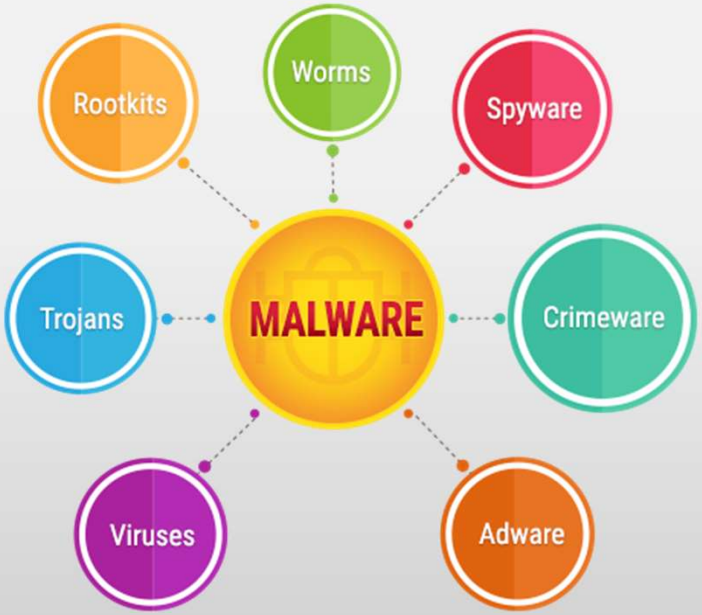
مهندسی اجتماعی

فریب دادن افراد برای فاش کردن پسورد یا سایر اطلاعاتی که به حدس پسورد کمک می‌کنند

1

بدافزار چیست؟

- بدافزارها یا Malware ها برنامه‌های کوچک و البته مخربی هستند که می‌توانند اطلاعات شما را نابود کنند یا در کار با رایانه اختلال ایجاد کنند.
- بدافزارها معمولا برای اهداف جاسوسی و سرقت اطلاعات تنظیم می‌شوند و می‌توانند هویت کاربران را نیز در خطر قرار دهند.



از طریق پیوست‌های ایمیل

ایمیل‌های دارای پیوست ممکن است حاوی بدافزار باشند.

با کلیک بر روی پیوست یک برنامه مخرب بر روی کامپیوتر نصب می‌گردد.

از طریق کارت حافظه‌های USB

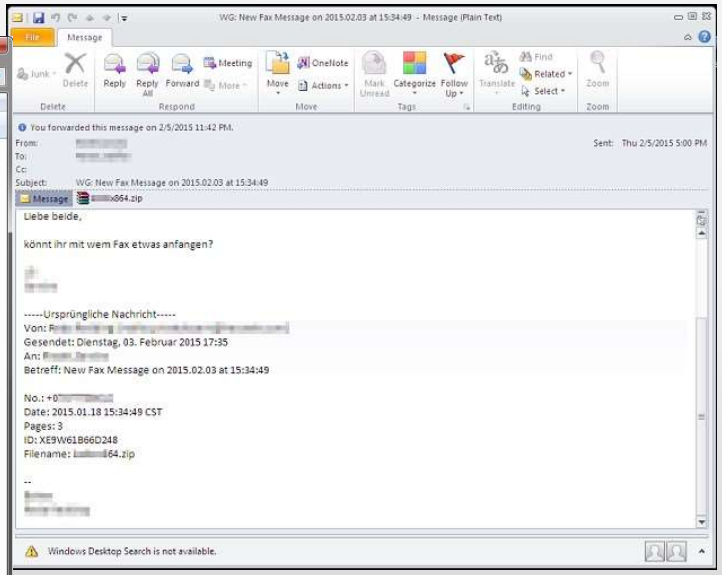
ویرویس یک فایل autorun.inf ایجاد می‌کند که یک فایل فقط خواندنی و پنهان است.

زمانی که کاربر فایل‌های درون USB را باز می‌کند autorun.inf اجرا شده و فایل‌های وردپرس را در سیستم کپی می‌کند.

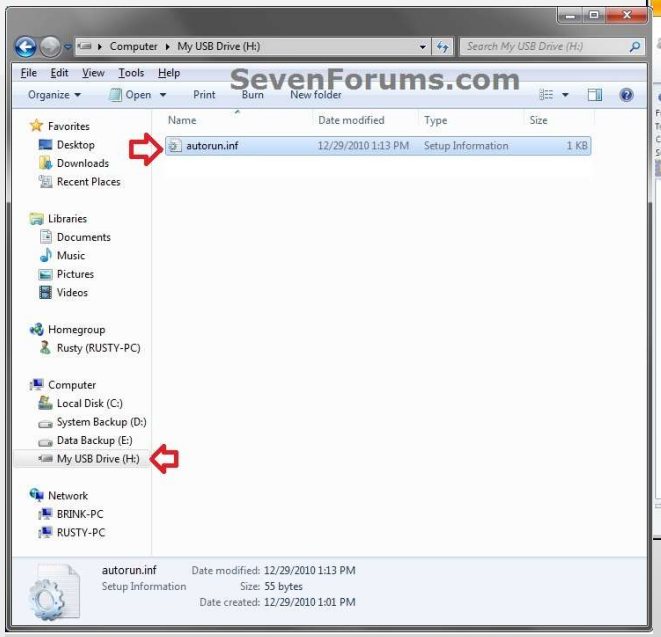
از طریق سایت‌های آلوده

بازدید از سایت‌های آلوده ممکن است منجربه نصب نرم‌افزارهای مخرب (که به منظور سرقت اطلاعات طراحی شده‌اند) بر روی کامپیوتر کاربر شود.

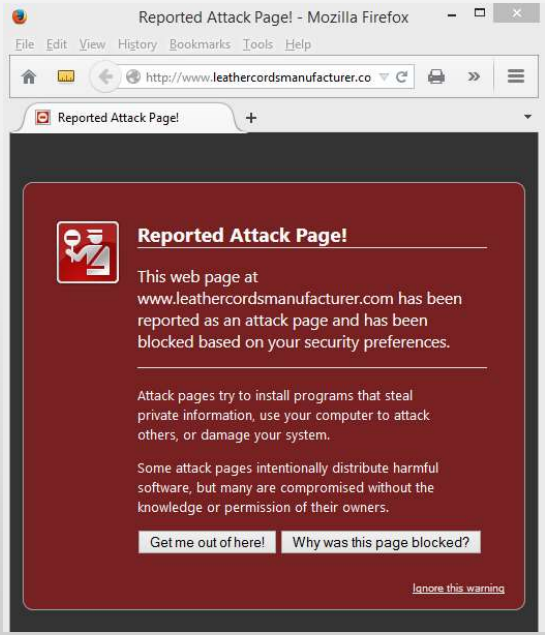
پیوست‌های ایمیل



کارت حافظه‌های USB



سایت‌های آلوده



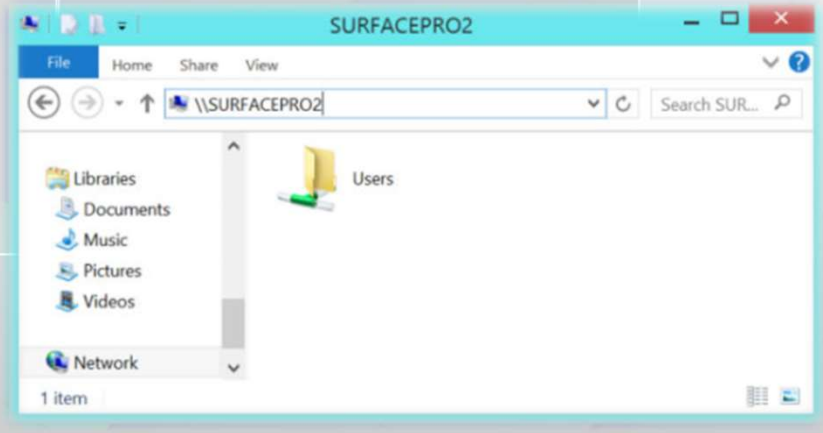
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

از طریق پوشه‌های اشتراک گذاری شده

بدافزار ممکن است از طریق اشتراک‌گذاری‌های شبکه پخش شود.

بدافزار ممکن است با کپی نمودن خود در پوشه‌های به اشتراک گذاشته شده گسترش یابد.



از طریق کدک

اگر کاربری بخواهد یک پلیر برای تماشای ویدئو دانلود و نصب نماید، کدک ممکن است یک برنامه مخرب باشد که بر روی سیستم دانلود می‌شود.

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

Cybersecurity

از طریق دانلودها

دانلود نرم افزار، آهنگ، عکس و ویدئو از سایت‌های نامعتبر ممکن است منجربه دانلود یک فایل مخرب آلوده به ویروس، کرم، تروجان و غیره گردد.

اپلیکیشن‌های مخرب زیادی در اینترنت وجود دارند که با جلات تحریک کننده می‌توانند کاربران را برای دانلود وسوسه کنند.

از طریق آنتی ویروس جعلی

آنتی ویروس ۲۰۰۹ یک آنتی ویروس جعلی است که وانمود به اسکن کردن سیستم نموده و ویروس‌هایی را نشان می‌دهد که وجود ندارند.

با کلیک بر روی دکمه Register یا Scan بدافزار بر روی سیستم دانلود می‌شود.

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

Cybersecurity

اشتراک گذاری فایل peer-to-peer

- ✓ امکان به اشتراک گذاری موسیقی، تصاویر، داکیومنت‌ها و برنامه‌های نرم‌افزاری بین دو کامپیوتر را از طریق بستر اینترنت فراهم می‌آورد.
- ✓ فایل‌های به اشتراک گذاشته شده ممکن است حاوی خطرات امنیتی مانند ویروس، جاسوس افزار و سایر نرم‌افزارهای مخرب باشند.
- ✓ مهاجمان می‌توانند بدافزار را به عنوان یک اپلیکیشن مفید جلوه دهند.

