دوره آشنایی با امنیت و فناوری اطلاعات

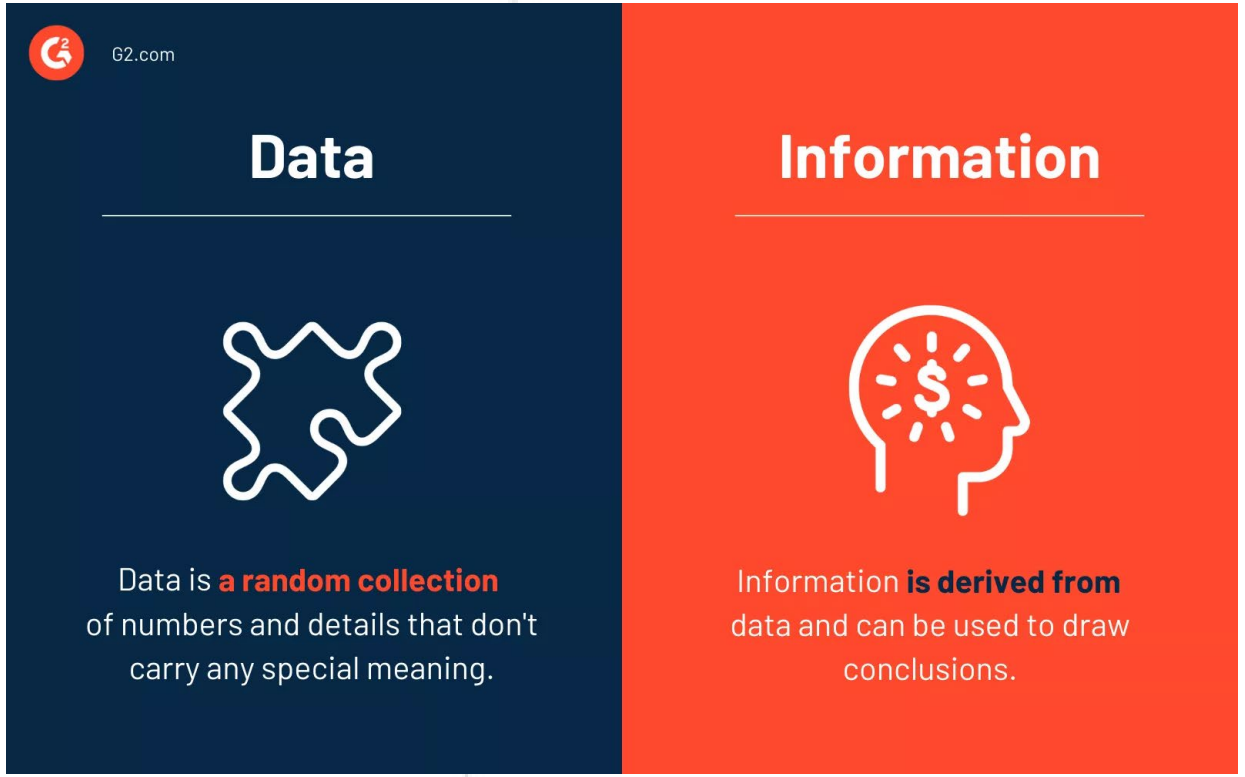
11/04/2025

Version: 00

ROUGINE
DAROU

تعریف داده و اطلاعات

- داده : همانطور که اشاره شد داده ها به عنوان مجموعه ای از حقایق یا آمار و ارقام خام تعریف می شوند. داده ها می توانند به شکل متن، مشاهدات، شکل ها، تصاویر، اعداد، نمودارها یا نمادها باشند. برای مثال، داده‌ها ممکن است شامل قیمت، وزن، آدرس، سن، نام، دما، تاریخ یا مسافت باشد.
- اطلاعات: به عنوان دانشی تعریف می شود که از طریق مطالعه، ارتباط، تحقیق یا آموزش به دست می آید. اساساً اطلاعات نتیجه تجزیه و تحلیل و تفسیر داده هاست. در حالی که داده ها ارقام، اعداد یا نمودارهای خام و فردی هستند، اطلاعات ادراک و نتایج حاصل شده از داده ها است.



ROUGINE DAROU

انواع اطلاعات

- اطلاعات می‌تواند:
- ایجاد شود،
- ذخیره شود،
- نابود شود،
- استفاده شود،
- انتقال یابد.

