پلتفورم های باز
و مهارت های دیجیتالی

(Open Platforms and Digital Skills)

TLM Level 2

صنوف دهم، یازدهم، دوازدهم

تسریعی ب و سطح 2 بین المللی

نویسنده: محمدعارف رضوان پناه

مهارت برای آینده | همکاری آنلاین | مدیریت معلومات | امنیت دیجیتالی | پادگیری عملی

پلتفورم های باز و مهارت های دیجیتالی

(Open Platforms and Digital Skills)

TLM Level 2

صنوف دهم، یازدهم، دوازدهم

تسریعی ب و سطح 2 بین المللی

رهنمایی آموزشی ICT و دیجیتال

این رهنمای آموزشی در چهار فصل و به‌صورت شارت‌نوت تهیه شده است. این مجموعه، مهم‌ترین عناوین و مهارت‌های عملی را در بر می‌گیرد و برای یادگیری مؤثر دانش‌آموزان بسیار ضروری است. با این حال، لازم است دانش‌آموزان علاوه بر مطالعه این جزوه، دوره عملی TLM Level 2 را نیز سپری کنند؛ زیرا اگر دانش‌آموزان تنها به مطالعه نوت‌های درسی اکتفا کنند، حداکثر حدود ۵۰ درصد از مفاهیم و مهارت‌های مرتبط با مضمون ICT را فرا خواهند گرفت.

از آنجا که مباحث این رهنما بیشتر جنبه نظری دارند، برای درک بهتر و تطبیق عملی این مفاهیم، ضروری است دانش‌آموزان به لابراتوار کمپیوتر مراجعه کرده، تمرین‌های عملی را انجام دهند و پورتفولیوی آنلاین خود را به‌طور کامل تکمیل نمایند.

فهرست مطالب

به تمام دختران باعزم، پرتلاش و جویندگان راه علم و دانش؛

این اثر با نهایت احترام، مهر و آرزوی موفقیت به شما اهداء می‌گردد؛ به دخترانی که با وجود دشواری‌ها و محدودیت‌ها، هنوز هم با امید، اراده و پشتکار در راه آموختن گام برمی‌دارند و باور دارند که دانش، روشنایی زندگی و کلید پیشرفت یک جامعه است.

شما چراغ‌های فروزان آینده این سرزمین هستید؛ دخترانی که با قلم، اندیشه و آگاهی می‌توانند تغییرات بزرگ به‌وجود آورند. هر صفحه‌ای که می‌خوانید، هر مهارتی که می‌آموزید و هر دانشی که به‌دست می‌آورید، نه تنها آینده شما، بلکه آینده نسل‌های بعدی را نیز روشن‌تر می‌سازد. جامعه‌ای که دختران آن باسواد، آگاه و دانا باشند، جامعه‌ای نیرومند، پیشرفته و سربلند خواهد بود.

راه دانش شاید همیشه آسان نباشد، اما ارزش آن بسیار بزرگ و ماندگار است. انسان دانا می‌تواند تاریکی نادانی را از میان بردارد و با خرد و آگاهی برای خود و دیگران راه درست را نشان دهد. شما جویندگان علم، سرمایه‌های واقعی این سرزمین هستید و تلاش شما برای یادگیری، نشانه امید برای فردایی بهتر است.

امید است هیچ مانع و مشکلی نتواند شما را از رسیدن به آرزوها و هدف‌های بلندتان باز دارد و همواره با ایمان، استقامت و امید به پیش بروید. باور داشته باشید که آینده از آن کسانی است که برای آموختن، رشد کردن و خدمت به جامعه دست از کوشش برنمی‌دارند.

با آرزوی روزی که صدای قلم، دانش و آگاهی در سراسر جامعه ما بلندتر از هر صدای دیگری باشد.

محمدعارف "رضوان پناه"

1405 ه.ش

2026 میلادی

پل آموزش برای افغانستان

(Open Platforms and Digital Skills)

TLM Level 2

صنوف دهم، یازدهم، دوازدهم

تسریعی ب و سطح 2 بین المللی

برای سنین بین

14 تا 16 سال

اهمیت و ضرورت این بسته آموزشی برای دانش آموزان

در دنیای امروزی، تکنالوژی دیجیتلی بخش مهم و جدایی‌ناپذیر زندگی انسان‌ها گردیده است. تقریباً تمام اداره‌ها، شرکت‌ها، مکاتب، پوهنتون‌ها، بانک‌ها، شفاخانه‌ها و حتی تجارت‌های کوچک برای انجام کارهای روزمره خود از سیستم‌های دیجیتلی استفاده می‌کنند. به ُهمین دلیل، فراگیری مهارت‌های دیجیتلی و آشنایی با امنیت سایبری، مدیریت معلومات، تولید محتوا و استفاده درست از سیستم‌های آنلاین، یکی از نیازهای اساسی هر فرد در جامعه امروز به شمار می‌رود. این بسته آموزشی نه تنها معلومات نظری ارائه می‌کند، بلکه مهارت‌های عملی و کاربردی را نیز آموزش می‌دهد تا فراگیران بتوانند در محیط واقعی کار از آن استفاده نمایند.

افرادی که این بسته آموزشی را فرا می‌گیرند، با مفاهیم مهمی مانند امنیت دیجیتلی، محافظت از معلومات شخصی، استفاده مصئون از اینترنت، مدیریت پروفایل دیجیتلی، تولید محتوا، استفاده از نرم‌افزارهای کاربردی و روش‌های مقابله با تهدیدات سایبری آشنا می‌شوند. این مهارت‌ها در عصر حاضر بسیار ارزشمند است؛ زیرا بسیاری از مشکلات و خطرات آنلاین ناشی از ناآگاهی کاربران می‌باشد. فردی که این آموزش‌ها را تکمیل کند، می‌تواند از معلومات شخصی و کاری خود بهتر محافظت کرده و در محیط دیجیتلی مسئولانه‌تر عمل نماید.

یکی از مهم‌ترین ارزش‌های این بسته آموزشی، آماده‌ساختن افراد برای بازار کار آینده است. امروزه بیشتر وظایف نیازمند آشنایی با کمپیوتر، اینترنت و ابزارهای دیجیتلی می‌باشند. کسانی که در این بخش مهارت داشته باشند، فرصت‌های کاری بیشتری نسبت به دیگران خواهند داشت. فراگیران پس از یادگیری این مهارت‌ها می‌توانند در بخش‌های مختلف فعالیت نمایند؛ مانند:

- اداره‌های دولتی و خصوصی
- بانک‌ها و شرکت‌های مالی
- مکاتب، پوهنتون‌ها و مراکز آموزشی
- رسانه‌ها و بخش تولید محتوا
- طراحی گرافیک و تولید دیجیتلی
- مدیریت شبکه‌های اجتماعی
- خدمات مشتریان آنلاین
- شرکت‌های تکنالوژی معلوماتی (IT)
- امنیت سایبری و محافظت سیستم‌ها
- فروشگاه‌ها و تجارت‌های آنلاین

همچنان این آموزش‌ها زمینه خوبی برای فریلنسری و کارهای آنلاین فراهم می‌سازد. بسیاری از جوانان امروز از طریق مهارت‌های دیجیتلی مانند طراحی، مدیریت صفحات اجتماعی، تولید محتوا، ساخت ویب‌سایت و خدمات آنلاین درآمد به‌دست می‌آورند. بنابراین، فراگیری این مهارت‌ها تنها محدود به وظیفه اداری نیست، بلکه می‌تواند راهی برای خوداشتغالی و کسب درآمد مستقل نیز باشد.

این بسته آموزشی همچنان باعث رشد مهارت‌های فکری و اجتماعی فراگیران می‌شود. شاگردان یاد می‌گیرند چگونه معلومات را تحلیل کنند، چگونه به‌صورت مصئون در فضای آنلاین فعالیت نمایند و چگونه از ابزارهای دیجیتلی برای حل مشکلات استفاده کنند. این مهارت‌ها اعتماد به نفس افراد را افزایش داده و آن‌ها را برای آینده تحصیلی و کاری آماده‌تر می‌سازد.

در جامعه امروزی، داشتن سواد دیجیتلی دیگر یک انتخاب نیست، بلکه یک ضرورت است. فردی که نتواند از تکنالوژی به‌گونه درست استفاده کند، در بسیاری از بخش‌های زندگی و کار با مشکل روبه‌رو خواهد شد. این بسته آموزشی تلاش می‌کند تا نسل جوان را با مهارت‌ها و دانشی مجهز سازد که در آینده بتوانند به‌عنوان افراد آگاه، مسئول و توانمند در جامعه نقش مثبت ایفا کنند.

در پایان می‌توان گفت که این آموزش‌ها تنها یادگیری چند نرم‌افزار یا ابزار نیست؛ بلکه آماده‌ساختن افراد برای زندگی، کار و ارتباطات در دنیای دیجیتلی امروز و آینده می‌باشد. هر فردی که این مهارت‌ها را بیاموزد، می‌تواند فرصت‌های بهتر آموزشی، شغلی و اجتماعی به‌دست آورده و با دانش و توانایی بیشتر در مسیر موفقیت گام بردارد.