نشانه‌های وجود یک بدافزار در رایانه:

- ✓ پاپ‌آپ‌ها (Pop-up)
- ✓ از کار افتادن ناگهانی سیستم
- ✓ فعالیت مشکوک هارد دیسک
- ✓ کمبود فضا روی هارد دیسک
- ✓ فعالیت غیرطبیعی شبکه
- ✓ تعویض صفحه نخست مرورگر، باز شدن سایت‌ها به صورت ناخواسته
- ✓ پیغام‌های غیرطبیعی یا باز شدن ناخواسته نرم‌افزارها
- ✓ کار نکردن نرم‌افزارهای امنیتی
- ✓ دریافت پیغام‌های غیرعادی توسط دوستانتان

Cybersecurity

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

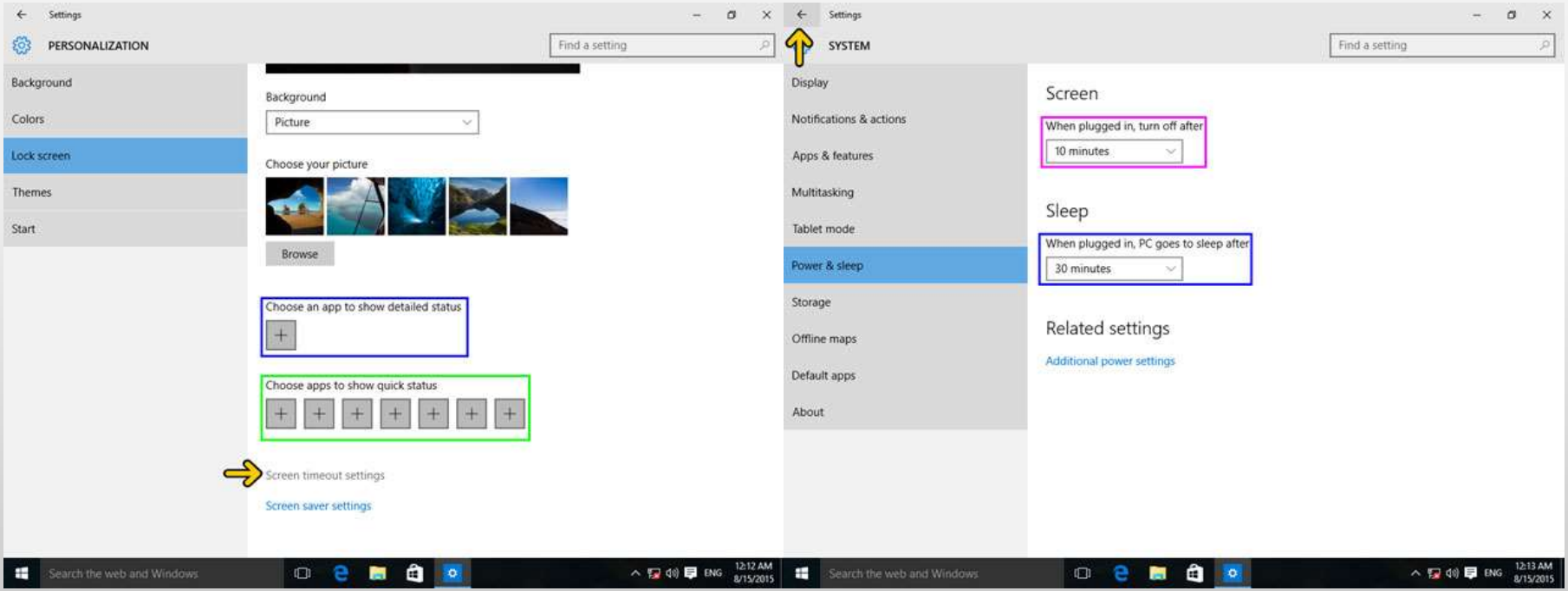
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

قفل نمودن سیستم زمانی که از آن استفاده نمی‌شود

در ویندوز ۱۰ به ۲ طریق می‌توان سیستم را قفل نمود:

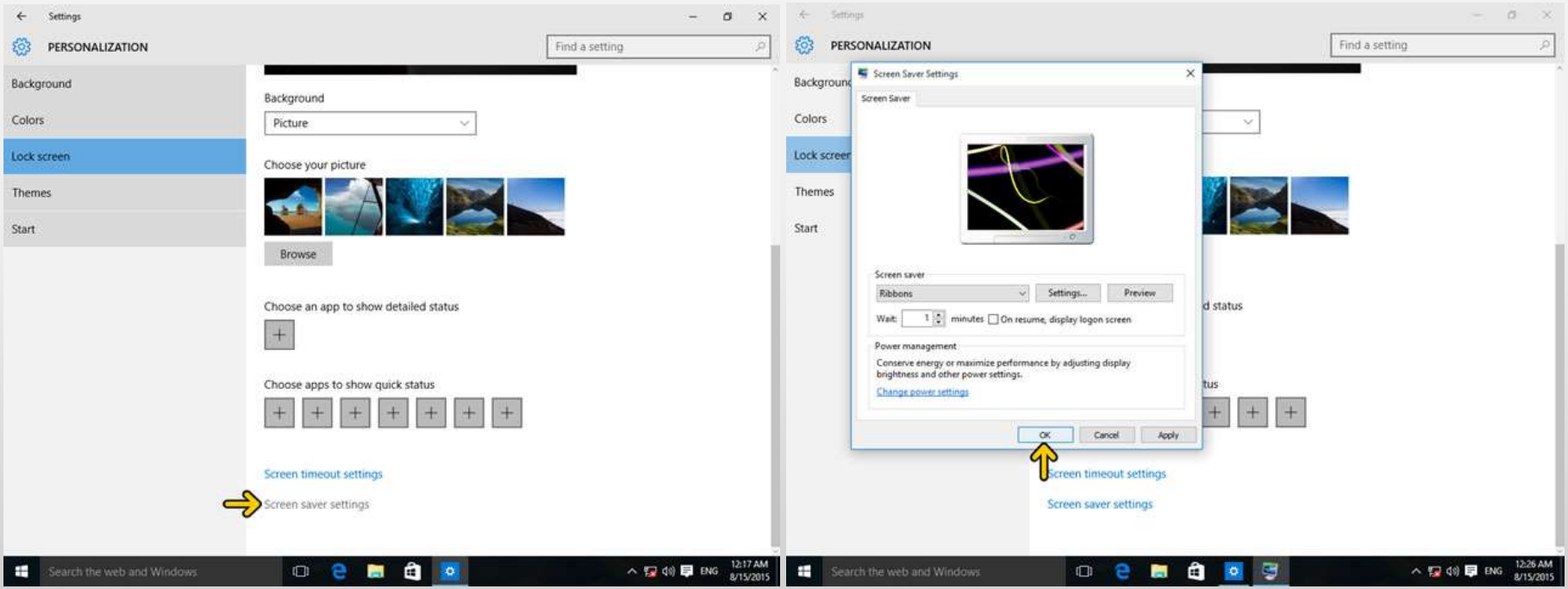
- فشردن همزمان Windows + L
- راست کلیک بر روی صفحه Desktop و انتخاب گزینه Personalize



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

Cybersecurity

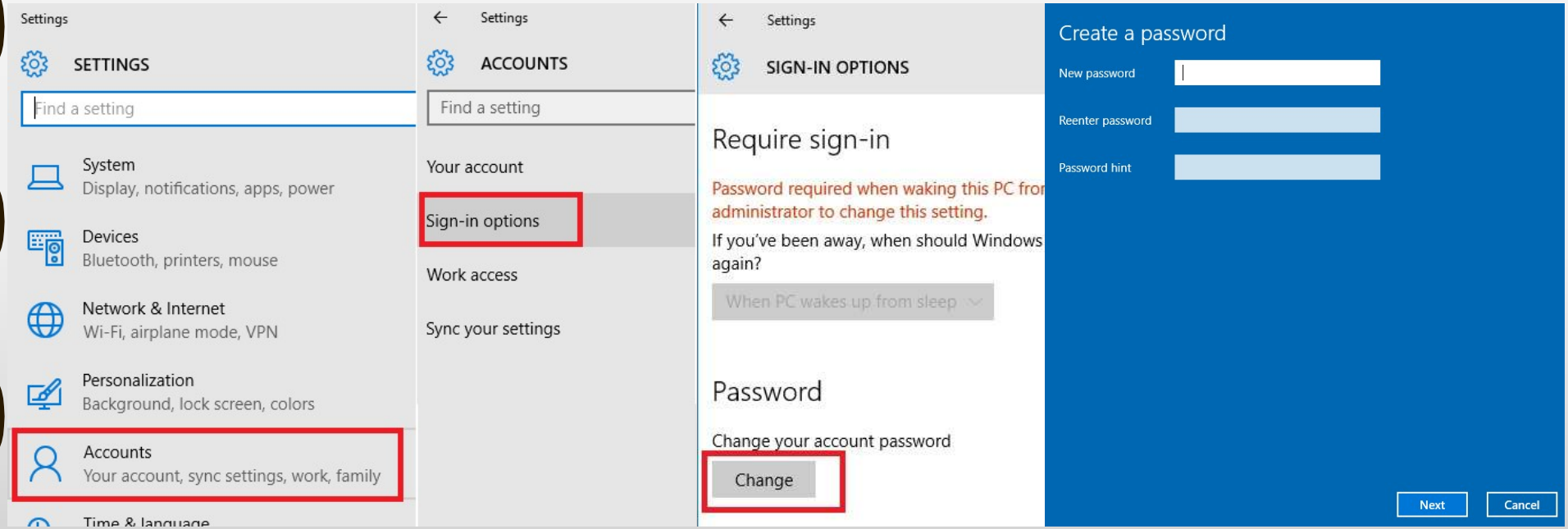
قفل نمودن سیستم زمانی که از آن استفاده نمی‌شود