قالب‌های اطلاعات:

- کاغذ
- پایگاه داده‌ها
- دیسک‌ها یا دیسکت‌ها
- CD-ROM
- نوارها(Tapes)
- نقشه‌ها یا طراحی‌ها
- فیلم‌ها
- مکالمات

ماهیت اطلاعات

- مالی
- استراتژیک
- عملیاتی
- شخصی

ROUGINE DAROU

امنیت اطلاعات چیست؟

- امنیت اطلاعات، حفاظت از داده‌ها در برابر طیف وسیعی از تهدیدها است تا:
- تداوم فعالیت‌های تجاری تضمین شود،
- خسارات سازمان به حداقل برسد،
- و بازده سرمایه‌گذاری و فرصت‌های تجاری به حداکثر برسد.

ROUGINE
DAROU

مثلث امنیت اطلاعات

- صحت و یکپارچگی اطلاعات (integrity)
- قابلیت دسترسی صحیح (Availability)
- رعایت اصول محرمانگی (Confidentiality)

ROUGINE
DAROU

10 قانون امنیت

1. محافظت از لپتاپ، کامپیوتر ، گوشی هوشمند و سایر لوازم الکترونیکی دارای اطلاعات
2. محافظت از پسورد و سایر دسترسیها
3. استفاده محتاطانه و درست از ایمیل
4. طبقه بندی کردن اطلاعات
5. به اشتراک گذاری اطلاعات
6. آنتی ویروس و بروز رسانیها
7. تهیه پشتیبان از فایلهای مهم
8. استفاده از نرم افزارهای تایید شده و معتبر
9. نحوه درست از بین بردن وسایل ذخیره داده ها
10. گزارش موارد امنیتی

ROUGINE
DAROU

محافظت از لپتاپ، کامپیوتر ، گوشی هوشمند و سایر لوازم الکترونیکی دارای اطلاعات

- از کیف و یا کوله های که مشخص است برای لپتاپ طراحی شده استفاده نکنید.
- در هر حالتی تماس فیزیکی با کیف و کوله را حفظ کنید
- اگر لپتاب را جایی به امانت میگذارید،بهتر است باتری را بردارید
- حتما رمز BIOS و هارد دیسک را فعال کنید
- در هنگام جابجایی و حرکت (در اتوبوس، قطار) از لپ تاپ استفاده نکنید
- در هنگام بازرسی دستگاه شبکه ایکس، در آخرین لحظه بار را روی ریل بگذارید.
- کیف را در ابتدای حرکت در صندوق عقب قرار دهید، هیچ وقت کیف لپتاب را بر روی صندلی قرار ندهید.
- در صورت استفاده از تلفن همراه در خودرو شیشه های ماشین را بسته و درب ها را قفل نمایید
- از قراردادن گوشی و لپتاب در مکان های عمومی مانند میزهای رستوران ها خودداری کنید
- در هنگام حوادث رانندگی قبل از ترک خودرو حتما ماشین را خاموش کرده و درب را قفل نمایید

ROUGINE
DAROU

محافظت از پسورد و سایر دسترسیها

1. بایدها و نبایدها
    1. پسورد خود را به هیچ کس ندهید !!!!
    2. پسورد خود را جایی یادداشت نکنید
    3. پسوردهای مهم و معمول خود را از تفکیک کنید.
    4. برای پسوردهای مهم خود به نرم افزارهای ذخیره پسورد اطمینان نکنید (Firefox,Chrome..)

ROUGINE
DAROU

گذرواژه: حداقل استاندارد

سایستهای حداقل پیچیدگی پسورد معمولا توسط ادمین شبکه تعیین میشود اما غالبا مانند موارد زیر است:

1. حداقل 8 کاراکتر
2. استفاده ترکیبی از حروف کوچک (abc…xyz)، حروف بزرگ (ABCD…XYZ)اعداد (123400)، حروف خاص (!@#$*&)
3. مانند 3 پسورد قبلی نباشد.
4. معمول و در دیکشنری نباشد
5. قابل حدس زدن نباشد (مااند نام کاربری، شهر ، نام سازمان ...)