مقدمه

در عصر حاضر، تکنالوژی دیجیتلی به بخش جدایی‌ناپذیر زندگی انسان‌ها تبدیل شده است. امروزه تقریباً تمام فعالیت‌های روزمره، از آموزش و تجارت گرفته تا ارتباطات، خدمات بانکی، اداره‌ها و حتی سرگرمی، وابسته به سیستم‌های دیجیتلی و اینترنت می‌باشد. در چنین شرایطی، داشتن دانش و مهارت در زمینه سواد دیجیتلی، امنیت سایبری و استفاده درست از تکنالوژی، دیگر یک انتخاب نیست؛ بلکه یک ضرورت اساسی برای هر فرد محسوب می‌شود. این مضمون آموزشی با هدف آشنا ساختن شاگردان با مفاهیم مهم دیجیتلی، امنیت آنلاین، مدیریت معلومات و استفاده مصئون از تکنالوژی طراحی شده تا نسل جوان بتواند در دنیای مدرن امروز به‌گونه آگاهانه و مسئولانه فعالیت نماید .

یکی از مهم‌ترین ویژگی‌های این مضمون، عملی و کاربردی بودن آن است. شاگردان در این مضمون تنها مفاهیم نظری را نمی‌آموزند، بلکه مهارت‌هایی را فرا می‌گیرند که مستقیماً در زندگی روزمره، ادامه تحصیل و آینده شغلی آنان مورد استفاده قرار می‌گیرد. موضوعاتی مانند محافظت از معلومات شخصی، شناخت تهدیدات آنلاین، استفاده ایمن از اینترنت، امنیت رمزهای عبور، مدیریت پروفایل دیجیتلی، شناخت بدافزارها، جلوگیری از کلاه‌برداری آنلاین و استفاده از نرم‌افزارهای کاربردی، همه از جمله مهارت‌هایی اند که در دنیای امروزی حیاتی شمرده می‌شوند. این مهارت‌ها سبب می‌شود تا شاگردان بتوانند در برابر خطرات فضای مجازی از خود محافظت کرده و از تکنالوژی به شکل مؤثر و سالم استفاده نمایند .

اهمیت این مضمون زمانی بیشتر روشن می‌شود که بدانیم بسیاری از مردم، مخصوصاً جوانان، هر روز از اینترنت و شبکه‌های اجتماعی استفاده می‌کنند؛ اما آگاهی کافی درباره تهدیدات سایبری، سرقت معلومات، فریب‌های آنلاین و امنیت دیجیتلی ندارند. نبود آگاهی در این بخش می‌تواند باعث مشکلات جدی مانند سرقت حساب‌ها، افشای معلومات شخصی، سوءاستفاده مالی و حتی آسیب‌های اجتماعی و روانی شود. بنابراین، آموزش چنین مضامینی نقش مهمی در بلند بردن سطح آگاهی جامعه و کاهش خطرات آنلاین دارد. این مضمون نه تنها شاگردان را برای استفاده بهتر از تکنالوژی آماده می‌سازد، بلکه آن‌ها را به کاربران مسئول، آگاه و قانون‌مدار در فضای دیجیتلی تبدیل می‌کند.

از سوی دیگر، این مضمون می‌تواند زمینه‌ساز فرصت‌های گسترده شغلی برای شاگردان باشد. افرادی که در بخش تکنالوژی و امنیت دیجیتلی مهارت داشته باشند، در آینده می‌توانند در بخش‌های مختلف مانند اداره‌های دولتی و خصوصی، بانک‌ها، رسانه‌ها، شرکت‌های تکنالوژی معلوماتی، مدیریت شبکه‌های اجتماعی، تولید محتوا، طراحی گرافیک، امنیت سایبری، آموزش دیجیتلی و تجارت آنلاین

فعالیت نمایند. همچنان این مهارت‌ها زمینه خوبی برای فریلنسری و کارهای آنلاین فراهم می‌کند؛ بخشی که امروزه در سراسر جهان رشد چشم‌گیری داشته است .

یکی از نکات بسیار مهم و قابل تأمل، نبود چنین مضمون‌های معیاری و به‌روز در ساختار درسی معارف افغانستان است. در حالی‌که بسیاری از کشورها آموزش سواد دیجیتلی و امنیت سایبری را از صنوف پایین آغاز کرده‌اند، در نظام آموزشی افغانستان هنوز هم تمرکز اصلی بر روش‌های سنتی آموزش قرار دارد و شاگردان کمتر با مهارت‌های عملی و تکنالوژی مدرن آشنا می‌شوند. این کمبود سبب شده است که تعداد زیادی از جوانان، با وجود استفاده روزانه از موبایل و اینترنت، آگاهی کافی درباره استفاده مصئون و حرفه‌ای از تکنالوژی نداشته باشند. افزودن چنین مضامین در نصاب تعلیمی می‌تواند نسل آینده را برای بازار کار جهانی، آموزش آنلاین و زندگی دیجیتلی آماده‌تر سازد.

این مضمون در حقیقت پلی میان آموزش سنتی و نیازهای دنیای مدرن است. آموزش مهارت‌های دیجیتلی، امنیت آنلاین و مدیریت معلومات، نه تنها یک ضرورت آموزشی، بلکه یک نیاز حیاتی اجتماعی و اقتصادی به شمار می‌رود. جامعه‌ای که جوانان آن دارای سواد دیجیتلی و آگاهی سایبری باشند، بهتر می‌تواند با تحولات سریع جهان همگام شود و در عرصه‌های علمی، اقتصادی و تخنیکی پیشرفت نماید. به همین دلیل، گسترش و حمایت از چنین آموزش‌هایی می‌تواند نقش مهمی در رشد علمی، فرهنگی و تخنیکی کشور داشته باشد.

خلاصه دوره ICT و دیجیتال

بخش حرفه‌ای : ICT و دیجیتال
کد QAN : 603/1204/X
محدوده سنی: 14 الی 16 سال

نحوه ارزیابی دوره:

- یک امتحان تحریری (آنلاین)
- کورس‌ورک (کارهای عملی) که توسط مرکز ارزیابی و توسط TLM نظارت (Moderation) می‌شود
- پورتفولیوی دیجیتال دانش آموز که استفاده او از یک پلتفرم دیجیتال را نشان می‌دهد

نحوه نمره‌دهی:

این دوره به درجات ذیل ارزیابی می‌شود:

درجه(Grade)	ترجمه به دری	توضیح
Pass	قبول	حداقل نمره قبولی
Merit	خوب	عملکرد بالاتر از حد متوسط
Distinction	عالی	عملکرد بسیار خوب
Distinction*	عالی‌تر	بالاترین سطح عملکرد

ثبت‌نام مراکز:

این دوره نیاز دارد که مراکز در TLM ثبت شوند و هر دانش آموز نیز در سایت TLM Markbook ثبت‌نام گردد.

یونیت‌های اجباری(Mandatory Units)

1. درک پلتفورم‌های دیجیتال و معیارهای باز(Open Standards)
2. مدیریت پلتفورم‌های دیجیتال و تطبیق مهارت‌های دیجیتال
3. حفاظت از پلتفورم‌های دیجیتلی و آماده ساختن آن‌ها برای استفاده در آینده
4. پلان‌گذاری، اجرا و ارزیابی سیستم‌های دیجیتال

تضمین کیفیت(Quality Assurance)

- بررسی سالانه برای تأیید کیفیت مراکز
- ورکشاپ‌های رایگان هفتگی برای معلمان
- اشتراک‌گذاری بهترین تجارب بین مراکز
- بررسی کورس‌ورک توسط TLM و کنترول سرقت ادبی(Plagiarism)

نمره‌دهی:

- 20 نمره برای کار خوب
- 10 نمره اضافی برای کار عالی
- امتحان از 70 نمره است
- مجموع: 100 نمره
- نمره قبولی: 50 از 100

زمان کوالیفکیشن(Qualification Time)

- GLH[1] ساعات آموزشی هدایت‌شده: **125 ساعت**
- TQT[2]مجموع زمان کوالیفکیشن: **140 ساعت**

جدول زمانی

یونیت	عنوان	GLH (ساعات درسی)	TQT اضافه	TQT مجموع
TLM1	درک پلتفورم‌های دیجیتال و معیارهای باز	25	3	28
TLM2	مدیریت پلتفورم‌های دیجیتال و مهارت‌های دیجیتال	25	3	28
TLM3	محافظت و آینده‌سازی پلتفورم‌های دیجیتال	25	3	28
TLM4	پلان‌گذاری، اجرا و ارزیابی سیستم‌های دیجیتال	50	6	56

[1] **GLH:** Guided Learning Hours

[2] **TQT:** Total Qualification Time

فصل اول

آشنایی با سیستم‌های دیجیتال و قوانین مشترک آن‌ها

(Open Standards)

شرایط بخش اول:

- **ساعت های درسی:** 25 ساعت
- **ساعت های اصافی:** 3 ساعت
- **مجموع ساعت های درسی:** 28 ساعت

در این بخش دانش آموزان می آموزند:

- **Strand 1**
  - درک این‌که سیستم‌های دیجیتال برای جمع‌آوری و پردازش حجم زیاد داده ساخته می‌شوند تا اطلاعات تولید کنند. همچنان روش‌هایی را می‌آموزند که اطلاعات برای قناعت‌دادن یا حتی فریب‌دادن استفاده می‌شود.
- **Strand 2**
  - شناخت انواع مواد دیجیتال در بخش‌های مختلف (دولتی و خصوصی) و درک تأثیر آن‌ها بر نتایج. همچنان آگاهی از استفاده‌های جرمی دیتا و اطلاعات.