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

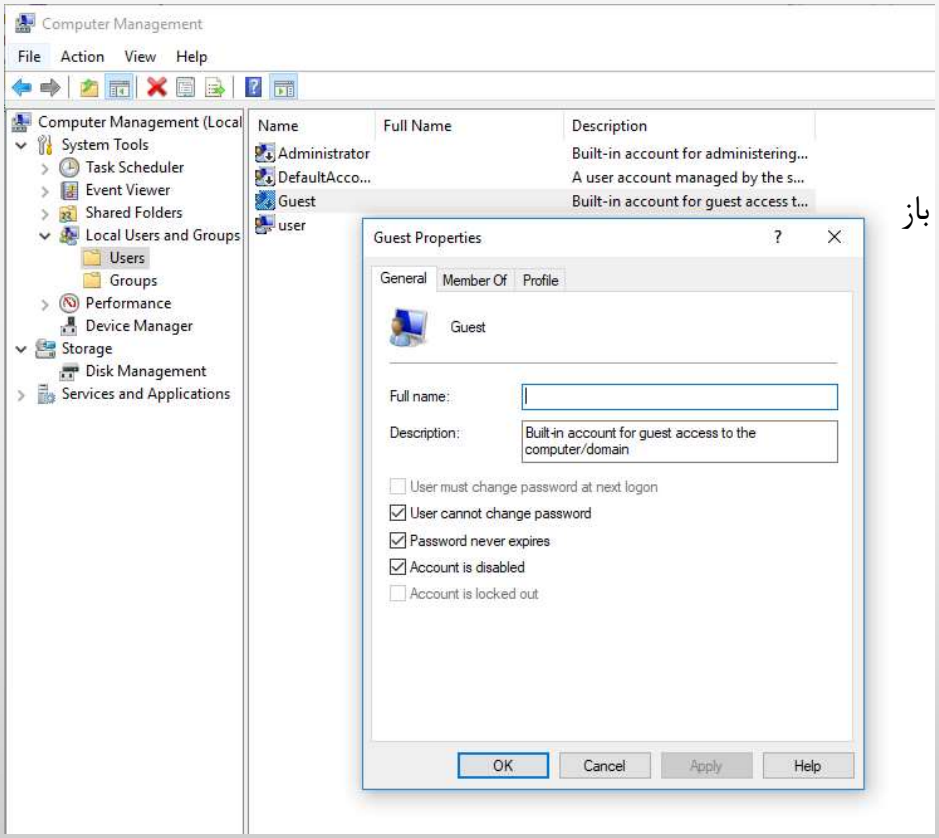
Cybersecurity

تغییر یا ایجاد پسورد قوی در ویندوز ۱۰



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

غیرفعال نمودن حساب کاربری Guest

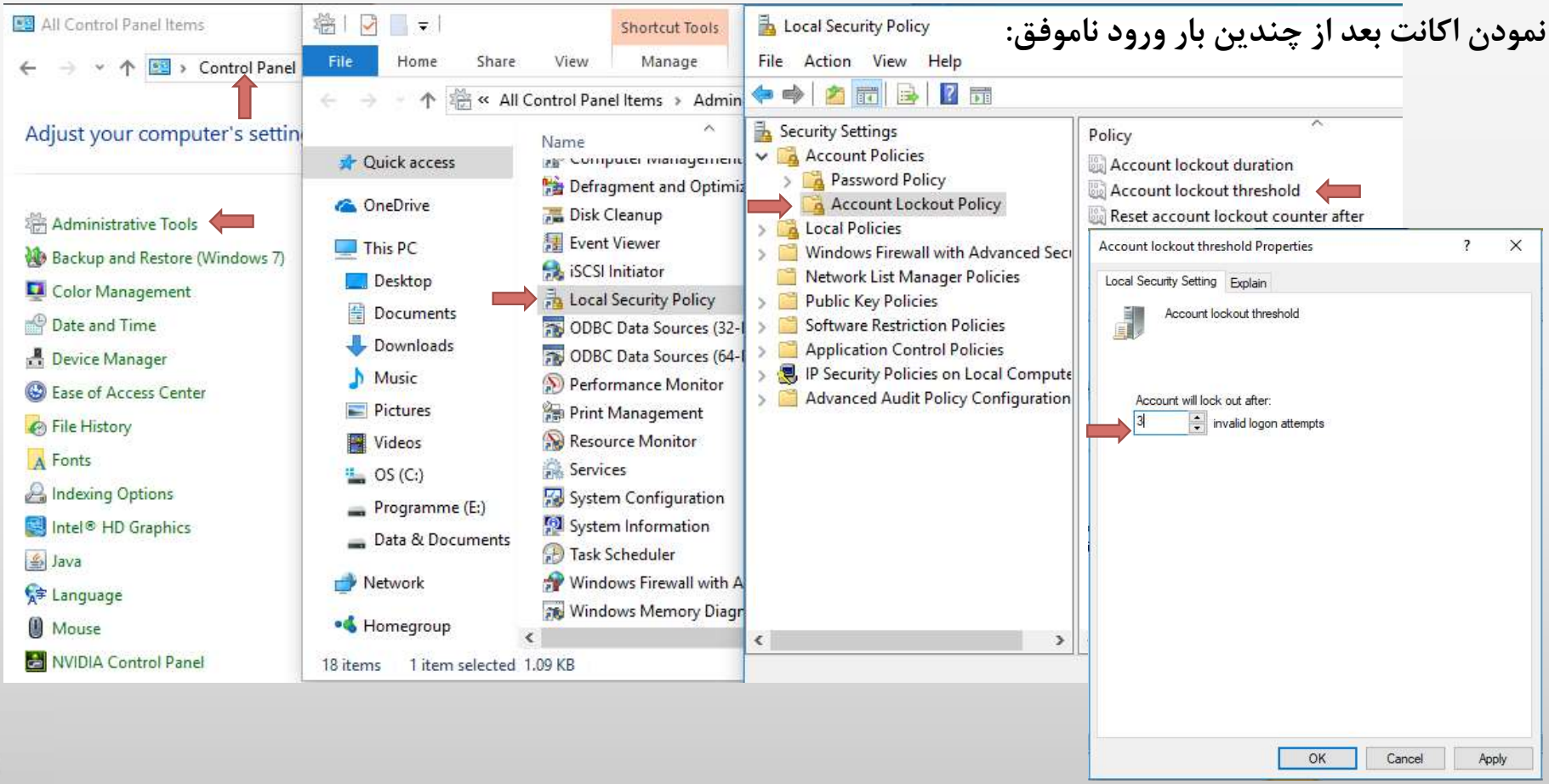


- روی This Pc کلیک راست نموده و Manage را انتخاب کنید.
- سپس به قسمت Local Users And Groups و سپس USER بروید
- روی نام حساب کاربری مورد نظر دابل کیک نموده و پنجره تنظیمات آن را باز کنید.

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

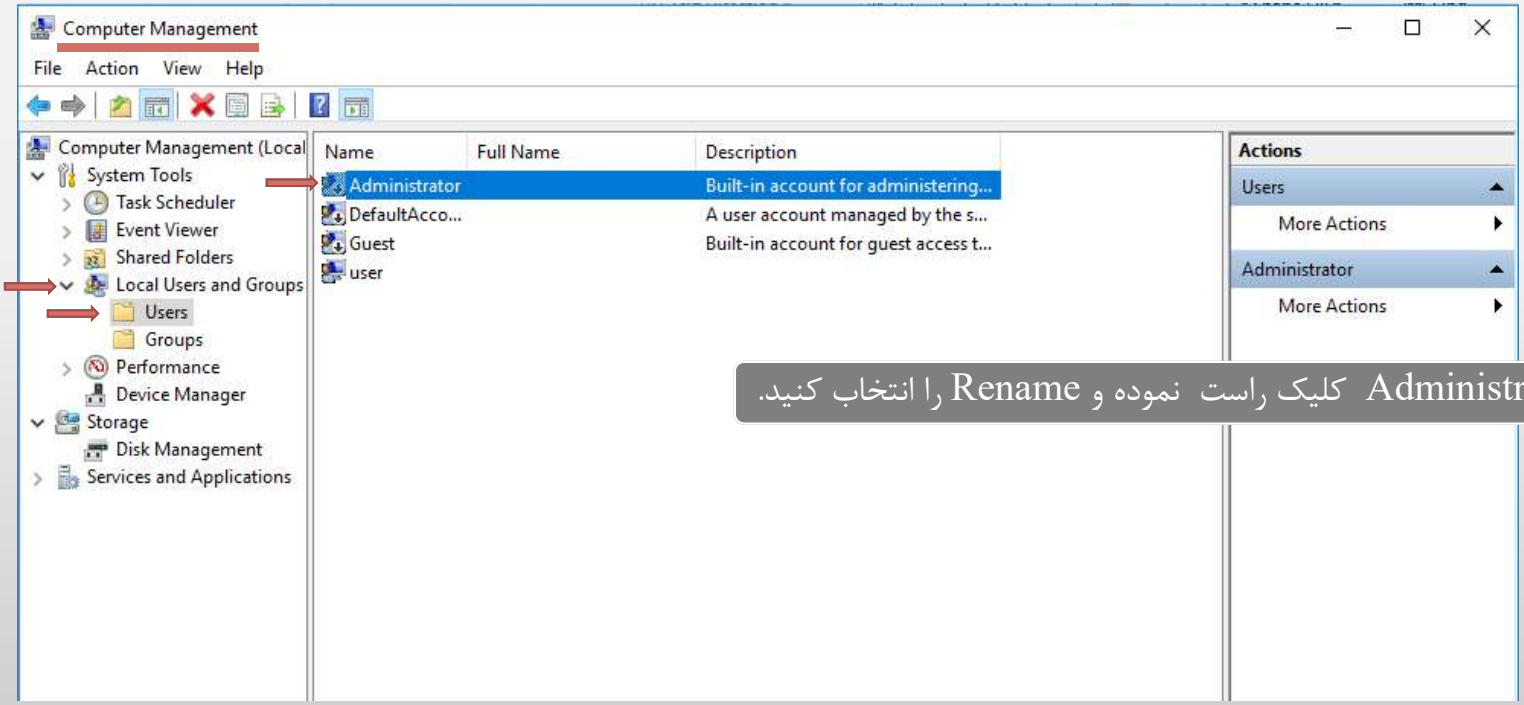
Cybersecurity

قفل نمودن اکانت بعد از چندین بار ورود ناموفق:



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

تغییر نام حساب کاربری Administrator در ویندوز

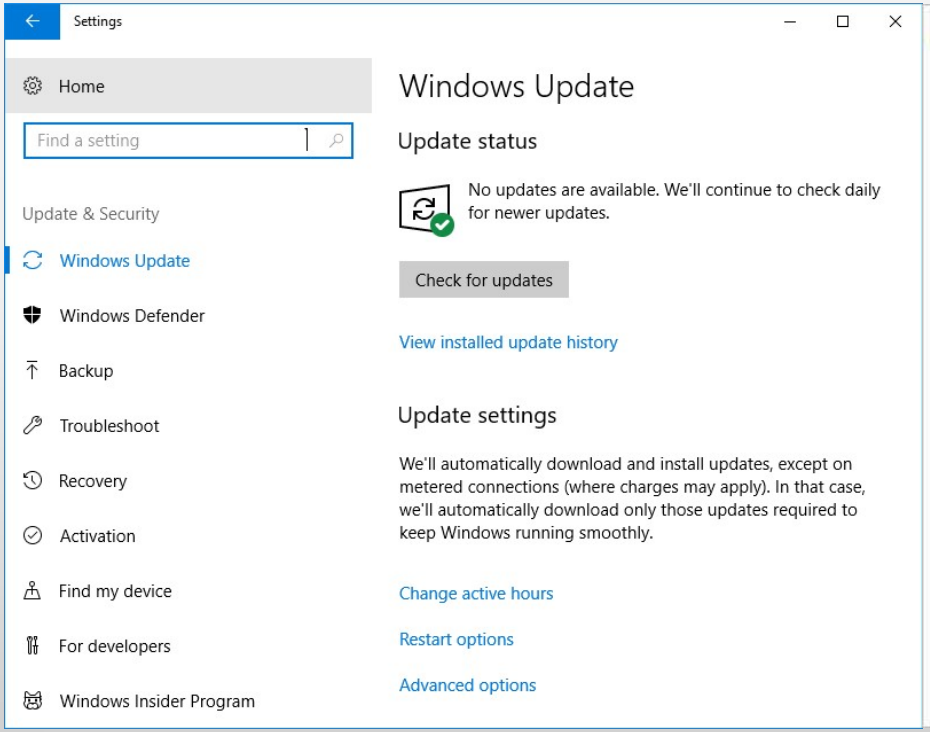


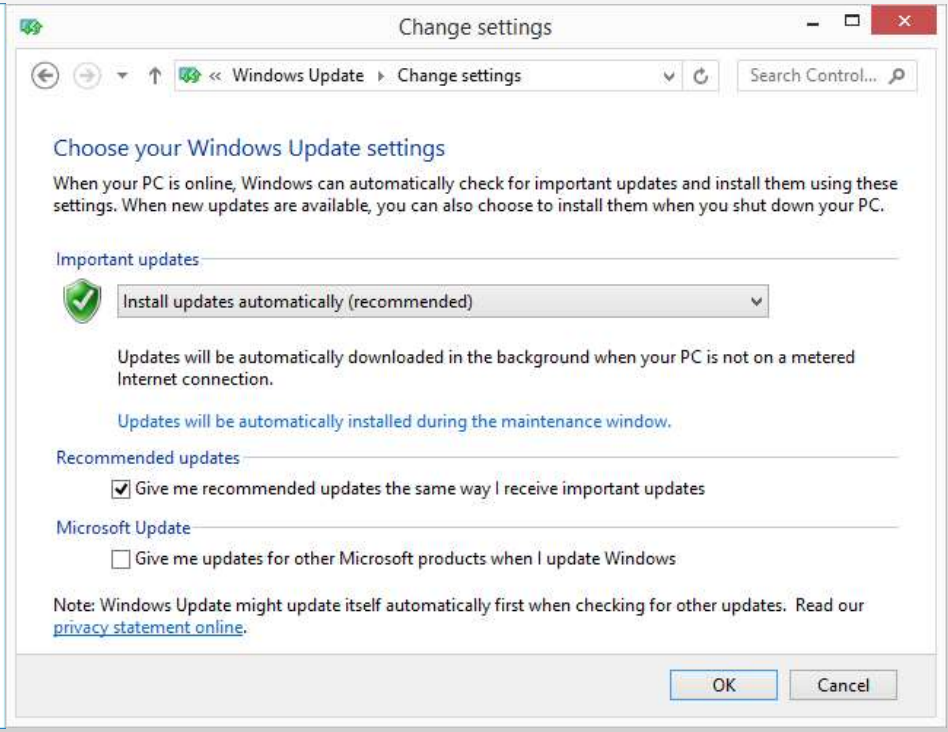
روی نام کاربری Administrator کلیک راست نموده و Rename را انتخاب کنید.

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

Cybersecurity

به روزرسانی در ویندوز ۸، ۱۰





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

Cybersecurity

توصیه‌هایی در رابطه با به روزرسانی

- همیشه سیستم عامل و برنامه‌های را با آخرین وصله‌های امنیتی وصله نمایید.
- وصله‌های امنیتی را فقط از منابع معتبر دانلود کنید، ترجیحا از سایت‌های معتبر عرضه کننده‌ی نرم‌افزار مانند مایکروسافت.
- تنظیمات را به گونه‌ای تنظیم نمایید که هشدار عرضه کنندگان در رابطه با آسیب‌پذیری‌ها برای شما ارسال شود.
- فایل‌های اجرایی را که از منابع مشکوک هستند باز نکنید.
- وصله‌های امنیتی را از طریق ایمیل ارسال نکنید.
- برای نصب آسانتر به روز رسانی‌ها از ابزارهای مدیریت پچ استفاده نمایید.

اعمال وصله‌های امنیتی نرم‌افزارها

بعد از شروع به روز رسانی نیازی به دخالت کاربر وجود ندارد

به روزرسانی خودکار می‌تواند به صورت زمان‌بندی شده باشد.

به روزرسانی‌ها می‌تواند به صورت دستی یا خودکار انجام گیرد.

به روز رسانی‌ها باید از سایت عرضه‌کنندگان نرم‌افزار نصب گردد.

به روز رسانی‌های نرم‌افزار برای به روز نگه داشتن سیستم‌عامل و سایر نرم‌افزارها مورد استفاده قرار می‌گیرد.

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

- طول رمزهای عبور خود را بیشتر از ۸ کاراکتر (حرف) انتخاب کنید. **aminbahrami**
- درون رمز عبور خود، هم از حروف بزرگ و هم از حروف کوچک استفاده کنید. **AminBahrami**
- درون رمز عبور خود، از اعداد نیز استفاده کنید. **aminbahrami1236**
- درون رمز عبور خود، از علائم انگلیسی مانند نقطه، فاصله، اعشار، و علائم دیگر مانند ~,!,@,#,$,%,^,&,*,_,=,+,\,/,|,?,>,<,...« استفاده کنید. **m1n 8ahraml@**
- درون رمز عبور خود، از حروف اضافه انگلیسی «,.,:,;,'," و ...» استفاده کند. **amin.:.bahrami;**
- درون رمز عبور خود، از انواع پرانتز ( ),(,),{,},[,],(,),[,]) استفاده کنید. **amin][bahrami]**

سیستم‌های مختلف ایمیل چگونه کار می‌کنند؟

- ایمیل یک روش تبادل پیام‌های دیجیتالی از یک فرستنده به یک یا چند گیرنده است.
- شرکت‌هایی مانند Microsoft، Yahoo، Google، AOL از حساب‌های ایمیل رایگان خود استفاده می‌کنند.
- حساب‌های ایمیل، از هر مرورگر وب یا کلاینت ایمیل مانند Microsoft Outlook، Mozilla Thunderbird و غیره قابل دسترسی است.

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

اگر امن‌سازی صورت نگرفته باشد، ایمیل‌های فرستاده یا دریافت شده می‌تواند جعل یا توسط دیگران خوانده شود.

ایمیل‌های ناامن، به مهاجمان اجازه می‌دهند تا به **اطلاعات شخصی و حساس کاربر** دسترسی پیدا کنند.

ارتباط از طریق ایمیل به طور **۱۰۰ درصد** امن نیست.

لازم است که ایمیل‌ها برای **ارتباطات امن** و **حفاظت از حریم خصوصی**، ایمن شوند.

ایمیل‌ها یکی از منابع **ویروس‌ها** و برنامه‌های مخرب هستند.

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

Cybersecurity

تهدیدات امنیتی ایمیل

Spamming

- کاربر ممکن است ایمیل‌های اسپمی را دریافت کند که حاوی نرم‌افزارهای مخرب باشد که به مهاجمین اجازه می‌دهد تا کامپیوتر کاربر را کنترل کند.

ایمیل Hoax/Chain

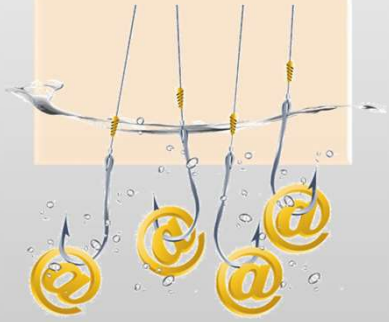
- ممکن است کاربر ایمیل‌های جعلی دریافت کند که شامل اطلاعات اشتباهی است که به او می‌گوید نامه‌ای را ارسال کند.

هدایت کاربر به یک آدرس مخرب

- ایمیل‌ها ممکن است حاوی لینک به سایت‌های مخرب یا دارای مطالب مربوط به pornographic باشند.

فیشینگ

- ایمیل‌های فیشینگ قربانیان را برای ارائه‌ی اطلاعات شخصی فریب می‌دهند.



پیوست‌های مخرب ایمیل

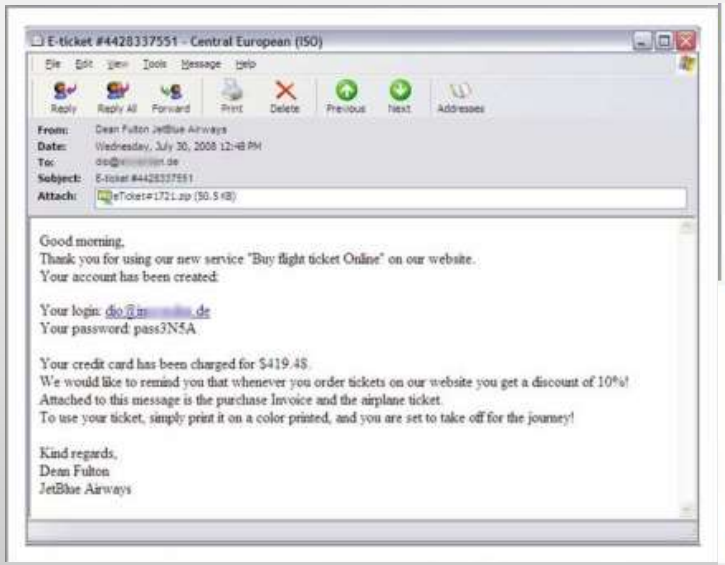
- فایل‌های ضمیمه ممکن است حاوی یک ویروس تروجان، کرم‌های keylogger و... باشد و باز کردن چنین پیوست‌هایی کامپیوتر را آلوده می‌کند.