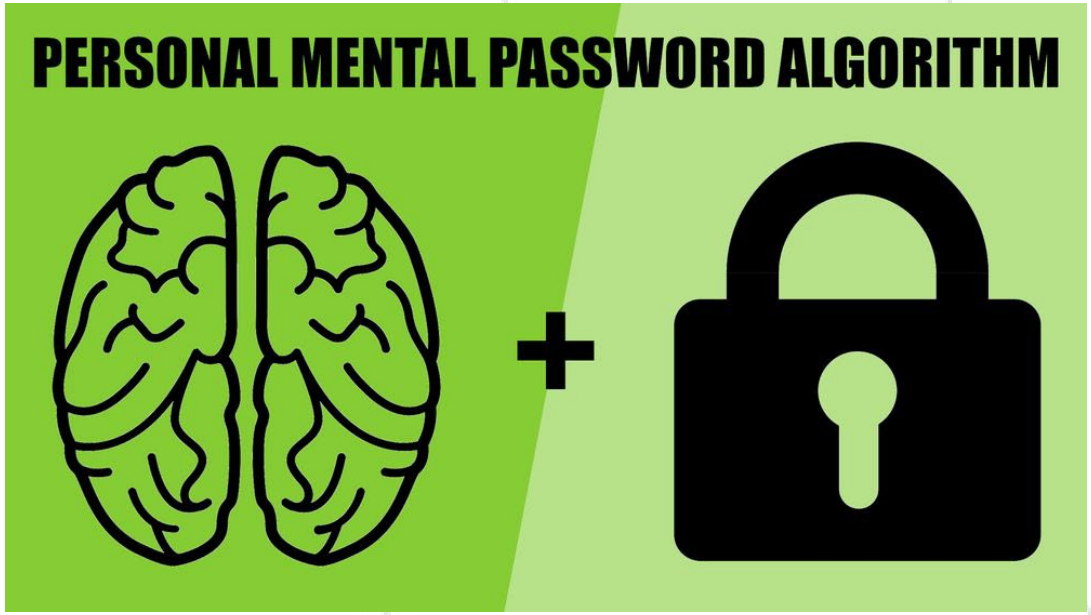
ROUGINE
DAROU

گذر واژه: روشهای انتخاب

1. انتخاب کلمه عبور بر طبق یک جمله.
    1. یکی از راههای خوب برای انتخاب یک پسورد خوب، استفاده از حروف یک جمله میباشد مانند:

I am working in Pharma Since 1395!

IawiPs95!



ROUGINE DAROU

گذرواژه: استفاده از نرم افزارهای مدیریت گذرواژه

1. KeePass
   - https://keepass.info/
2. LastPass…
   - https://www.lastpass.com/
3. Roboform
   - https://www.roboform.com/
4. Kaspersky Password Manager
   - https://www.kaspersky.com/password-manager
5. Dashlane
   1. https://www.dashlane.com/

ROUGINE
DAROU

استفاده محتاطانه و درست از ایمیل

1. عدم استفاده از ایمیل کاری در سایتهای متفرقه
2. در صورت امکان احراز هویت دومرحله‌ای را فعال کنید.
3. معرفی روشهای مختلف انجام جرم در ایمیل
    1. تشویق به باز کردن یک لینک اینترنتی
    2. تشویق به باز کردن یک فایل پیوست
    3. از طریق تهدید به افشای اطلاعات شخصی و اخاذی

ROUGINE DAROU

طبقه بندی کردن اطلاعات

- نمونه طبقه بندی اطلاعات
  - عمومی Public
  - خصوصی Private
  - محرمانه Restricted
  - سری Confidential

ROUGINE
DAROU

سطوح دسترسی شرکت روژین دارو

سطح	نوع اطلاعات	دسترسی
عمومی(Public)	غیرحساس	همه افراد می‌توانند دسترسی داشته باشند.
داخلی(Internal)	غیرحساس	تمامی کارکنان دسترسی دارند.
محرمانه(Restricted)	حساس	برخی مدیران با مجوز مدیرعامل دسترسی دارند.
سری(Confidential)	بسیار حساس	فقط مدیرعامل دسترسی دارد؛ سایر مدیران ارشد تنها در صورت امضای توافق‌نامه محرمانگی می‌توانند دسترسی یابند.

ROUGINE DAROU

قوانین نگهداری اطلاعات شرکت روژین دارو

نوع / برچسب	Internal	Restricted	Confidential
سوابق کاغذی	می‌تواند در کابینت بدون قفل نگهداری شود	باید در کابینت قفل‌دار نگهداری شود	در مکان ایمن ذخیره شود
Digital Files	فضای اشتراک‌گذاری عمومی	فضای اشتراک‌گذاری خصوصی	در سیستم افراد مجاز با محدودیت دسترسی لازم ذخیره شود
Removable Device	در محل عمومی	در محل خصوصی کارمند مربوطه	در محل افراد مجاز با محدودیت دسترسی لازم نگهداری شود
Email	در دستگاه اختصاصی هر کارمند و روی سرور داخلی شرکت روژین دارو	در دستگاه اختصاصی هر کارمند و روی سرور داخلی شرکت روژین دارو	روی سرور داخلی شرکت روژین دارو با محدودیت دسترسی لازم ذخیره شود