- **Strand 3**
  - یادگیری روش‌های جمع‌آوری دیتا خام و استفاده از آن در برنامه‌ها با فرمت‌های مختلف. همچنین آشنایی با قوانین و مقررات مربوط به دیتاها.
- **Strand 4**
  - درک تفاوت بین داده و اطلاعات و این‌که چه زمانی داده به اطلاعات تبدیل می‌شود. همچنان شناخت نقش معیارهای باز (Open Standards) در اینترنت و تأثیرات مثبت و منفی آن.
- **Strand 5**
  - بررسی این‌که چرا اطلاعات به شکل خاصی استفاده می‌شود (مثلاً تأثیر پول یا مسائل اجتماعی). همچنین تأثیر آن بر کارهای دیجیتال خودشان و نقش قوانین در حفاظت از آن‌ها.

محتوا:

متحوایی این کتاب در تما فصول مانند یک خلاصه نویسی میباشد و نیاز به ویدیوهای آموزشی نظر به موضوعات و مرور مقالات و کتابها نیز میباشد. چون در این کتاب نظر به حجم زیاد موضوعات بعضی موضوعات بسیار فشرده پرداخته شده است.

1.1 آشنایی با سیستم‌های دیجیتال و قوانین مشترک آن‌ها

1. دیتا چیست؟

دیتا معلومات خام است که هنوز هیچ تحلیل و پروسس بالایی آن انجام نشده است. به عبارت دیگر:

- ترتیب ندارد
- تحلیل نشده
- معنی واضح ندارد
- دیتا می‌تواند باشد: 255 و 100
- متن (کابل، احمد)
- تصویر (عکس)
- صدا (Voice)
-
- **نکته مهم:**

دیتا به تنهایی **ارزش زیاد ندارد** تا وقتی که تحلیل و پروسس نشود.

2. اطلاعات (Information) چیست؟

اطلاعات زمانی ساخته می‌شود که:

✓ دیتا ترتیب داده شود.

✓ با هم ارتباط پیدا کند.

✓ یک معنی مشخص داشته باشد.

یعنی:

دیتا + تحلیل + معنی = اطلاعات (Information)

فکر کنید که چند نوع دیتا را میشناسید؟ آیا تا به حال به اونواع دیتا فکر کرده اید؟

3. مراحل تبدیل دیتا به اطلاعات

این بخش خیلی مهم است:

1. جمع‌آوری دیتا (Collection)

مثال: موبایل شما مکان را ثبت می‌کند

2. ذخیره دیتا (Storage)

دیتا در سیستم یا سرور ذخیره می‌شود

3. پردازش دیتا (Processing)

دیتاها تحلیل و بررسی می‌شوند

4. تبدیل به اطلاعات (Output)

نتیجه قابل فهم ساخته می‌شود

تعریف کامل اطلاعات:
دیتایی که پروسس (پردازش)، تحلیل و تنظیم شده باشد و دارای معنی واضح و قابل استفاده برای تصمیم‌گیری باشد.
دیتا + پروسس (Processing) + تحلیل + معنی = معلومات
درصورت که دیتا پروسس نشود در این صورت بازهم این دیتا یک معلومات نیست بلکه دیتایی ناقص است.
فقط "دیتا + معنی = معلومات" → ناقص است

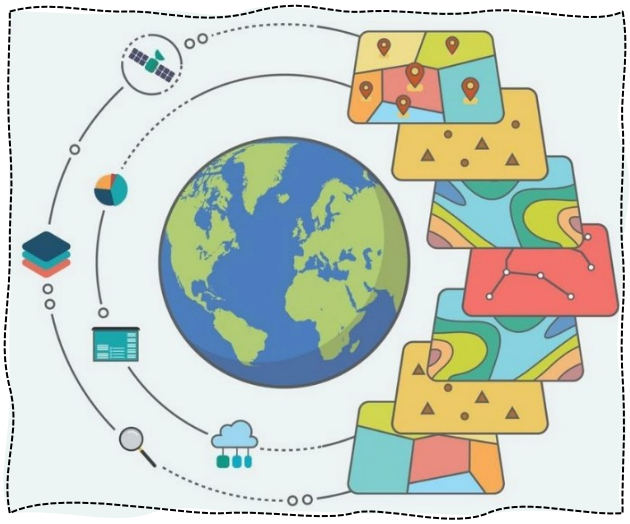
4. مثال واقعی

فرض کنید شما:

- در گوگل جستجو می‌کنید: "هیدفون گمینگ " یا پایه‌ای دوربین
- وارد یک سایت می‌شوید
- چند انواع **هیدفون** و **پایه‌ای دوربین** را می‌بینید

این‌ها همه دیتا است:

- کلمه جستجو
- زمان جستجو
- نوع محصول



نکته

وقتی ما در مورد دیتا صحبت می‌کنیم، این دیتا می‌تواند در اطراف و محیط ما وجود داشته باشد و ما بارها آن را با چشم دیده یا با گوش شنیده باشیم. اگر به این دیتا ضرورت نداشته باشیم، ممکن است بی‌اهمیت به نظر برسد. اما نکته مهم این است که اهمیت دیتا بسیار زیاد مهم است. بعضی موارد دیتا وجود دارد ولی ما هرگز به آن نیاز نداریم و به همین دلیل به آن دیتاهای کم‌اهمیت گفته می‌شود که در اینترنت و طبیعت به وفور یافت می‌شود.

5. انواع دیتا

- دیتای عددی(Quantitative)
  - عددی است
  - مثال: سن، نمره، قیمت
  -
- دیتای توصیفی(Qualitative)
  - توضیحی است
  - مثال: رنگ، نظر، احساس

6. نکات مهم در مورد دیتا:

اگر دیتا درست استفاده نشود:

- ممکن است حریم شخصی نقض شود
- امکان هک وجود دارد
- ممکن است افراد فریب داده شوند

جدول مقایسه دیتا و معلومات

موضوع	دیتا (Data)	معلومات (Information)
تعریف	معلومات خام و ابتدایی	دیتای پردازش‌شده و معنی‌دار
معنی	ندارد یا کم است	واضح و قابل فهم است
حالت	نامنظم	منظم
استفاده	مستقیم قابل استفاده نیست	برای تصمیم‌گیری استفاده می‌شود
مثال	25، کابل، احمد	احمد 25 ساله در کابل زندگی می‌کند

برای برَّسی بیشتر دیتا و معلومات به چینل های یوتیوب:

- Crash Course
- BBC Bitesize
- Techquickie

سوال چالشی؟

فرض کنید شما از موبایل خود استفاده می‌کنید و کارهای ذیل را انجام می‌دهید: جستجوی "کفش ورزشی"، دیدن ویدیوهای فوتبال و خرید آنلاین.
توضیح دهید که:

1. کدام بخش‌ها دیتا محسوب می‌شود؟
2. این دیتا چگونه به اطلاعات تبدیل می‌شود؟
3. این اطلاعات چگونه می‌تواند در ارسال تبلیغات هدفمند برای شما استفاده شود؟

جواب:

دیتا عبارت از معلومات خام مانند اعداد، متن یا تصاویر است که به تنهایی معنی واضح ندارد. زمانی که دیتا تحلیل، پروسس و تنظیم شود، تبدیل به اطلاعات می‌شود. به طور مثال، وقتی من از موبایل خود استفاده می‌کنم، معلوماتی مانند مکان و جستجوهای من ثبت می‌شود که این‌ها دیتا هستند. وقتی این دیتاها تحلیل شود، شرکت‌ها می‌توانند علایق مرا تشخیص داده و تبلیغات مناسب ارسال کنند.

2.1 تشریح انواع مواد دیجیتلی (Digital Material)

تعریف مواد دیجیتلی

مواد دیجیتلی عبارت اند از هر نوع محتوا یا معلوماتی که به شکل دیجیتلی ذخیره، استفاده و یا انتقال داده می‌شود. یعنی هر چیزی که در کمپیوتر، موبایل یا اینترنت دیده، شنیده یا استفاده می‌کنیم.
مواد دیجیتلی می‌تواند به شکل‌های مختلف باشد، مثل:

- نوشته ها (Documents)
- تصویر
- صدا
- ویدیو

این مواد در بخش‌های مختلف زندگی مانند تعلیم، تجارت، ارتباطات و سرگرمی استفاده می‌شوند.

انواع مواد دیجیتلی با مثال و توضیح

1. اسناد دیجیتلی(Digitally Stored Documents)

فایل‌هایی که به شکل دیجیتلی ذخیره می‌شوند

مثال:

- Word (مکتوب‌ها)
- PDF (کتاب‌ها)
- Excel (جدول ها)

کاربرد:

- نوشتن اسناد
- نگهداری معلومات
- استفاده در مکاتب و دفاتر

انواع مواد دیجیتلی

2. تصاویر(Photographs)

عکس‌هایی که با موبایل یا کمره گرفته می‌شود

مثال:

- عکس‌های شخصی
- عکس‌های خبری
- عکس‌های درسی

کاربرد:

- اشتراک‌گذاری در شبکه‌های اجتماعی
- استفاده در تعلیم
- ثبت خاطرات

3. پادکست‌ها (Podcasts)

فایل‌های صوتی که می‌توانیم آنرا گوش داد در انواع دستگاه دیجیتلی گوش داد.