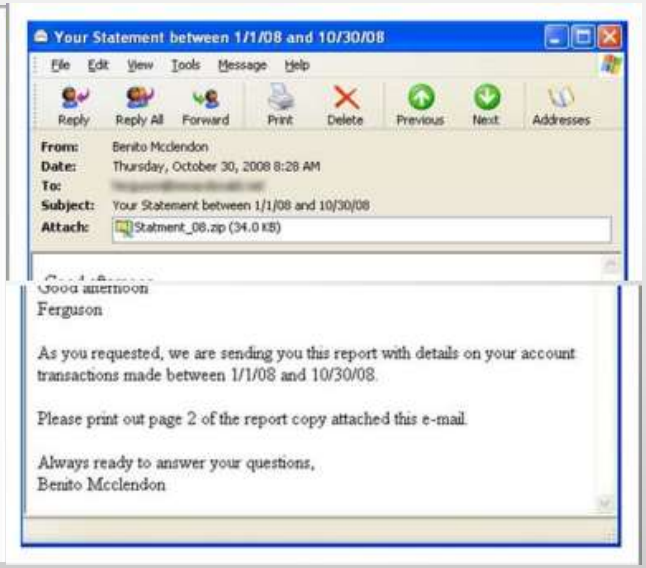
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

پیوست‌های مخرب ایمیل

- پیوست‌های ایمیل تهدیدات امنیتی عمده‌ی ایمیل هستند، زیرا آنها ساده‌ترین و قویترین راه‌ها را برای حمله به یک کامپیوتر، به مهاجمان ارائه می‌دهند.
- بیشتر پیوست‌های مخرب، یک ویروس، تروجان، نرم‌افزار جاسوسی یا هر نوع دیگر از بدافزار را نصب می‌کنند که به زودی شما آنها را باز می‌کنید.





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

Cybersecurity

پیوست های ایمیل: هشدارها

پیوست‌های حاوی فایل‌هایی با **پسوندهای مشکوک و ناشناخته** باز نکنید. به عنوان مثال: *.exe, *.vbs, *.bat, *.ini, *.bin, *.com, *.pif, *.zzx

هرگز **پیوست‌های ایمیل** ارسال شده از منابع غیرقابل اعتماد را باز نکنید.

بررسی کنید که ایمیل از یکی از **مخاطبین** شما فرستاده شده است.

بررسی کنید که آیا **موضوع ایمیل** با **نام پیوست** هماهنگی دارد یا خیر.

قبل از باز کردن، تمام پیوست‌ها را **ذخیره و اسکن** کنید.

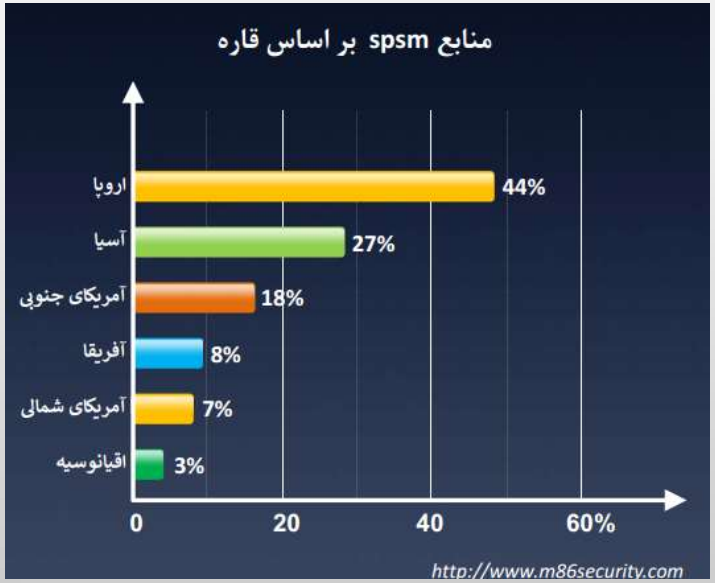
بررسی کنید که آیا ایمیل از یک **منبع قابل اعتماد** دریافت شده است یا خیر

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

Cybersecurity

Spamming

- استفاده از سیستم‌های ایمیل برای ارسال توده پیام‌های ناخواسته، بدون در نظر گرفتن صندوق‌های پستی کاربران است.
- ایمیل‌های اسپم ممکن است حاوی برنامه‌های کامپیوتری مخرب مانند ویروس‌ها و تروجان‌ها باشند.
- طبق گفته‌ی سیمانتک، اسپم ۸۹.۱ درصد از کل ترافیک ایمیل را تشکیل می‌دهد.



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

Cybersecurity

راه‌های مقابله با Spamming

- هرگز لینک‌های موجود در پیام‌های اسپم را دنبال نکنید.
- از ابزارهای آنتی اسپم یا فیلتر اسپم کلاینت ایمیل استفاده کنید.
- از باز شدن پیام‌های اسپم جلوگیری کنید (مرتب شده توسط فیلترهای اسپم).
- هنگام ارسال پیام به هر انجمن عمومی، از یک آدرس ایمیل متفاوت استفاده کنید.
- برای ثبت‌نام در هر وب‌سایت، از آدرس ایمیل رسمی استفاده نکنید.
- ایمیل‌های اسپم مشکوک را گزارش کنید.

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

ابزار آنتی اسپم SPAM fighter

این ابزار از تمام حساب های ایمیل در یک کامپیوتر در برابر "فیشینگ"، سرقت هویت و دیگر فریب های ایمیل محافظت می کند.

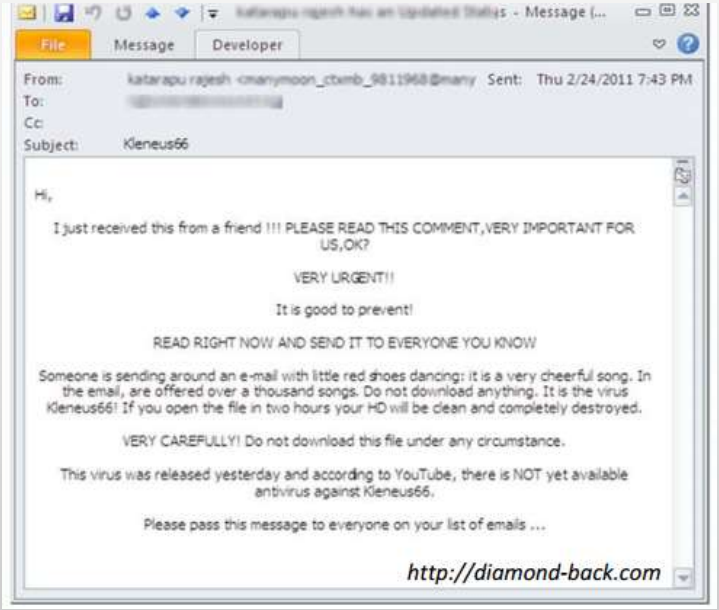
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

ایمیل‌های Hoax/Chain و Scam

Hoaxs، پیام‌های هشدار در مورد تهدیدات غیرواقعی به گیرندگان ایمیل هستند.

به کاربران در مورد اثرات نامطلوب ارسال نکردن آن ایمیل به دیگران هشدار داده می‌شود.



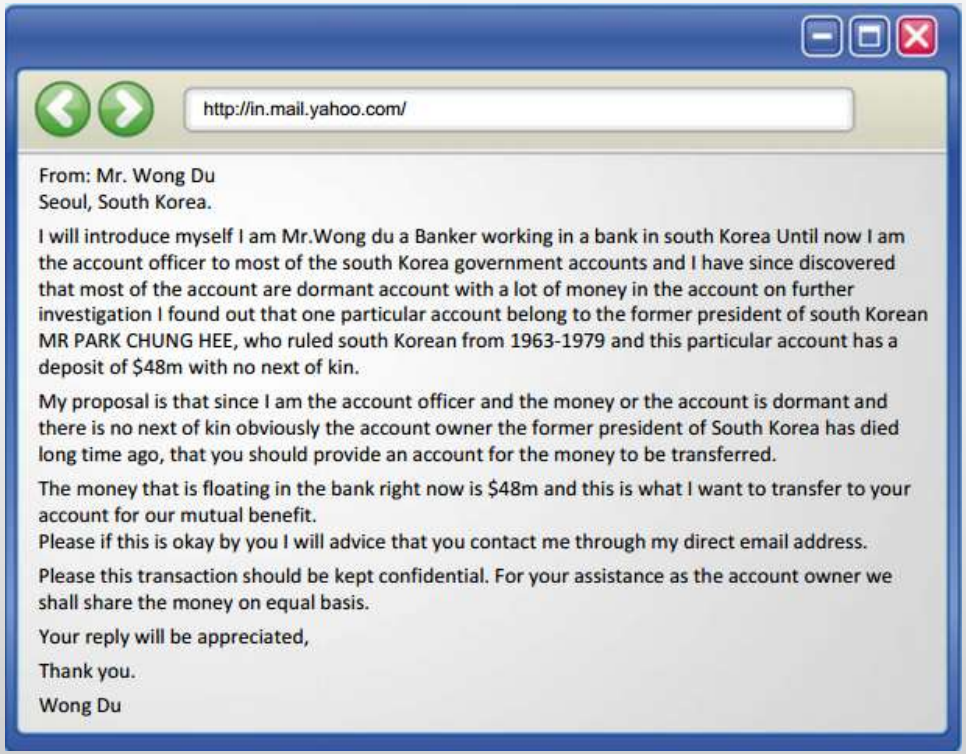
یک ایمیل Scam، اطلاعات شخصی مانند اطلاعات حساب بانکی، شماره کارت اعتباری، رمز عبور و ... را از کاربر درخواست می‌کند.

فرستنده ایمیل Scam، همچنین ممکن است از گیرنده بخواهد که ایمیل را به تمام کسانی که در لیست مخاطبانش وجود دارند ارسال کند.

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

کلاهبرداری نیجریه‌ای:

- کلاهبرداری نیجریه‌ای یا Nigerian Scam نوعی پیش پرداخت یا انتقال پول است.
- دلیل نام‌گذاری این کلاهبرداری به کلاهبرداری نیجریه‌ای این است که ابتدا در نیجریه آغاز شده است اما می‌تواند در هر جای دنیا انجام شود.
- با استفاده از این کلاهبرداری، کلاهبرداران با ارسال یک ایمیل و پیشنهاد یک سهم در یک سرمایه هنگفت با شما تماس می‌گیرند.
- آنها می‌گویند که می‌خواهند پولی را که در طی جنگ‌های داخلی در بانک‌ها بلوکه شده است به حساب شما انتقال دهند.
- همچنین آنها ممکن است دلایل مختلفی از قبیل مشکل ارثی بزرگ، محدودیت‌های دولت یا مالیات در کشور کلاهبردار را ذکر کنند.
- کلاهبرداران از شما می‌خواهند که پول یا اطلاعات حساب بانکی خود را برای کمک به آنها در انتقال این پول ارسال کنید.