ROUGINE DAROU

سیاست حفظ حریم خصوصی(Privacy Policy)

- سیاست حفظ حریم خصوصی، بیانیه یا سند حقوقی است که برخی یا تمامی روش‌های جمع‌آوری، استفاده، افشا و پردازش داده‌های کارکنان یا سایر اشخاص ذی‌نفع را تشریح می‌کند.
- اطلاعات شخصی شامل هرگونه داده‌ای است که بتوان از آن برای شناسایی یک فرد استفاده کرد، از جمله (اما نه محدود به): نام، آدرس، تاریخ تولد، وضعیت تأهل، اطلاعات تماس، شماره شناسایی، سوابق مالی، سوابق پزشکی، مکان‌های سفر و نیت خرید کالا یا خدمات.

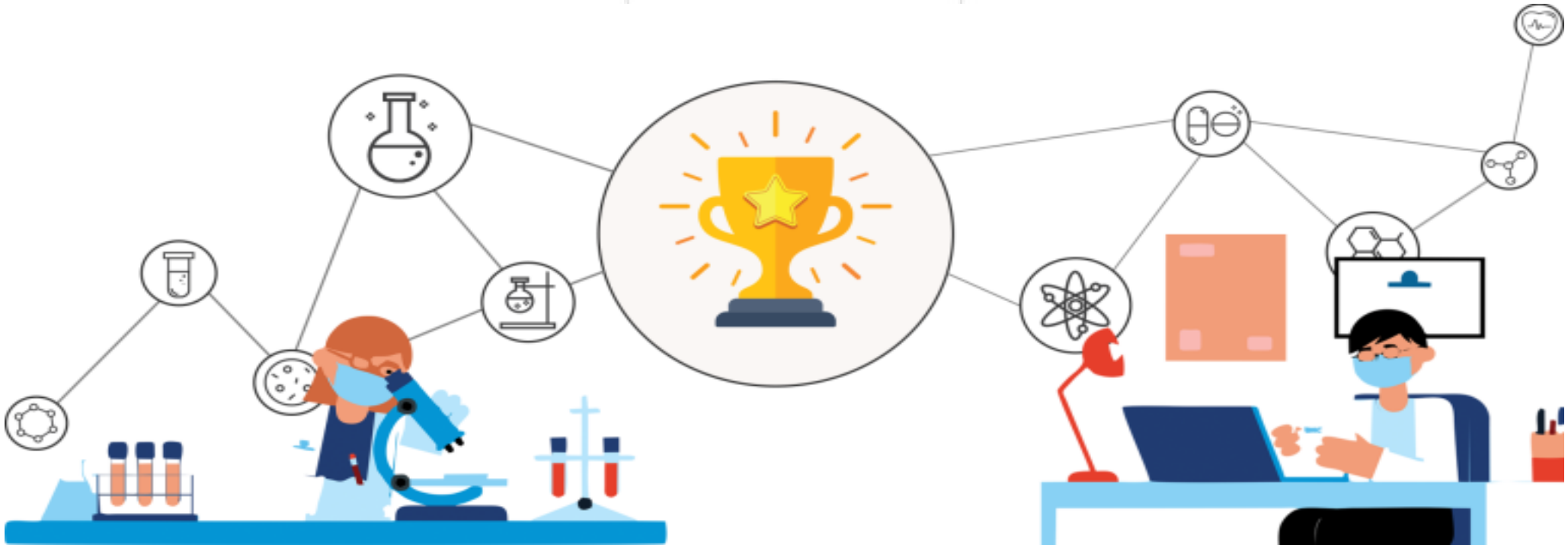
ملاحظات مربوط به اطلاعات شخصی(Personal Information Considerations)

- جمع‌آوری و استفاده از داده‌های شخصی شما
- نحوه استفاده از داده‌های شخصی
- اشتراک‌گذاری داده‌های شخصی
- نگهداری داده‌های شخصی
- انتقال داده‌های شخصی
- افشای داده‌های شخصی
- امنیت داده‌های شخصی
- پردازش داده‌های شخصی
- حقوق شما بر اساس مقرراتGDPR

ROUGINE
DAROU

اشتراک گذاری اطلاعات

- ضرورت داشتن راهکرد در زمینه اشتراک گذاری اطلاعات در شرکت
- اشتراک گزاری بر روی شبکه محلی
- اشتراک گزاری بر روی اینترنت
- اشتراک گذاری بر روی شبکه های اجتماعی