مثال:

- برنامه‌های آموزشی

- داستان‌ها
- اخبار صوتی
- کتابهای صوتی

کاربرد:

- یادگیری بدون خواندن
- استفاده در موبایل هنگام سفر
- یکی از روشهای مدرن مطالعه

پادکســـت‌ها اخیراً در میان تولیدکنندگان محتوا در فضــازی مجازی طرفداران زیاد پیدا کرده است. **تماشا کنید!**

نکته

پادکست‌ها معمولاً به شکل صوتی نشر می‌شوند، اما در برخی موارد می‌توانند به شکل ویدیویی نیز ارائه گردند. پادکست‌های ویدیویی علاوه بر صدا، شامل تصویر نیز هستند و در بعضی حالات ممکن است مدت زمان آن‌ها نسبت به پادکست‌های صوتی کوتاه‌تر باشد. امروزه بسیاری از پادکست‌ها به هر دو شکل صوتی و تصویری در دسترس قرار دارند. به عنوان مثال، می‌توان به چینل‌های یوتیوب اشاره کرد که پادکست‌ها را به صورت ویدیو نشر می‌کنند و کاربران می‌توانند همزمان صدا و تصویر را مشاهده نمایند.

4. بلاگ، ولاگ و ویکی (Blogs, Vlogs, Wikis)

ولاگها

وبلاگها

ویکها

پاکستها

- **بلاگ(Blog)**

نوشته‌های آنلاین

مثال:

- مقالات آموزشی
- تجربیات شخصی

- **ولاگ(Vlog)**

ویدیو بلاگ

مثال:

- ویدیوهای یوتیوب
- آموزش‌های تصویری

- **ویکی(Wiki)**

سایت‌هایی که معلومات عمومی دارند:

مثال:

- ویکی‌پدیا

کاربرد:

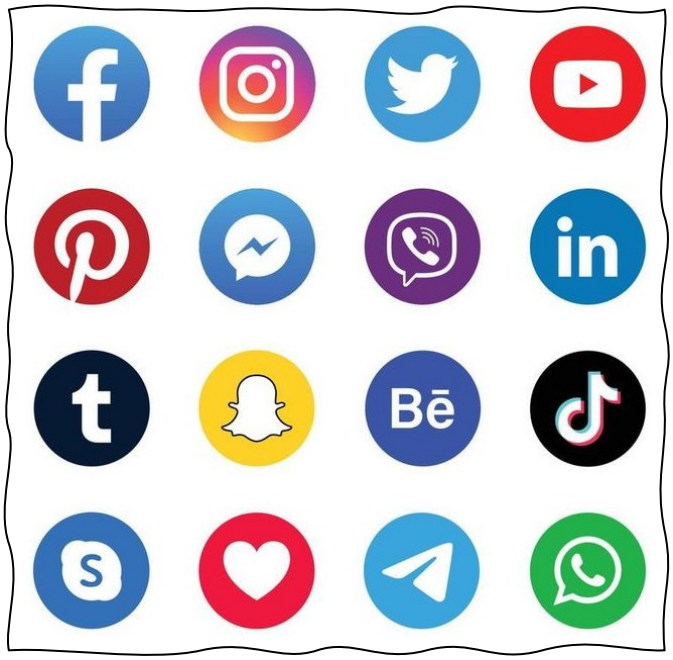
- جستجوی معلومات
- یادگیری موضوعات مختلف

5. شبکه‌های اجتماعی(Social Media)

پلتفورم‌هایی برای ارتباط با دیگران (دوستان، اقوام، همکاران، والدین...)

مثال:

- فیسبوک
- واتساپ
- اینستاگرام
- تلگرام
- توییتر (ایکس)
- ویچت (WeChat)
- لینکداین (LinkedIn)
- تیک‌تاک (TikTok)



کاربرد:

- ارتباط با دوستان
- اشتراک‌گذاری عکس و ویدیو
- دریافت اخبار
- Reels
- سرگرمی
- تبلیغات محصولات

نکته

شبکه‌های اجتماعی علاوه بر این‌که وسیله ارتباطات هستند، مردم می‌توانند از این طریق کسب درآمد نیز داشته باشند. بعد از سال 2019 که کرونا شیوع پیدا کرد، مردم در سراسر دنیا بیشتر به فروشات آنلاین از طریق شبکه‌های اجتماعی روی آوردند. امروزه بسیاری از پلتفورم‌ها مانند فیسبوک، تیک‌تاک و یوتیوب قابلیت کسب درآمد از طریق بازدید و ویدیوها را فراهم کرده‌اند. این نشان می‌دهد که شبکه‌های اجتماعی از یک وسیله ارتباطی به یک منبع درآمد آنلاین تبدیل شده و مفهوم جدیدی پیدا کرده‌اند. بنابراین شبکه های اجتماعی محل تبادل معادلات انترنت شده است.

6. ایمیل (Email)

ارسال و دریافت پیام به شکل رسمی

مثال:

- Gmail
- Yahoo

کاربرد:

- ارسال مکتوب‌ها
- ارتباط رسمی
- ارسال فایل

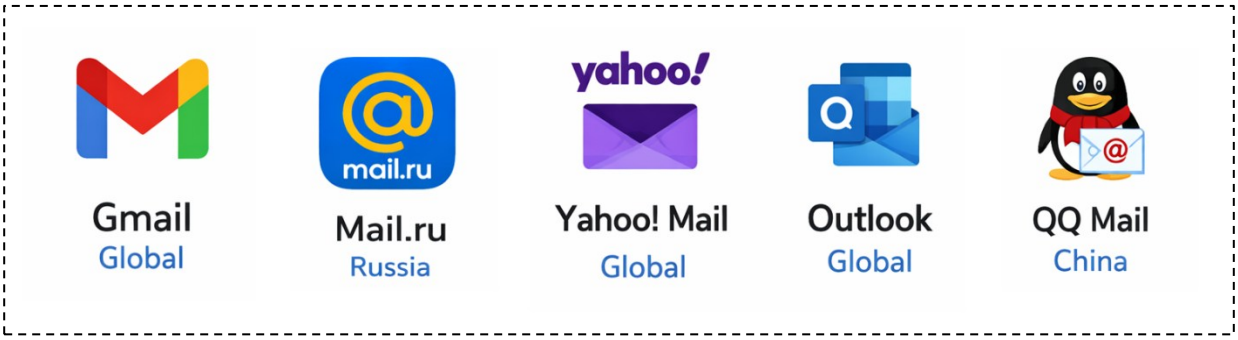
ایمیل‌ها یکی از قدیمی‌ترین و مهم‌ترین ابزارها برای تبادله پیام در عرصه‌های مختلف، به‌خصوص در سازمان‌ها و ارتباطات رسمی، می‌باشند. با وجود پیشرفت روزافزون تکنالوژی و به‌میان آمدن ابزارهای جدید ارتباطی مانند شبکه‌های اجتماعی و پیام‌رسان‌ها، ایمیل‌ها هنوز هم جایگاه خود را حفظ کرده‌اند و اهمیت آن‌ها کاهش نیافته است.

شرکت‌ها، دانشگاه‌ها، سازمان‌ها و ارگان‌های دولتی از ایمیل به عنوان یک وسیله رسمی برای ارسال و دریافت پیام‌ها، اسناد و معلومات استفاده می‌کنند. ایمیل‌ها امکان ارسال متن، فایل، تصاویر و سایر محتواها را به شکل منظم و قابل ثبت فراهم می‌سازند.

همچنان، ایمیل به دلیل داشتن ساختار رسمی، در مکاتبات اداری و مسلکی بسیار قابل اعتماد می‌باشد و می‌تواند به عنوان یک سند قابل مراجعه در آینده نگهداری شود.

دلایل محبوبیت و استفاده از ایمیل

1. **رسمی بودن**: مناسب برای مکاتبات اداری و رسمی
2. **قابل ذخیره بودن**: پیام‌ها قابل نگهداری و مراجعه مجدد هستند
3. **ارسال فایل**: امکان ارسال اسناد، عکس و فایل‌های مختلف
4. **امنیت نسبی**: نسبت به بسیاری از روش‌ها امن‌تر است
5. **دسترسی آسان**: در هر زمان و مکان قابل استفاده است
6. **ارتباط جهان**: امکان ارتباط با افراد در سراسر جهان
7. **ثبت و سندیت**: می‌تواند به عنوان مدرک رسمی استفاده شود



تصویر بالا لیست مشهورترین خدمات ایمیل رسانی در سراسر جهان میباشد. بعضی آنها در کشورهای خاص کاربرد دارد و بعضی آنها بصورت گسترده استفاده میشود.

پیام‌ها (SMS,MMS)

SMS[1]: پیام متنی کوتاه که شما خیلی زیاد آنرا دریافت میکند.

مثال:

- "سلام، کجایی؟"
- **از طرف مخابراتی:** شما 100 افغانی به حساب خود کریدیت علاوه نمودید!
- **یا:** شما 50% بسته انترنتی خود را مصرف نمودید!