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

Cybersecurity

لایه‌های کنترل امنیت ایمیل:

- ❖ فیلترهای اکتشافی
- ❖ شناسایی زبان
- ❖ فیلترهای URL
- ❖ امضاها
- ❖ سرویس اعتبار
- ❖ لیست فرستندگان غیرمجاز
- ❖ لیست فرستندگان مجاز
- ❖ فیلترهای محتوا

روش‌های امنیتی ایمیل

- ایجاد و استفاده از پسورد قوی
- تهیه آدرس ایمیل جایگزین برای بازیابی ایمیل
- آخرین لاگین را بررسی کنید
- از Https برای اتصال به مرورگر استفاده کنید
- گزینه‌های Singed In/ Remember Me, Keep Me را غیرفعال کنید یا انتخاب نکنید
- پیوست‌ای ایمیل را جهت یافتن نرم افزارهای مخرب اسکن کنید
- قابلیت پیش نمایش را خاموش کنید و تنظیمات دانلود را در کلاینت‌های ایمیل تغییر دهید
- فیلتر ایمیل کم اهمیت را در کلاینت‌های ایمیل ایجاد کنید
- پیام‌های ایمیل خود را به صورت دیجیتالی امضا کنید
- با استفاده از فیلترها، از ایمیل‌های ناخواسته جلوگیری کنید

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

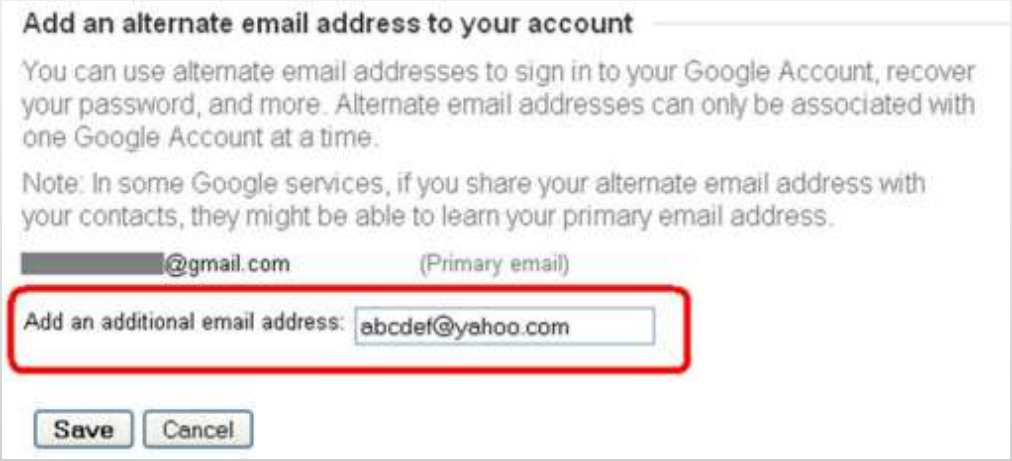
ایجاد پسوردهای قوی

- پسوردهای قوی برای کرک و حدس زدن دشوار هستند (ر.ک اسلاد ۴۰)
- یک پسورد قوی می‌تواند با ترکیبی از اعداد و حروف کوچک و بزرگ کاراکترهای خاص ساخته شود
- یک پسورد قوی و آسان برای به یاد آوردن ایجاد کنید و آن را هر جایی یادداشت نکنید

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

آدرس ایمیل جایگزین

- آدرس ایمیل جایگزین، یک آدرس ایمیل اضافی و ضروری است برای ثبت نام در بسیاری از سرویس‌های ایمیل مانند Gmail و Yahoo
- توسط ارائه دهندگان سرویس برای تایید تشخیص سازنده حساب، استفاده می‌شود.
- آدرس‌های ایمیل جایگزین برای بازیابی پسورد در صورت فراموشی، مورد استفاده قرار می‌گیرند.



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

Keep Me Signed In/Remember Me

- بیشتر کلاینت‌های ایمیل محبوب، گزینه‌های Keep me signed in یا Remember Me را دارند.
- بررسی این گزینه‌ها به کلاینت ایمیل اجازه می‌دهد تا صندوق پستی کاربر رت بدون پر کردن مجدد اطلاعات لاگین، بازیابی کند.
- این گزینه‌ها به کاربران دیگر اجازه می‌دهند تا به ایمیل کاربر دسترسی پیدا کنند.
- کاربران باید این گزینه‌ها را هنگام دسترسی به ایمیل از یک کامپیوتر عمومی، انتخاب نکنند.

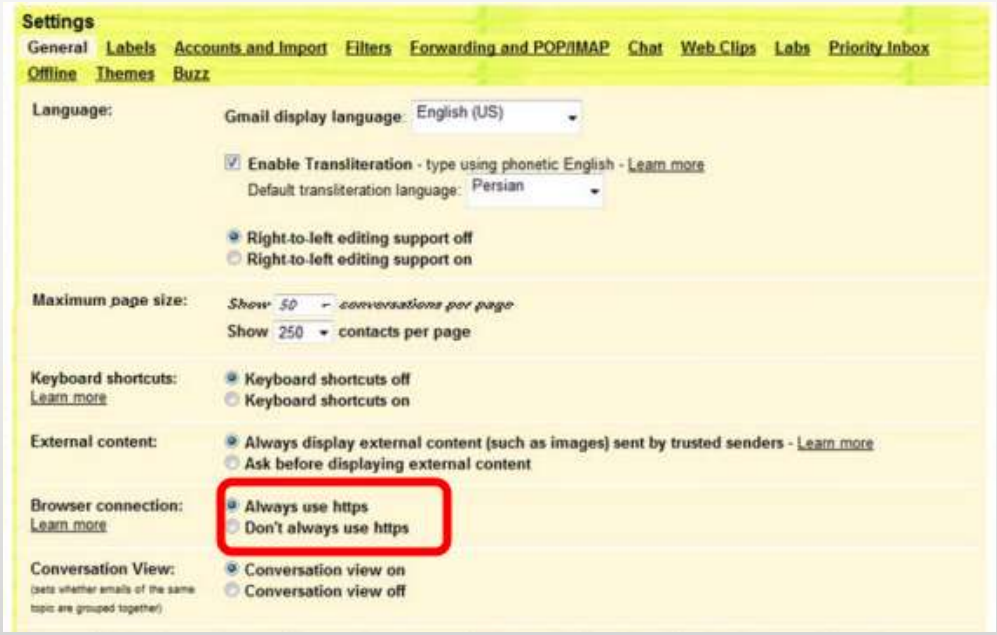
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

استفاده از HTTPS

- حساب‌های کاربری ایمیل تحت وب مانند Gmail، Yahoomail، AOL Mail و غیره یک گزینه برای انتخاب پروتکل ارتباطی برای اتصال مرورگر دارند.

- تنظیمات اتصال مرورگر را برای دریافت ایمیل با استفاده از پروتکل HTTPS (HTTP Secure) تغییر دهید.



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

Cybersecurity

چک کردن آخرین فعالیت حساب کاربری

در صورت در دسترس بودن این ویژگی در سرویس ایمیل، همیشه آخرین فعالیت حساب کاربری را بررسی کنید.

آخرین فعالیت حساب کاربری شامل اطلاعاتی مانند: نوع دسترسی (مرورگر، تلفن همراه و غیره)، موقعیت (آدرس IP) و تاریخ و زمان فعالیت‌های حساب کاربری است.

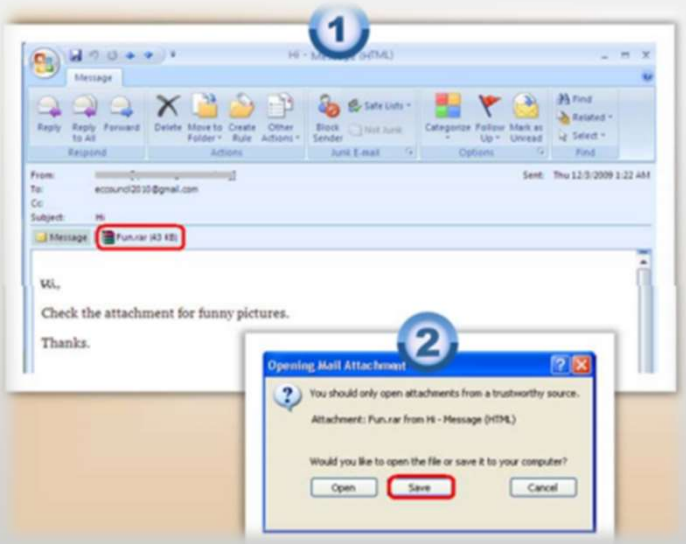
برای بررسی فعالیت حساب کاربری در Gmail به پایین صفحه بروید و روی Details کلیک کنید.

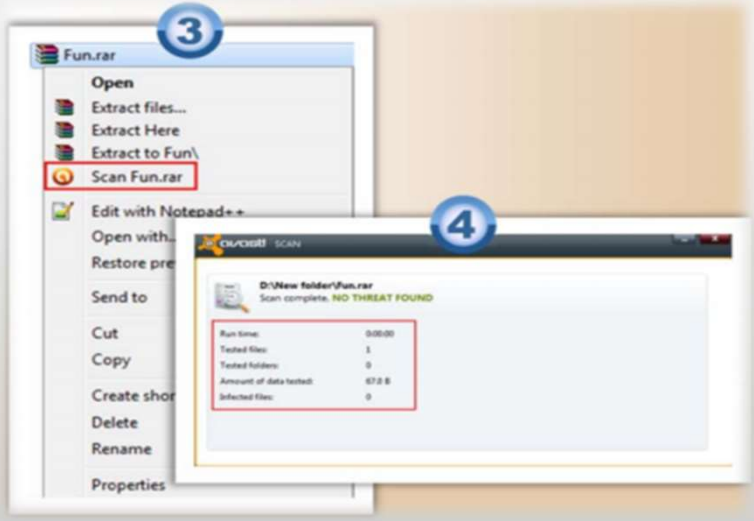
در صورت مشاهده هر فعالیت مشکوک، بلافاصله پسورد و نشانه‌های آن را تغییر دهید.

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

اسکن کردن پیوست های ایمیل

- هنگام باز کردن هر پیوست ایمیل احتیاط کنید.
- همه‌ی فایل‌های پیوست را ذخیره کنید و آنها را قبل از باز کردن، با استفاده از یک آنتی ویروس جهت یا فتن بدافزارها اسکن کند.
- فعال کردن آنتی ویروس به طور خودکار همه‌ی ایمیل‌ها و دانلودها را اسکن می‌کند.