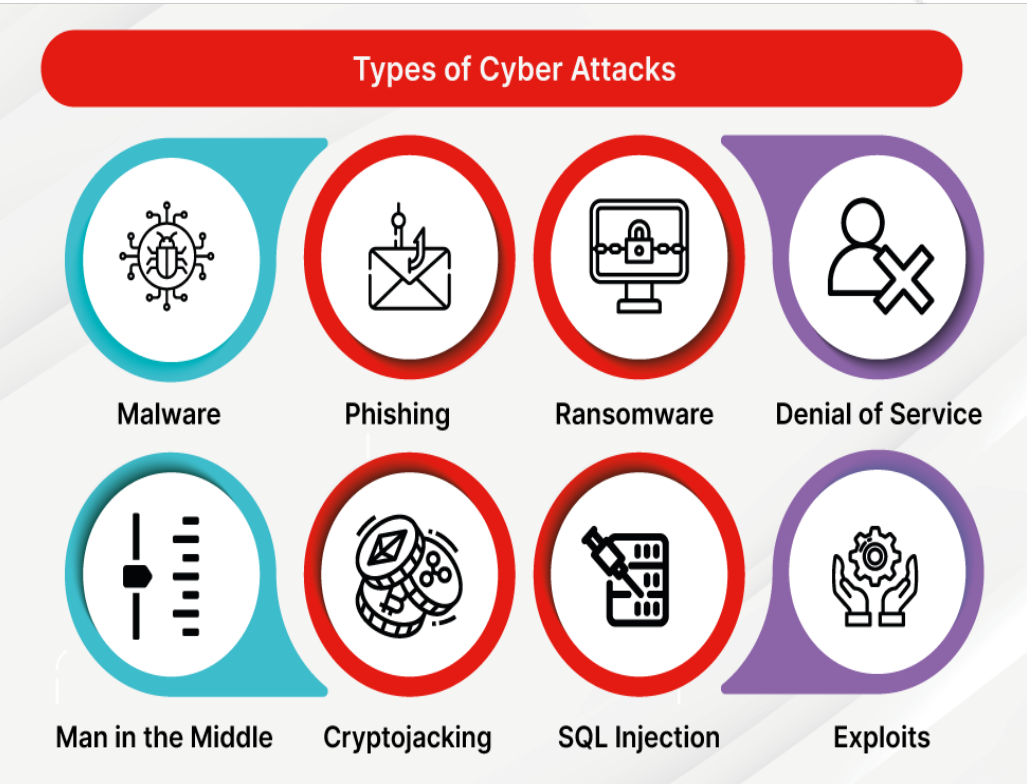
ROUGINE
DAROU

امنیت سایبری چیست؟(What is Cyber Security?)

امنیت سایبری، به معنای حفاظت از رایانه‌ها، سرورها، دستگاه‌های همراه، سیستم‌های الکترونیکی، شبکه‌ها و داده‌ها در برابر حملات مخرب است.
به آن "امنیت فناوری اطلاعات" یا "امنیت اطلاعات الکترونیکی" نیز گفته می‌شود.
این مفهوم در زمینه‌های مختلفی از جمله کسب‌وکار تا محاسبات همراه کاربرد دارد و به چند دسته رایج تقسیم می‌شود.

ROUGINE
DAROU

انواع حملات سایبری:(Cyber Attack Types)



- **بدافزارها :(Malware)** شامل تروجان، کرم، ویروس و...
- **باج‌افزار :(Ransomware)** رمزگذاری فایل‌ها توسط هکرها برای اخاذی
- **مهندسی اجتماعی :(Social Engineering)** یافتن نقاط ضعف انسانی یا سیستمی
- **فیشینگ :(Phishing)** ارسال ایمیل‌ها یا پیام‌های جعلی برای فریب کاربران
- **تهدیدات داخلی :(Insider Threats)** جاسوسی یا افشای اطلاعات توسط افراد داخلی یا طرف سوم
- **سایر موارد**

ROUGINE DAROU

ضعیف ترین حلقه زنجیره امنیت ؟؟؟؟؟

ROUGINE
DAROU

مهندسی اجتماعی

- **مهندسی اجتماعی** سوء استفاده زیرکانه از تمایل طبیعی انسان به اعتماد کردن است، که به کمک مجموعه‌ای از تکنیک‌ها، فرد را به فاش کردن اطلاعات یا انجام کارهایی خاص متقاعد می‌کند.
- مهاجم به جای استفاده از روش‌های معمول و مستقیم نفوذ جمع‌آوری اطلاعات و عبور از دیواره آتش برای دسترسی به سیستم‌های سازمان و پایگاه داده‌های آن، از مسیر انسان‌هایی که به این اطلاعات دسترسی دارند و با استفاده از تکنیک‌های فریفتن آنها، به جمع‌آوری اطلاعات در راستای دستیابی به خواسته‌های خود اقدام می‌کند.