MMS[2]**:** پیام همراه با تصویر، صدا یا ویدیو همراه میباشد.

مثال:

- ارسال عکس، ویدیو، صوت... در واتساپ، تلگرام، ایمو، فیسبوک...
- ارسال عکس، ویدیو، صوت، عکس در پیامک موبایل

کاربرد:

- ارتباط سریع
- ارسال فایل‌های کوچک

به‌صورت معمول، این خدمات در سیمکارت‌های شبکه‌های مخابراتی افغانستان به‌گونه پیش‌فرض فعال نمی‌باشد. در صورتی که فعال باشد، هزینه ارسال این نوع پیام‌ها با پیام‌های SMS (پیام کوتاه) تفاوت دارد. این هزینه ثابت نبوده و نظر به پالیسی هر شبکه مخابراتی متفاوت می‌باشد.

نکته: MMS بدو طریقه انجام میشود انترنت و کریدیت موبایل که در حساب سیمکارت خود دارید. از طریق انترنت این پیام از طریق اپلیکشن های مانند: WhatsApp, Telegram وغیره برنامه پیام رسان میتوانید انجام دهید.

سوال چالشی:

مواد دیجیتلی چیست و انواع آن را با ذکر حداقل سه مثال از زندگی روزمره توضیح دهید؟

جواب:

مواد دیجیتلی عبارت از محتواهایی است که به شکل دیجیتلی ذخیره و استفاده می‌شود. انواع آن شامل اسناد دیجیتلی، تصاویر، پادکست‌ها، بلاگ‌ها، ولاگ‌ها، ویکی‌ها، شبکه‌های اجتماعی، ایمیل و پیام‌ها می‌باشد. به طور مثال، یک فایل PDF یک سند دیجیتلی است، عکس‌ها نوعی تصویر هستند و واتساپ یک شبکه اجتماعی است که برای ارتباط استفاده می‌شود.

---

[1] **SMS** (Short Message Service)

[2] **MMS** (Multimedia Messaging Service)

3.1 مفهوم جمع‌آوری مواد دیجیتلی(Digital Data Capture)

مواد دیجیتلی یعنی هر نوع **دیتا** که به شکل دیجیتلی ذخیره می‌شود (مثل تصویر، ویدیو، متن، موقعیت مکانی و...).
این دیتا معمولاً به دو روش جمع‌آوری می‌شود:

1. **خودکار** → **(Automatic)** توسط سیستم‌ها و دستگاه‌ها بدون دخالت انسان
2. **دستی** → **(Manual)** توسط انسان (مثل تایپ کردن یا وارد کردن دیتا)

نکته مهم:
امروزه بیشتر دیتاها **از راه دور (Remote)** یا **به‌صورت خودکار** جمع‌آوری می‌شوند.

مثال‌های مهم از جمع‌آوری خودکار دیتا

1. کمره‌های ترافیکی (ANPR[1], Speed Camera):

- **ANPR** = تشخیص نمبر پلیت موترها
- این کمره‌ها:
  - نمبر موتر را ثبت می‌کنند
  - سرعت موتر را اندازه می‌گیرند

استفاده‌ها:

- جریمه سرعت
- امنیت جاده‌ها

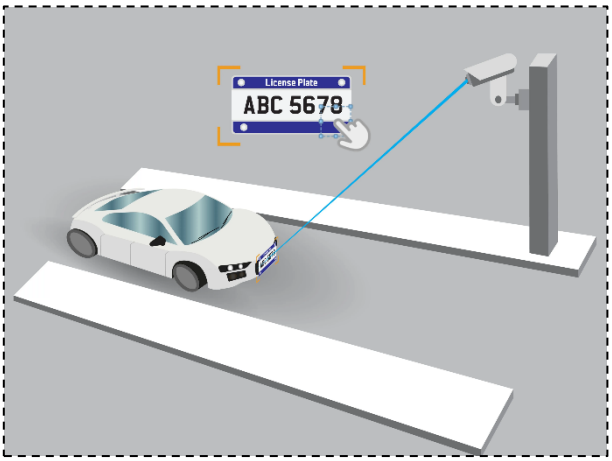
مزایا:

- دقیق و سریع
- بدون نیاز به انسان

معایب :

- نگرانی‌های حریم خصوصی
- هزینه نصب بالا

Automatic Number Plate Recognition (ANPR)



جریان اسکن پلیت موترها توسط دوربین های ANPR در سرکها در عین رفتار

2. سیستم‌های فروش (EPOS)

EPOS[2] = سیستم فروش در فروشگاه‌ها

چگونه کار می‌کند؟

- اسکن Barcode یا QR Code
- دیتاهای محصول ثبت می‌شود:
  - قیمت

[1] Automatic Number Plate Recognition (**ANPR**)

[2] Electronic Point of Sale (**EPOS**)

- تعداد
- زمان خرید

مزایا:

- سریع و دقیق
- کاهش اشتباه انسانی

معایب:

- وابسته به برق و سیستم
- در صورت خرابی، کار متوقف می‌شود

Electronic Point of Sale (EPOS)

3. دیتاهای موبایل (Mobile Data Tracking)

- وقتی موبایل روشن است:
  - بین دکل‌های مخابراتی (Mast) جابجا می‌شود

سیستم‌ها می‌توانند:

- موقعیت تقریبی شما را مشخص کنند

کاربردها:

- تماس و انترنت
- پیدا کردن موقعیت افراد

نکته:

این نوع دیتاها پیوسته و خودکار جمع‌آوری می‌شوند.

SATNAV برای موترها، تکسی ها

4. سیستم GPS و SATNAV

GPS = سیستم موقعیت‌یابی ماهواره‌ای

کاربرد:

- نقشه‌ها(Google Maps)
- پیدا کردن مسیر
- تعقیب وسایل نقلیه

مزایا:

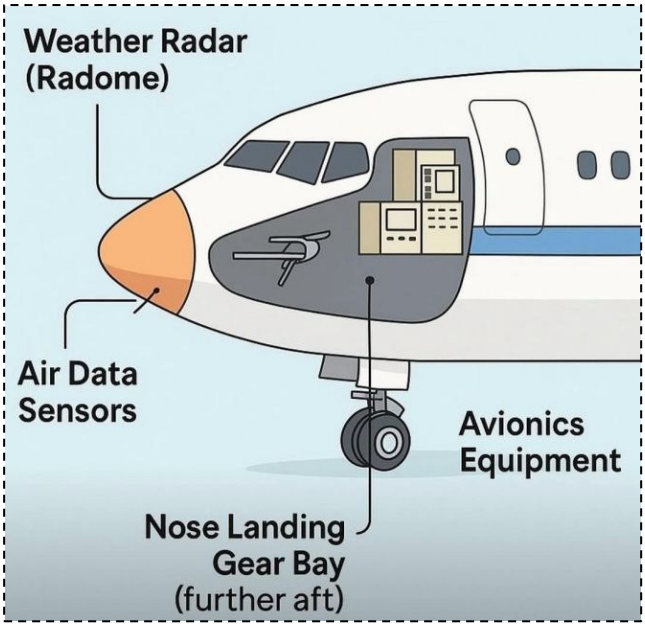
- بسیار دقیق
- کمک به مسیریابی

معایب :

- نیاز به سیگنال ماهواره
- مصرف باتری

Global Positioning System (GPS)

5. سنسورها و دیتالاگرها در طیاره‌ها



Nose-cone Airplane Sensors

در قسمت جلوی طیاره:(Nose-cone)
سنسورها این دیتاها را جمع‌آوری می‌کنند:

- دما
- فشار هوا
- سرعت باد

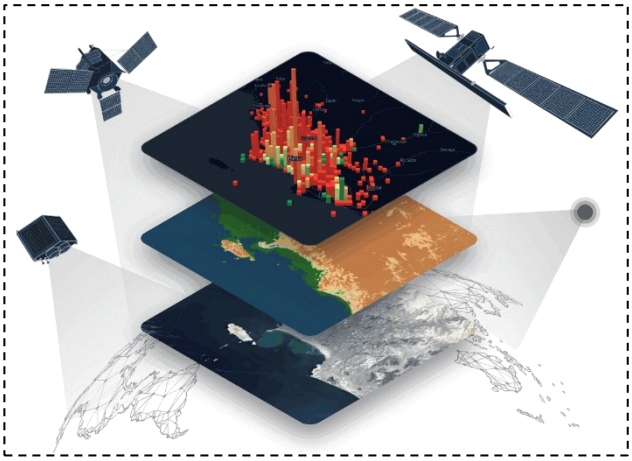
استفاده:

- پیش‌بینی هوا
- ایمنی پرواز

دقیقاً در قسمت نوک طیاره ها سنسور برای جمع آوری وضعیت جوی سرعت باد... جاسازی شده که اطلاعات مربوط را جمع آوری و به خلبان ها اطلاع داده شود. وقت آن قسمت نارنجی را باز نمایید با یک بخش تجهیزات پیشرفته روبرو میشویم که شما سنسورهای:

- **Weather Radar:** تشخیص طوفان و بارندگی در مسیر پرواز
- **Air Data Sensors:** اندازه‌گیری سرعت و ارتفاع طیاره
- **Angle of Attack (AoA) Sensors:** جلوگیری از سقوط ناگهانی (Stall).
- **Landing Guidance Antennas:** راهنمایی برای فرود دقیق در میدان هوایی
- **Lightning Diverter Strips:** محافظت در برابر رعد و برق