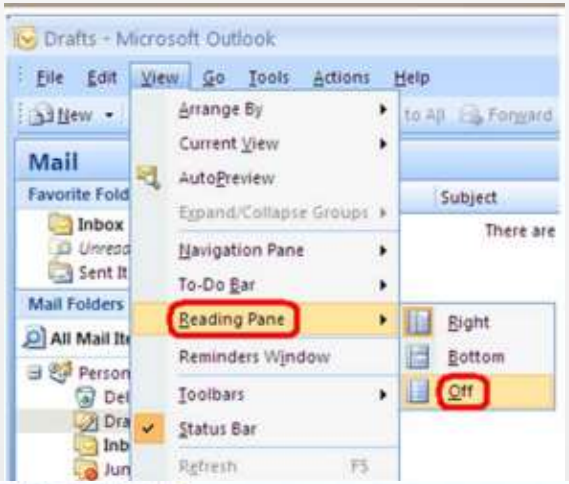


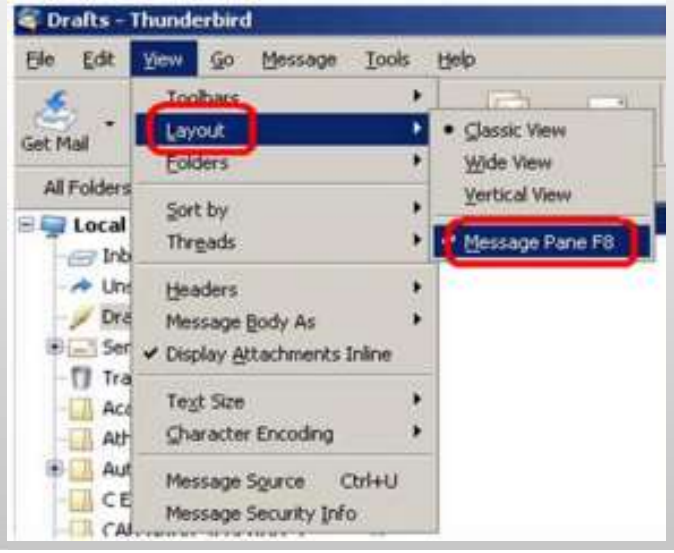
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

خاموش کردن ویژگی پیش نمایش

- کلاینت‌های ایمیل یک گزینه برای ارائه‌ی پیش نمایشی از ایمیل دارند.
- این ویژگی ایمیل را در کلاینت‌های ایمیل خاموش کنید.
- با فعال کردن این ویژگی ممکن است بدون اینکه پیام را باز کنید یک **کد اسکریپت** اجرا شود.
- برای خاموش کردن ویژگی پیش نمایش در **Microsoft Outlook**:
  به منوی View بروید و Reading Pane را انتخاب کنید.
  بر روی گزینه Off کلیک کنید.
- برای خاموش کردن این ویژگی در **Mozilla Thunderbbird**:
  به منوی View بروید و Layout را انتخاب کنید.
  گزینه‌ی Message Pane را غیرفعال کنید.



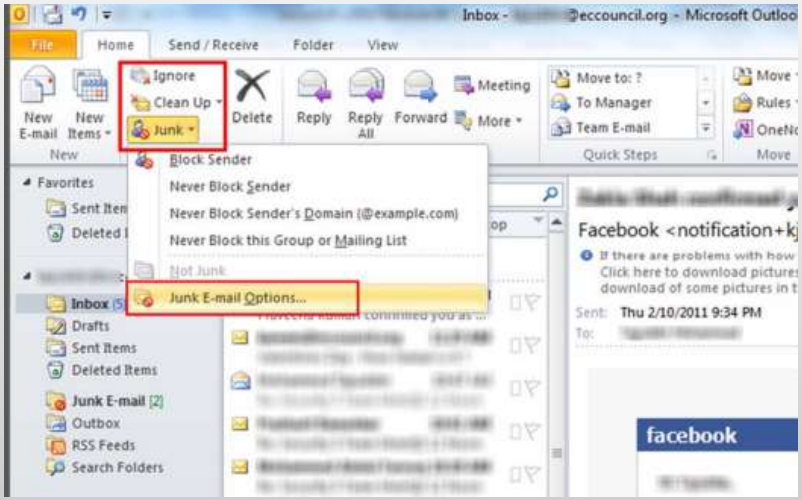


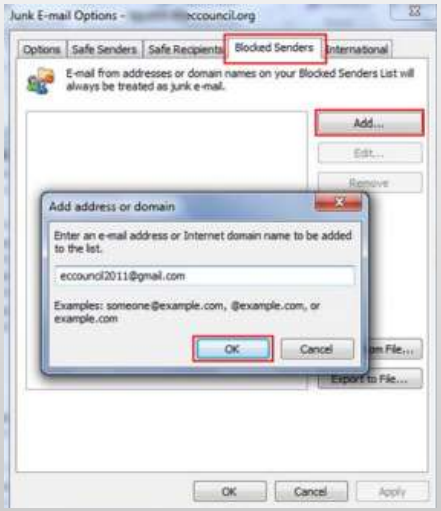
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

فیلتر کردن ایمیل: اجتناب از ایمیل‌های ناخواسته

- فیلتر کردن ایمیل فرایند سازماندهی ایمیل‌ها براساس یک معیار مشخص است.
- فیلترهای ایمیل معمولا برای شناسایی و دسته‌بندی ایمیل‌های اسپم استفاده می‌شوند.
- برای جلوگیری از ایمیل‌های ناخواسته در **Outlook2010**، در منوی **Home** به قسمت **Delete group** بروید، روی گزینه‌ی **Junk** و سپس **Junk E-mail Options** کلیک کنید، در منوی **Blocked Sender**، روی گزینه‌ی **Add** کلیک کنید.
- یک آدرس ایمیل ی نام دامنه وارد کنید و روی گزینه‌ی **OK** کلیک کنید.





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

Cybersecurity

امضای دیجیتالی ایمیل‌ها

- امضاهای دیجیتال برای تایید هویت فرستنده یک پیام یا امضا کننده یک داکیومنت، استفاده می‌شوند.
- همچنین می‌توانند برای اطمینان از اینکه محتوای اصلی پیام تغییر نکرده است، مورد استفاده قرار گیرند.
- کاربران به یک گواهینامه ایمیل برای امضای دیجیتالی ایمیل‌ها نیاز دارند.
- می‌توانید امضاهای دیجیتال را از متصدیان صدور گواهینامه دریافت کنید.
- **چند نمونه از متصدیان صدور گواهینامه در ایران**

Icert (https://www.icert.ir)	Iranssl (http://www.iranssl.com)
pardazit(https://www.ssl.pardazit.net)	Sarvssl (https://www.sarvssl.com)

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

نحوه دریافت گواهینامه دیجیتال

- به وب سایت متصدیان صدور گواهینامه مراجعه کنید.
- یک گوهینامه دیجیتال را خریداری و دانلود کنید.
- برخی از متصدیا صدور گواهینامه، گواهینامه رایگان ارائه می‌دهند.
- Comodo یک نمونه از گواهینامه‌های امنیتی ایمیل است اطلاعات شخصی را برای دانلود گواهینامه، ارئه دهید.
- به حساب کاربری ایمیل خود که هنگام دانلود گواهینامه ارائه دادید، لاگین کنید.
- صندوق پستی خود را جهت مشاهده لینک نصب گواهینامه، بررسی کنید.

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

نصب یک گواهینامه دیجیتال

- برای نصب گواهینامه دیجیتال روی لینک نصب کلیک کنید.
- در مرورگر اینترنت اکسپلورر، به مسیر زیر بروید:

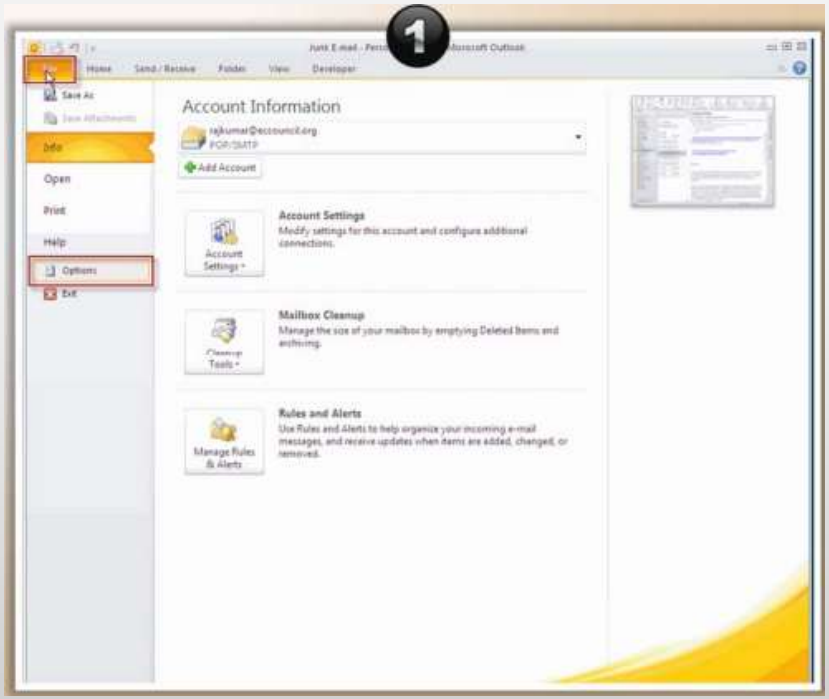
Tools -> Internet Options -> Content tab

- در Content tab روی دکمه Certificates کلیک کنید.
- گواهینامه را انتخاب کنید و روی دکمه Export کلیک کنید.
- روی دکمه Next کلیک کنید.
- Yes را انتخاب کنید private key را اکسپورت کنید.
- روی Next کلیک کنید.
- از private key با دادن یک پسورد و confirm آن، محافظت کنید.
- فایل مورد نظر خود برای اکسپورت را انتخاب کرده و آن را در یک مکان خاص ذخیره کنید.