ROUGINE
DAROU

امنیت شبکه های اجتماعی

- مراقب اطلاعات شخصی باشید.
  - حتی یک پست ساده می‌تونه اطلاعات زیادی از شما فاش کنه.
- لینک‌ها و پیام‌های ناشناس را باز نکنید.
  - هر لینکی که می‌گه "اکانت شما قفل شد" یا "جایزه بردی" را نزنید.
- مراقب دسترسی به حساب باشید.
  - برنامه‌های متفرقه یا مشکوک را به حساب خود متصل نکنید.
  - هر چند وقت یکبار در تنظیمات حساب، Active Sessions را بررسی کنید
- خروج از حساب در دستگاه‌های عمومی.
  - اگر از سیستم شرکت یا کافی‌نت وارد حساب شدی، حتماً بعد از کار Logoutکن.

ROUGINE DAROU

فیشینگ

- به تلاش برای بدست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و... از طریق جعل یک وب‌سایت، آدرس ایمیل و... گفته می‌شود. و یا به عبارت ساده‌تر وقتی شخصی سعی می‌کند شما را فریب دهد تا اطلاعات شخصی‌تان را در اختیارش بگذارید، یک حمله فیشینگ اتفاق می‌افتد.

ROUGINE
DAROU

انواع حملات فیشینگ

1. فیشنگ وبسایت
   1. http://www.ebanking.bankmellat.ir/ebanking
   2. ~~https://ebanking.bankemellat.com/ebanking/~~
2. فیشینگ ایمیل
3. فیشنگ تلفنی
4. فیشینگ کارت بانکی ATM

ROUGINE DAROU

باج افزارها
Ransomwares

- باج‌افزارها (به انگلیسی: Ransomware) گونه‌ای از بدافزارها هستند که دسترسی به سیستم را محدود می‌کنند و ایجادکننده آن برای برداشتن محدودیت درخواست باج می‌کند. برخی از انواع آن‌ها روی فایل‌های هارددیسک رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سیستم را قفل کنند و پیام‌هایی روی نمایشگر نشان دهند که از کاربر می‌خواهد مبالغی را واریز کنند

ROUGINE DAROU

تهیه پشتیبان از فایلهای مهم

1. چرا باید پشتیبان گرفت
    1. خطاهای سخت افزاری
    2. خطاهای انسانی
    3. محافظت در برابر برنامه های مخرب (باج افزار، ویروس...)
2. از چه فایلهایی باید پشتیبان گرفت
3. روشهای پشتیبان گیری و استراتژی آن
    1. پشتیبان کامل
    2. پشتیبان افزایشی
    3. پشتیبان افتراقی
    4. پشتیبان Mirror

ROUGINE DAROU

آنتی ویروس و بروز رسانیها

روزانه از عملکرد آنتی ویروس خود اطمینان حاصل نمایید و در صورت عدم فعالیت حتما با دپارتمان فناوری اطلاعات مطرح کنید

استفاده از نرم افزارهای تایید شده و معتبر

ROUGINE
DAROU

از بین بردن وسایل دارای اطلاعات

- هیچ گاه وسایل ذخیره اطلاعات خود را مانند :

•سی-دی، هارد، فلش و ...

- را به گمان اینکه خراب هستند و دیگر کار میکنند به سادگی در سطل آشغال نیاندازید.

ROUGINE DAROU

گزارش موارد امنیتی

- در صورت مشاهده هر گونه موارد مشکوک حتما در سریع ترین زمان دپارتمان فناوری اطلاعات را مطلع کنید