6. دیتاهای ماهواره‌ای (Satellite Data)



ماهواره‌ای جمع آوری دیتا

ماهواره‌ها انواع مختلف دیتا جمع می‌کنند:

- IR (Infrared) حرارت
- UV (Ultraviolet) اشعه
- Visible تصاویر معمولی

کاربردها:

- پیش‌بینی هوا
- نقشه‌برداری
- نظارت و امنیت

جمع‌آوری دیتا خودکار در مقایسه دیتای دستی دیتا

ویژگی	(Automatic) خودکار	(Manual) دستی
سرعت	بسیار سریع	کند
دقت	بالا	احتمال خطا
هزینه	بالا در شروع	کم
نیاز به انسان	کم	زیاد
انعطاف‌پذیری	کم	زیاد

مزایا و معایب کلی

مزایای جمع‌آوری خودکار دیتا:

- سرعت بالا
- دقت زیاد
- ذخیره‌سازی پیوسته
- کاهش خطای انسانی

معایب:

- هزینه اولیه بالا
- مشکلات حریم خصوصی
- وابستگی به تکنالوژی

سوال چالشی:

فرض کنید در یک شهر، تمام سیستم‌های جمع‌آوری دیتا خودکار) مثل کمره‌های ترافیکی، GPS و سیستم‌های فروش (به‌طور کامل فعال هستند.
به نظر شما، اگر این سیستم‌ها حذف شوند و همه چیز به‌صورت دستی انجام شود:
چه مشکلاتی به‌وجود می‌آید و آیا می‌توان همان سطح دقت و سرعت را حفظ کرد؟ توضیح دهید.

جواب:

اگر سیستم‌های خودکار حذف شوند و جمع‌آوری دیتا به‌صورت دستی انجام شود:

مشکلات:

- سرعت کار بسیار کاهش می‌یابد
- احتمال اشتباه انسانی زیاد می‌شود
- نیاز به نیروی انسانی بیشتر خواهد بود
- ثبت و ذخیره دیتا به‌صورت منظم دشوار می‌شود
- خدماتی مانند مسیریابی (GPS) یا کنترل ترافیک مختل می‌شود

نتیجه:
خیر، حفظ همان سطح **دقت و سرعت** ممکن نیست، زیرا سیستم‌های خودکار قادرند دیتا را به‌صورت سریع، دقیق و پیوسته جمع‌آوری کنند، در حالی‌که روش دستی محدود و خطاپذیر است.

4.1 مفهوم تبدیل دیتا به اطلاعات

دیتا:(Data)

- حقایق خام و بدون معنی
- مثال: اعداد، کلمات پراکنده، تصاویر بدون توضیح

اطلاعات:(Information)

- دیتای پردازش‌شده که معنی و مفهوم دارد
- مثال: گزارش، جدول تحلیل‌شده، متن منظم

نکته مهم:

تا زمانی که دیتا پردازش (Process) نشود و زمینه (Context) نداشته باشد، تقریباً بی‌فایده است.

1. چگونه دیتا به اطلاعات تبدیل می‌شود؟

مراحل ساده:

1. **جمع‌آوری دیتا**
2. **پردازش دیتا(Processing)**
3. **دادن زمینه(Context)**
4. **نمایش(Presentation)**

نتیجه:
دیتا → تبدیل به اطلاعات مفید و قابل درک می‌شود. این چهار مرحله بعضی وقت ها ما در زندگی روز مره خود بارها تکرار میکنم ولی مراحل آنرا از نظر علمی نمیدانیم.

2. نقش نرم‌افزارها در تبدیل دیتا به اطلاعات

نرم‌افزارها کمک می‌کنند تا دیتا:

- مرتب شود
- تحلیل شود
- به شکل قابل فهم نمایش داده شود

در ادامه انواع مهم نرم‌افزارها:

1.2 برنامه‌های پردازش اسناد (Document Processing)

شامل:

- Word Processor مانند: (Microsoft Word)
- Desktop Publisher
- سیستم‌های عددی: مثل (Excel)

چگونه دیتا را تبدیل می‌کنند؟

- متن خام → تبدیل به سند منظم
- اعداد → تبدیل به جدول و نمودار

مثال:

لیست نمرات دانش آموزان → تبدیل به گزارش منظم با جدول

آیکن برنامه مایکروسافت ورد

2.2 برنامه‌های ارائه(Presentation Applications)

برنامه‌های ارائه اطلاعات به ما کمک می‌کنند تا مفاهیم را به شکل ساده‌تر و قابل فهم‌تر به مخاطب منتقل کنیم. این برنامه‌ها موضوعات پیچیده را در قالب تصاویر، متن‌های جذاب و منظم ارائه می‌کنند و باعث می‌شوند درک موضوع برای بیننده آسان‌تر شود.

در نتیجه، بیننده می‌تواند یک تصویر واضح و کامل از موضوع در ذهن خود ایجاد کند و مطالب را بهتر یاد بگیرد.

برنامه‌هایی که در بخش ارائه مطالب استفاده می‌شوند عبارتند از:

مثل:

- Microsoft PowerPoint
- Google Slide
- Prezi

آیکن برنامه مایکروسافت PowerPoint

کارکرد این برنامه ها:

- ترکیب چند نوع دیتا:
  - متن
  - تصویر
  - صدا
  - ویدیو
  - اشکال
  - تصویرها سه بعدی
  - آیکن ها

نتیجه:

تبدیل دیتاها به یک **ارائه (Presentation)** قابل فهم و جذاب، می‌تواند مخاطبان را نسبت به موضوع آگاه ساخته و توجه آن‌ها را به‌خوبی جلب کند. این کار باعث می‌شود مفاهیم به شکل واضح‌تر منتقل شده و درک مطالب برای بیننده آسان‌تر گردد.

3.3 دیتابیس (Database Applications)

دیتابیس‌ها محل ذخیره‌سازی انبوه اطلاعات به‌صورت دیجیتالی هستند که دیتا را در قالب جدول‌ها سازمان‌دهی می‌کنند. مدیریت و کار با این دیتا معمولاً با استفاده از زبان SQL انجام می‌شود.

انواع:

- Flat Database
- Relational Database

آیکن دیتابیس

چگونه کار می‌کند؟

- ذخیره دیتا در جدول‌ها
- اجرای Query (جستجو)
- انجام محاسبات

مثال:

دیتای دانش آموزان → جستجو: "دانش آموزان کامیاب"
تبدیل به اطلاعات مفید

Flat Database نوعی دیتابیس است که تمام دیتا را در یک جدول یا فایل ذخیره می‌کند و بین اطلاعات هیچ ارتباط (Relation) پیچیده‌ای وجود ندارد.

ویژگی‌ها:

- ساختار ساده
- فقط یک جدول دارد
- مناسب برای اطلاعات کم و ساده

مثال:

نام	صنف	مکتب
Ali	10	مکتب خصوصی همای سعادت
Sara	9	مکتب خصوصی همای سعادت

همه دیتا در یک جدول ذخیره میشود بطور منظم و ساختار یافته میباشد. مشهورترین برنامه که در این زمینه استفاده میشود مایکروسافت اکسل (Microsoft Excel) و گوگل شیت (Google Spreadsheet) این دو برنامه ساختار مشابه هم دارند:

1. Microsoft Excel بصورت آنلاین و آفلاین
2. Google Spreadsheet فقط آنلاین در گوگل درایف کار میشود.

نکته: برنامه اکسل توسط شرکت مایکروسافت با قابلیت های خیلی زیاد و بینظیر در اختیار کاربران قرار میگیرد. اما برنامه گوگل شیت با امکانات محدود عرضه میشود.

Microsoft Excel

Google Spreadsheet

Relational Database (دیتابیس رابطه‌ای) نوعی دیتابیس پیشرفته است که دیتا را در چندین جدول جداگانه ذخیره می‌کند و بین آن‌ها ارتباط (Relation) برقرار می‌کند.

ویژگی‌ها:

- چندین جدول دارد
- ارتباط بین جدول‌ها (کلید اصلی و خارجی)
- مناسب برای سیستم‌های بزرگ

اطلاعات شخصی دانش آموز

ID	Name
1	Ali
2	Sara

جدول 1

اطلاعات تعلیمی دانش آموز

ID	Grade
1	10
2	9

جدول 2

به دو جدول بالا نگاه کنید:

- اطلاعات شخصی دانش آموز
- اطلاعات تعلیمی دانش آموز

هر دو در دو جدول جداگانه است اما توسط یک کلید (Foreign Key) دیتا هر دو جدول بهم به اشتراک گذاشته میشود.