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

Cybersecurity

امضا کردن ایمیل‌ها



- به مسیر زیر بروید:

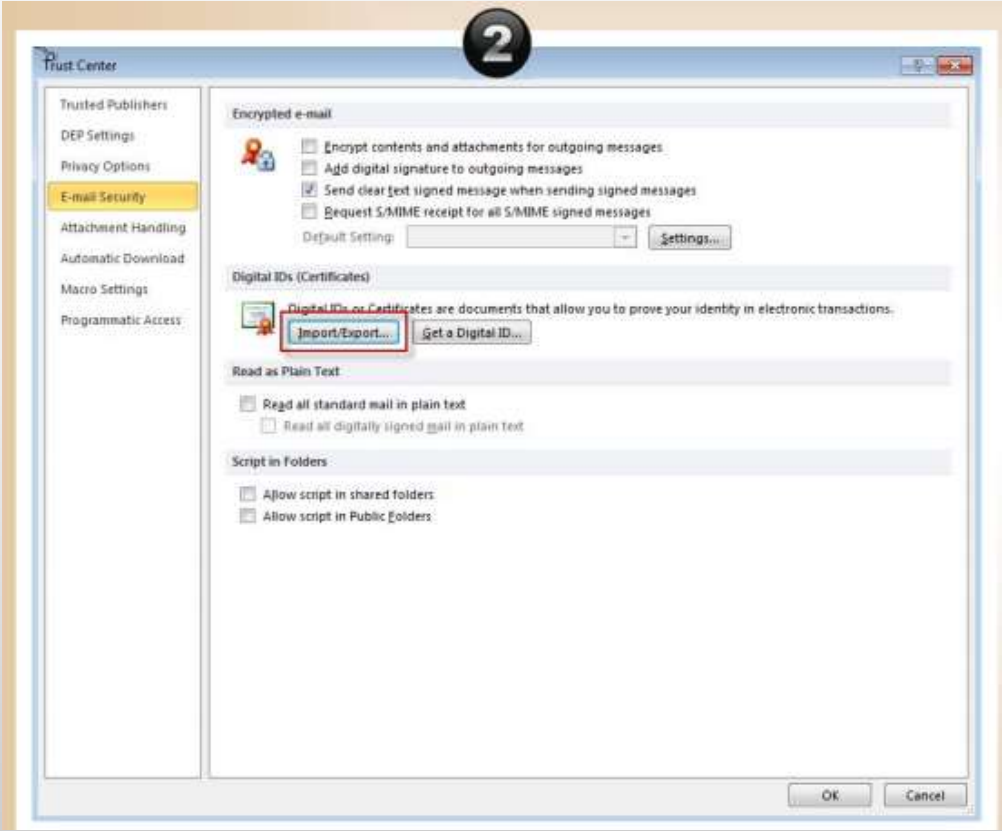
Microsoft Outlook -> File -> Option

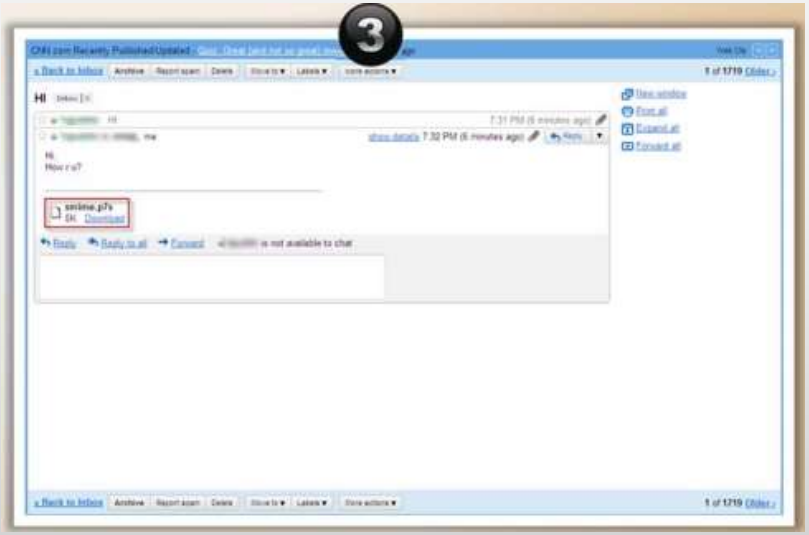
- به ترتیب روی دکمه‌های زیر کلیک کنید:

Trust Center -> Trust Center Setting -> Email Security

- با انتخاب check boxes مناسب در زیر بخش Encrypted e-mail ایمیل را رمزگذاری کنید.
- روی دکمه Import یا Export کلیک کنید
- با انتخاب دکمه Browse، فایل را باز کنید و پسورد و شناسه نام دیجیتال را وارد کنید.
- روی دکمه OK کلیک کنید.
- برای نوشتن یک پیام، روی دکمه New Mail کلیک کنید
- پس از کلیک روی دکمه send رمزگذاری پیام آغاز خواهد شد
- روی دکمه Send Unencrypted کلیک کنید (اگر گیرندگان private key ندارند)
- اگر گیرنده Private key دارد روی دکمه Continue کلیک کنید.

امضا کردن ایمیل‌ها

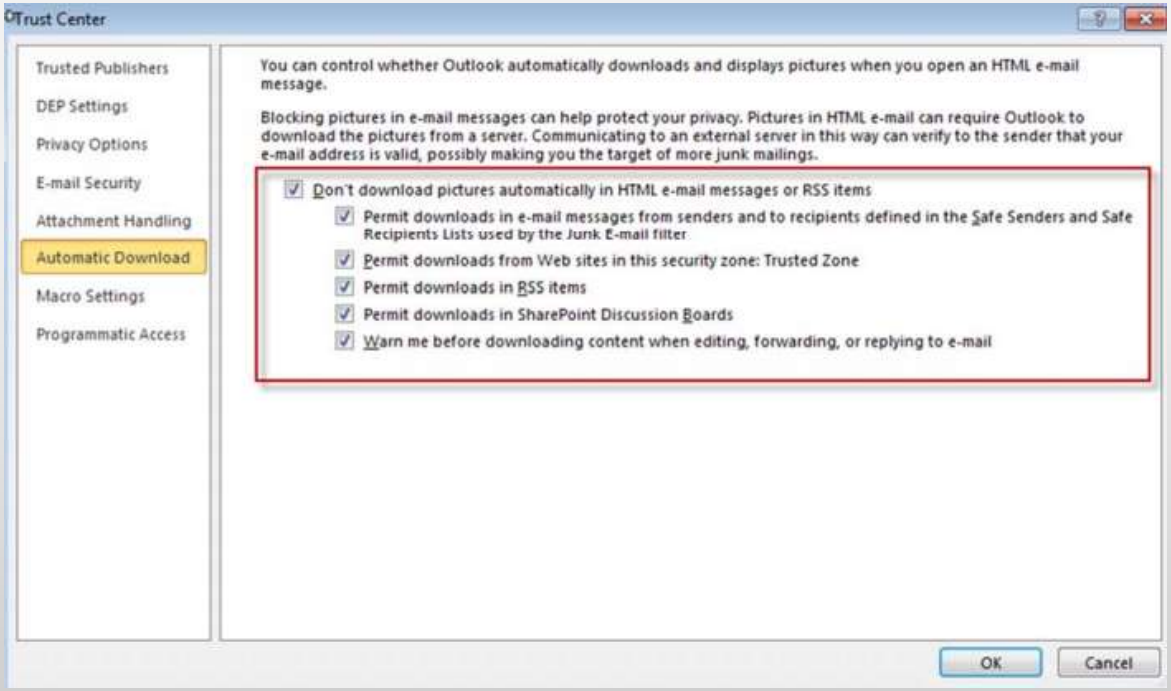




مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

- در بخش Trust Center، روی بخش Automatic Download کلیک کنید و با توجه به شکل گزینه‌ها را انتخاب کنید.



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

Cybersecurity

سیستم آنلاین رمزگذاری ایمیل: Lockbin

- Lockbin یک سرویس رایگان برای ارسال ایمیل‌های محرمانه است.
- این سیستم برای ارسال اطلاعات محرمانه مانند جزئیات کارت اعتباری و اطلاعات کسب و کار، استفاده می‌شود.

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

Cybersecurity

ابزارهای امنیتی

خلاصه

- Email (electronic mail) یک روش تبادل پیام‌های دیجیتال از یک فرستنده به یک یا چند گیرنده است.
- فایل‌های ضمیمه (پیوست‌ها) می‌توانند حاوی برنامه‌های مخرب باشند، که باز کردن چنین پیوست‌هایی می‌تواند کامپیوتر را آلوده کند.

- Spamming فرایند اشغالکردن صندوق ورودی کاربر با ایمیل‌های ناخواسته و بی ارزش است.
- Hoaxes هشدارهای دروغین با ادعای گزارش‌های مربوط به یک ویروس غیرواقعی هستند.
- پاک کردن Cache، پسوردها و history مرورگر را فراموش نکنید.
- تنظیمات تلفن همراه را فقط برای دانلود header ایمیل‌ها در نظر بگیرید نه برای تمام ایمیل
- امضاهای دیجیتال برای تایید هویت فرستنده یک پیام یا امضا کننده یک داکیومنت، استفاده می‌شوند.
- ابزارهای امنیتی ایمیل از پسوردها و خروج خودکار از حساب‌های کاربردی ایمیل، محافظت می‌کنند.

چک لیست امنیت ایمیل

- هنگام ارسال ایمیل به تعدادی از گیرندگان، از گزینه Bcc استفاده کنید.
- هرگز پسورد خود را در مرورگر وب ذخیره نکنید.
- پیام‌ها را براساس الویت، موضوع، تارخ، فرستنده و دیگر موارد مرتب کنید. این کار به شما در جستجوی ایمیل‌ها کمک می‌کند.
- از ارسال اطلاعات محرمانه، حساس، شخصی و طبقه‌بندی شده در ایمیل‌ها اجتناب کنید.
- صندوق وردوی خود را مرتبا پاک کنید.
- پوشه‌هایی را ایجاد کنید و ایمیل‌ها را براساس خانواده، دوستان، کار و غیره به آنها انتقال دهید.
- ایمیل‌هایی را که ارسال می‌کنید، به صورت دیجیتالی امضا کنید.

چک لیست امنیتی برای بررسی ایمیل‌ها در موبایل

- تنظیمات موبایل برای دانلود Header ایمیل‌ها در نظر بگیرید نه برای تمام ایمیل
- فایل‌های پیوست بزرگ را از طریق موبایل، ارسال و باز نکنید.
- لینک‌هایی که توسط ایمیل یا پیام‌های متنی فرستاده شده‌اند، دنبال نکنید.
- یک آنتی ویروس موبایل نصب کنید و آن را آپدیت نگه دارید.
- گزینه نمایش تصاویر را در مرورگر موبایل خود غیرفعال کنید.
- برای کاهش اندازه ایمیل، آنها را یک متن ساده ارسال کنید.
- فایل‌های مهم را به صورت Zip ارسال کنید.

با تشکر از توجه شما

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