ROUGINE
DAROU

تیکتینگ

- سازماندهی درخواست ها
- تسریع در در رسیدگی
- مستندسازی
- بهبود کیفیت خدمات IT

ROUGINE
DAROU

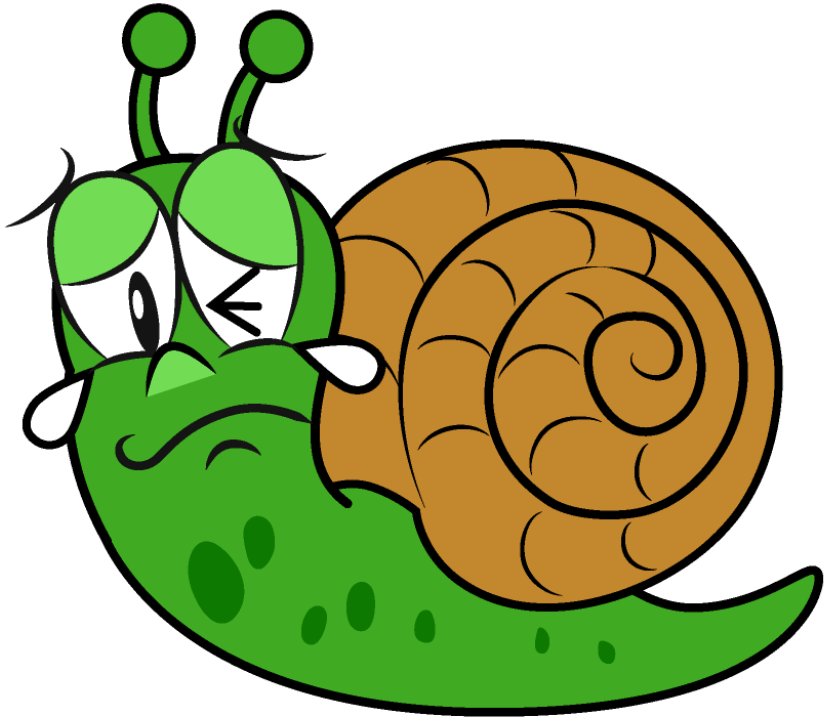
مشکلات رایج ایمیل

- بروز نشدن جلسات
- حذف شدن ایمیل
- Indexing
- نداشتن امضا
- اسپم
- Failed شدن ایمیل

پیغام	علت
Delivery has been delayed	ایمیل هنوز به مقصد نرسیده ولی Failed هم نشده.
Message size exceeds limit	بیشترین بودن حجم فایل ضمیمه از حد مجاز(20MB)
Greylisting delay	سرور مقصد ایمیل شما رو اسپم تشخیص داده
Failed to connect to the recipient's mail server	برقرار نبود ارتباط با سرور مقصد
Delivery not authorized	ایمیل شما خلاف قوانین میل سرور مقصد میباشد

ROUGINE
DAROU

کندی سیستم



- ساعت اسکن آنتی ویروس
- پر شدن RAM
- درگیر بودن CPU
- قدیمی بودن Hard Disk
- برنامه های پس زمینه
- پر شدن درایور C

ROUGINE
DAROU

مشکلات عمومی

- مانیتور وصل هست ولی تصویر ندارم؟
  - WIN + P برای تنظیم مانیتور دوم
  - خرابی کابل HDMI و یا تبدیل
- باتری لپتاپ زود تموم میشه.
  - سلامت باتری معمولاً بعد از ۳۰۰–۵۰۰ چرخه شارژ کامل شروع به افت می‌کنه.
  - بررسی با نرم افزار **BatteryInfoView**

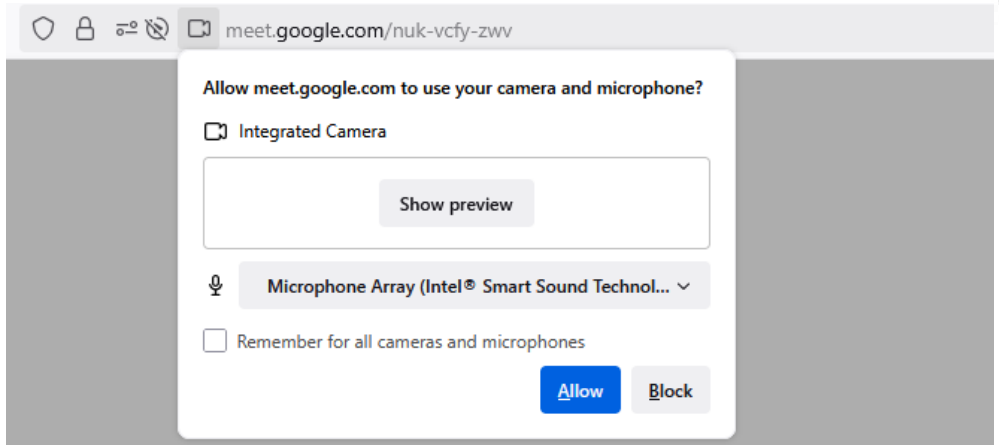
درصد سلامت (Battery Health)	تفسیر	پیشنهاد
90–100%	عالی	نگهدارنده خوب
75–89%	خوب	طبیعی برای باتری چندساله
60–74%	ضعیف	عملکرد و شارژ کمتر حس می‌کنی
زیر 60%	خیلی ضعیف	بهتره باتری تعویض بشه