دیتابیس های رابطه چند اپلیکشن مشهور و پرکاربرد دارد که در ذیل به آنها می پردازیم:

- MySQL

- Microsoft SQL Server
- Oracle Database

جدول مقایسه‌ای دیتابیس ساده و رابطه‌ای

Flat Database	Relational Database
یک جدول	چند جدول
ساده	پیشرفته
بدون ارتباط	دارای ارتباط
مناسب کارهای کوچک	مناسب سیستم‌های بزرگ

MySQL Database

SQL Server Database

Oracle Database

به یاد داشته باشید که دیتاهای تمام شرکت های بزرگ مانند:

- فیسبوک
- گوگل
- آمازون
- واتسپ
- Shopify
- انستاگرام
- یوتیوب
- تیک تاک
- لینکداین
- گیت هاپ
- وغیره

آیکن دیتابیس آنلاین Cloud

همه در این اپلیکشن های دیتابیس ذخیره شده و بصورت آنلاین در سراسر دنیا خدمات داده مجموعه‌ای انبوه دیتاعظیم در آنها میشود.

5.1 وب‌سایت‌ها (Website)

وب‌سایت‌ها یکی از پرمحتواترین منابع اطلاعاتی هستند که حجم زیادی از دیتاهای مفید را در اختیار کاربران قرار می‌دهند. این اطلاعات می‌تواند شامل گزارش‌های دسته‌بندی‌شده، دیتاهای خام، و یا دیتاهای نیمه‌پردازش‌شده و کاملاً پروسس‌شده باشد.
این نوع اطلاعات برای جمع‌آوری، تحلیل و آمارگیری بسیار مفید بوده و به کاربران کمک می‌کند تا درک بهتر و تصمیم‌گیری دقیق‌تری داشته باشند. این دیتاها بشکل در وب سایت ها قرار میگیرند که کابران با دیدن ساختار آنها متوجه منظور دسته بندی معلومات میشوند. معلومات آمیخته با تصاویر جدولها و کتکوری بنده شده نمایش داده میشود که کاربران به سادگی مفهوم و منظور نویسنده و دسته اطلاعات درک میکند.

کارکرد:

- نمایش دیتا به شکل قابل فهم برای کاربران

مثال:

یک سایت خبری:

- دیتا → اخبار خام
- اطلاعات → خبر تنظیم‌شده با عنوان و تصویر

ویکی پدیا[1]:

- یکی از نمونه های اطلاعات قالب بندی شده سایت ویکی پدیا است. مانند منابع،بیوگرافی، عناوین همه مرتب و منظم میباشد که خوانندان به آسانی میتواند اطلاعات را جمع آوری یا منظور نویسنده را درک کند.

وب سایت‌های خرید مانند: آمازون، شاپفای، علی بابا... وغیره همه اطلاعات منظم با ساختار که قابل فهم و دسته بندی شده دارند. این اطلاعات ساختارهای چون:

- تصاویر
- ویدیو
- متن ساده
- اعداد و سمبولها
- لینک ها
- جدول ها
- آیکن ها

ترکیب شدند و مفهوم خاص را برای مخاطب ارائه میدهد. اما وب سایتها میتواند کتگوریهای مختلف داشته باشند. وب سایت های که فقط ویدیو پخش میکند مانند: یوتیوب، آمازون پرایم، نتفلکس یا وب سایت که فقط موزیک پخش میکند مانند: ...Spotify, SoundCloud وب سایت های است که فقط تصاویر را منتشر میکند مانند: Pinterest, Freepik, Stock, Getty Image وغیره وب سایت ها.

[1] https://www.wikipedia.org

6.1 برنامه‌های ویدیو و تصویر(Video & Imaging)

در برنامه های ویدیویی مانند افترافکت After Effect, Primer Pro, DaVinci Resolve, CupCut وقت شما یک ویدیویی تبلیغاتی طراحی میکند مقدار زیاد از دیتاخام را ترکیب کرده و یک معلومات تولید میکند. مانند تبلیغات شرکت مخابراتی افغان بیسیم یا شرکت مخابراتی روشن که همه‌ای این تبلیغات از دیتاهای خام تشکیل شده با استفاده از موارد ذیل تبدیل به یک معلومات تأثیرگذار در ذهن مخاطب میگردد:

- ✓ صدا
- ✓ متن
- ✓ عکسها
- ✓ ویدیوها
- ✓ افکت های جذاب
- ✓ رنگها
- ✓ آیکن‌ها
- ✓ ایموجی ها
- ✓ Transitions حرکات ویژه

تمام این عناصر نقش اساسی در تبدیل دیتای خام به یک پیام مؤثر و قابل درک دارند. این روند باعث می‌شود که انتقال معلومات به شکل عمیق‌تر انجام شده و در ذهن مخاطب ماندگار گردد. علاوه بر این، طراحی (Design) و نحوه چیدمان (Layout) این عناصر نیز اهمیت بسیار زیاد دارد. اگر یک دیزاین بدون نقص بوده و ترکیب رنگ‌ها با هویت برند (Branding) شرکت هماهنگ و یک‌دست باشد، باعث می‌شود که مخاطب بیشتر درگیر شده و پیام تبلیغاتی را بهتر درک کرده و برای مدت طولانی‌تری در ذهن خود حفظ نماید.

DaVinci Resolve

Adobe After Effect

Adobe Premiere Pro

Cup Cut Pro

همچنان در برنامه‌های طراحی بنرها، پوسترها، کتاب‌ها و اعلان‌های در سرکها نصب می‌شود و اینترنتی مانند فتوشاپ(Photoshop) ، کانوا(Canva) ، ایلستراتور(Illustrator) ، کورل(CorelDRAW) ، فیگما (Figma)و سایر ابزارها، روند مشابهی وجود دارد.

در این برنامه‌ها نیز طراح، یک مجموعه بزرگ از دیتاهای خام را با هم ترکیب کرده و یک مفهوم مشخص و هدفمند ایجاد می‌کند. این دیتاهای خام می‌تواند از منابع مختلفی مانند:

✓ وب‌سایت‌ها
✓ کتاب‌ها
✓ تجربیات و گفته‌های افراد نخبه به‌دست آمده باشد.

تمام این موارد در ابتدا به‌عنوان «دیتای خام» شناخته می‌شوند؛ اما زمانی که توسط دیزاینر مورد پردازش(Processing) ، تحلیل (Analysis) و ترکیب اصولی قرار می‌گیرند، به «معلومات مفید و قابل استفاده» تبدیل می‌شوند.

در واقع، طراحی (Design) همان مرحله‌ای است که در آن دیتا معنا پیدا می‌کند و به شکلی منظم، زیبا و قابل درک برای مخاطب ارائه می‌گردد.

آیکن های برنامه دیزاین پسترها

این برنامه که در تصویر بالا آیکنهای آنها را مشاهده میکند از محبوبترین و پر استفاده ترین برنامه ها در سطح جهانی است که روزانه میلیون دیزاینر با آنها بیلیون پستر دیزاین میکند و امرار معاش میکنند.

نتیجه

تمام دیتاهای خام با استفاده از این برنامه ها دیزاین یعنی پروسس و تحلیل شده به معلومات تبدیل میشود.

7.1 مفهوم استفاده از مواد دیجیتلی برای اهداف مشخص

مواد دیجتیلی یا همان مواد خام وقت پروسس میشود و بدون شک که برای هدف خاص ترتیب داده شده است. لذا مواد دیجیتلی بدون هدف، مقصد هیچ مفهوم ندارد، باید هر مواد دیجیتلی یک مفهوم

خاص به مخاطب انتقال بدهد. در نتیجه گفته میتوانیم که: مواد دیجیتلی زمان ارزشمند است که برای مخاطر مفهوم خاص داشته باشند:

- برای یک **هدف مشخص (Purpose)** ساخته شوند.
- برای یک **مخاطب خاص (Target Audience)** مناسب باشند.

یعنی اینکه دیتا طوری نمایش و ترتیب داده شود که:

- قابل فهم باشد.
- نیاز مخاطب را برآورده کند.

در این صورت این مواد دیجیتلی ارزشمند و مفید میباشد.

1. اهداف مختلف استفاده از مواد دیجیتلی

مواد دیجیتلی می‌توانند برای اهداف مختلف استفاده شوند:

اطلاع‌رسانی(Inform)

- مثال: گزارش، خبر، وب‌سایت
- هدف: انتقال معلومات

آموزش(Educate)

- مثال: اسلاید درسی، ویدیوی آموزشی
- هدف: یاد دادن یک موضوع

تجاری(Business)

- مثال: تبلیغات، گزارش فروش
- هدف: افزایش فروش یا تصمیم‌گیری

قانع‌سازی(Persuade)

- مثال: کمپاین، تبلیغات
- هدف: تغییر نظر یا رفتار مردم

موارد بالا همه در سطح عمومی مواد دیجیتلی را تحت پوشش قرار میدهند. چون وقتی مواد دیجیتلی بین افراد تبادله میشود زیر چتر یکی از موارد بالا میباشد.

2. شناخت مخاطب (Target Audience)

قبل از تحلیل این موضوع سوال:
آیا تا هنوز فکر کرده‌اید وقت پیام در گروه واتسپ نشر میکند یا نشر میشود مخاطب کیست؟ منظور از نشر پیام چیست؟ پست در فیسبوک یا وب سایت نشر میکنید مقصد چیست؟
بدون شک که مخاطبین این پیام و یا پست مشخص میباشد. هیچ مواد دیجیتلی بدون مخاطب نیست و اگر هیچ مخاطب نداشته باشد این مواد دیجیتلی بی ارزش میباشد.