مشکلات عمومی

- دکمه های نرم افزار آفیس غیرفعال شدن،چرا؟
  - تموم شدن Activation
- اعداد در آفیس فارسی نیستند.
  - رفتن به مسیر File => Options =>Advanced و تغییر گزینه Numeral به Context
- رمز ورود به چارگون یا Output messenger میگه اشتباه هستش.
  - زمان تغییر دوره ای رمزتون رسیده و رمز قبلی از کار افتاده با قفل کردن سیستم(WIN + L) مجدد رمز رو میزنیم و رمز جدید میزاریم.
- هرچی تو اکسل نوشته بودم پرید.
  - کم کردن زمان Auto Save از File => Options => Save

ROUGINE
DAROU

مشکلات جلسات آنلاین



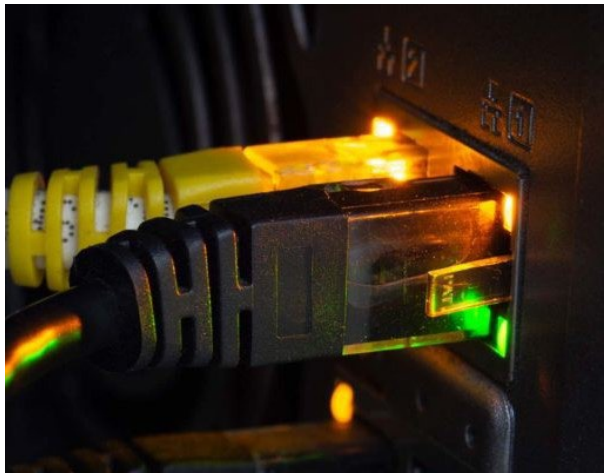
- نداشتن صدا/تصویر در جلسات آنلاین
  - ندادن دسترسی دوربین و میکروفون توسط کاربر

- لینک جلسه باز نمیشه.

سرویس دهنده	مشکل	راهکار
Teams	خطا هنگام اجرای نرم افزار	باز کردن در مرورگر بجای اپلیکیشن
Zoom	خطای اشتباه بودن کد جلسه	استفاده از VPN و خاموش کردن پس از ورود
Meet	باز نشدن لینک	نیاز به لاگین شدن به جیمیل

ROUGINE DAROU

مشکلات پرینتر و اسکنر



- خط روی تصویر اسکن شده
  - کثیفی صفحه اسکنر روی لنز
- پرینت میفرستم ولی پرینت نمیگیره.
  - چک کردن چراغ کابل شبکه

- انواع لکه و کثیفی روی پرینت

مشکل	دلیل	راه حل
کثیفی پراکنده	کثیفی کارتریج یا دستگاه	تمیز کردن کارتریج
خط صاف	خراب شدن کارتریج یا قطعه پرینتر	تعویض کارتریج
کم رنگی بعضی نواحی	پخش نشدن جوهر کارتریج	تکان دادن کارتریج

ROUGINE
DAROU

مشکلات شبکه و اینترنت

- Ping چیست؟
  - ابزاری برای تست ارتباط بین دو دستگاه در شبکه (مثلاً کامپیوتر شما و یک سایت).
- SAP کند هستش،گوگل هم باز نمیشه.
  - استفاده از Speed Test
  - با استفاده از ابزار Ping متوجه میشیم مشکل از چیه(سراغ کی بریم).
  - ابزار CMD رو در ویندوز سرچ و باز میکنیم:

Ping 192.168.100.26 یا Ping google.com

پینگ داخلی	پینگ خارجی
<10	<100

ROUGINE DAROU

ابزار های کاربردی تحت وب

- Ilovepdf : فشرده سازی PDF
- Convertio : تبدیل فرمت ها
- Removebg : حذف پس زمینه تصاویر
- writetone : ابزار های اصلاح متن با هوش مصنوعی
- Miro : تخته سفید دیجیتال
- TotalVirus : آنتی ویروس همه کاره آنلاین
- Leakfa : سامانه ردیابی نشت اطلاعات

ROUGINE
DAROU

سوال

ROUGINE
DAROU

Thank You

ROUGINE
DAROU