برای تولید مواد دیجیتلی موفق باید بدانیم:

Target Audience

مخاطب کیست؟

- دانش آموزان
- استادان
- مشتریان
- عموم مردم

چه چیزی مهم است؟

- سطح دانش (ساده یا پیشرفته)
- زبان (ساده یا تخصصی)
- سن و علاقه
- نیازهای مخاطب

مثال:

- برای دانش آموزان → ساده و تصویری
- برای مدیران → خلاصه و رسمی

استفاده از نرم‌افزارها (حداقل 3 مورد)

دانش آموزان باید کارکردن با سه مورد از ابزارهای که در بخش (4.1 مفهوم تبدیل دیتا به اطلاعات) گفته شد را عملی کار کنند و نحوه ترتیب اطلاعات را در این برنامه یاد داشته باشند. از جمله برنامه پروسس متن (Word) پریزنتیشن (Presentation) شیت (Excel) و وب سایت ها (Website) را باید کار کنند:

- Word Processing (Microsoft Word)
- Presentation (Microsoft PowerPoint)
- Spreadsheet (Microsoft Excel)
- Websites

1. Word Processing (Microsoft Word) برنامه مایکروسافت ورد

درکارهای عملی دانش آموز بتوانند:

- اطلاعات را بصورت درست در برنامه تنظم و نمایش بدهند
- تصاویر با متن ترکیب نموده ساختار سند منظم باشد
- Header, Footer مرتب و بدون نقض تنظیم شود
- رسم کردن اشکال، جدول و وارد کردن تصاویر
- فهرست بندی مطالب و اشکال

- بخش بندی مطالب
- ذخیره اسناد با فرمت های مختلف

پروژه:

ترتیب گزارش نتایج امتحان دانش آموزان، فهرست بندی مطالب در یک کتاب، ساخت سی وی

2. Presentation (Microsoft PowerPoint) برنامه مایکروسافت پاورپوینت

دانش آموزان بتوانند موارد ذیل را در برنامه PowerPoint کار کنند:

- ایجاد سلاید و تنظم متن، تصویر،ویدیو ها، اشکال از منابع مختلف بصورت منظم ترتیب و نمایش آنها
- اعمال کردن سلایدها و انیمشن ها
- ذخیره سازی سلایدها به فرمت های مختلف

پروژه:

ترتیب سلاید که در آن تصویر،آیکن ها، اشکال، ویدیو، متن ساده جدول استفاده شده باشد و همه طور تنظیم شده باشند که مخاطب حذب کند.

3. Spreadsheet (Microsoft Excel)

دانش آموزان کار کردن با برنامه اکسل را یادبگیرند ازجمله:

- ایجاد یک Worksheets
- تب های Home, Insert, Page Layout, Data, Formula با جزئیات کار کنند
- رابطه بین شیت ها مختلف و گزارش گیری آنها
- ترتیب اطلاعات و پاک سازی آنها
- ایجاد جدول اعلان نتایج دانش آموزان
- ایجاد جدول مصارف یک سازمان (مانند مواد غذایی بعضی موارد لوجستگی...)
- ذخیره سازی شیت ها با فرمت های مختلف

پروژه:

1- ترتیب جدول برای یک هوتل از اقامت مسافران در یک هفته، شامل اطاق، سفارشات غذایی و بعضی خدمات دیگر...

2- ترتیب جدول فروشات یک شرکت مواد شویند در طی سه روز اخیر شامل موارد:

1. مشخصات مشتری
2. محصولات که فروخته شده
3. ولایات که در آن فروش شده
4. مقدار فروشات محصولات
5. مبلغ دریافت و باقی مانده
6. تخفیف

بعضی موارد را خود دانش آموز میتواند به آن علاوه کند و یک گزارش کامل از آن ارائه کند.

4. Website وب سایت (اختیاری)

دانش آموزان کار کردن با انواع وب سایت ها را یادبگیرند. از جمله:

1. شاخت انواع لینک در وب سایت
2. Header, Footer وب سایت را بشناسد
3. ذخیره تصاویر و دانلود ویدیوها
4. کپی کردن متن ها بصورت درست و پست کردن آن در برنامه های: ورد، پاورپوینت اکسل
5. ثبت نام کردن در وب سایت
6. آپلود کردن فایل ها
7. تفکیک وب سایت از نظر محتوا و مخاطب

پروژه:

دانش آموزان تمام مراحل که در بالا یاد شدند باید کار کنند و یک گزارش مکمل در مورد این مراحل بنویسند.

جدول مواد آموزش

شماره	موضوع	منبع آموزش
1	آموزش کامل ورد 2025	یوتیوب (ویدیوها)
2	آموزش کامل برنامه اکسل 2025	یوتیوب (ویدیوها)
3	آموزش کامل برنامه پاورپوینت 2025	یوتیوب (ویدیوها)
4	آموزش نحوه استفاده از وب سایت ها	یوتیوب (ویدیوها)

برای تمرین این برنامه، شما می‌توانید به یوتیوب (YouTube) مراجعه کرده و در باکس جستجو عبارت **MARP** را تایپ نمایید. سپس وارد اولین چینلی شوید که برای شما نمایش داده می‌شود و ویدیوهای مورد نظر خود را پیدا کرده و مشاهده نمایید.

همچنان، می‌توانید از طریق جدول بالا، روی گزینه «**ویدیوها**» با استفاده از موبایل یا کمپیوتر کلیک کنید تا تمام بخش‌های ویدیویی مربوطه به‌صورت کامل برای شما نمایش داده شود.

علاوه بر این، شما می‌توانید منابع بسیار زیادی را در یوتیوب در این زمینه پیدا کرده، تماشا نموده و با تمرین مداوم مهارت خود را تقویت کنید.

2. درک استفاده از معلومات دیجیتلی برای اهداف مختلف

مواد دیجیتلی (Digital Information) می‌تواند برای اهداف مختلف استفاده شود. این مواد می‌تواند به اشکال گوناگون به مخاطبان منتقل گردد، مانند: تصاویر، ویدیوها، کتاب‌های(PDF) ، مقالاتی که در ژورنال‌ها نشر می‌شوند، درام‌ها و قصه‌های کوتاه، داستان‌ها و خاطرات در قالب برنامه‌های مختلف، و حتی به شکل صوتی. در عصر حاضر، نشر و انتشار مواد دیجیتلی به‌طور چشم‌گیری افزایش یافته و با سرعت بسیار بالا انجام می‌شود.
از آن جمله به چند نکته مهم میشود مرتب به این موضوع پرداخت:

2.1 انتقال مفکوره‌ها به مخاطبین گسترده(Communicate Ideas)

هدف:
رساندن پیام یا مفکوره به تعداد زیاد مردم
ابزارها:

- وب‌سایت‌ها
- شبکه‌های اجتماعی
- ویدیوها
- پریزنتیشن‌ها
- کانفرانس ها
- جلسات آنلاین
- پلتفرم های صوتی (پاکستها)

مثال:

- یک ویدیوی آموزشی در مورد محیط زیست، تأثیرات هوش مصنوعی
- یک پُست فیسبوک درباره اهمیت آموزش

نتیجه:
یک پیام به هزاران یا میلیون‌ها نفر منتقل می‌شود و برای سالها تأثیر گذار و نسلهای زیادی آگاه میشود.

2. مدل‌سازی و پیش‌بینی نتایج(Model & Predict Outcomes)

هدف:
استفاده از دیتا برای پیش‌بینی آینده یا بررسی سناریوها مختلف و تصمیم‌گیری در مورد عواقب و یا جلوگیری از فاجعه‌ها و برعلاوه بررسی نتایج موفقیت ها
ابزارها:

- Excel
- نرم‌افزارهای تحلیل داده (Tableau , Power BI)

مثال:

- پیش‌بینی نتایج امتحان دانش آموزان

- پیش‌بینی فروش یک شرکت در ماه آینده
- پیش بینی وضعیت خشکسالی به اساس دیتاها و آمار بارندگی های سه ماه اخیر
- بررسی پاکی شهر به اساس بررسی ها شاروالی شهر و میزان آلودگی هوا

چگونه این دیتا جمع آوری میشود؟

- وارد کردن دیتا
- استفاده از فرمول‌ها و نمودارها
- تحلیل نتایج
- ارزیابی و جمع آوری دیتا از بخش های مختلف
- رأی گیری و نظرسنجی ها
- جمع آوری انتقادات و پیشنهادات...

3. ارائه مدرک در تحقیقات(Provide Proof)

هدف:

اثبات یک موضوع با استفاده از دیتا

ابزارها:

- گزارش‌ها میدانی (مستندات)
- تصاویر
- ویدیوها
- دیتابیس‌ها
- مخشصات مکانها و نقشه ها ماهواره‌ای

مثال:

- استفاده از عکس برای اثبات یک حادثه مانند: سیلاب، زلزله طوفانهای شدید
- استفاده از آمار برای اثبات یک تحقیق مانند: جمع آوری اطلاعات و میزان خسارات از قریه جات و شهرهای که آسیب دیده و یا در بیماریهای شیوه یافته از بین رفتند.

نتیجه:

دیتا به‌عنوان **مدرک (Evidence)** استفاده می‌شود و برای جلوگیری و کمک رساندن به آسیب دیده گان اقدامات مناسب و از واقع های بعدی جلوگیری صورت میگیرد.

معلومات اضافی

1. تحلیل و بررسی مواد دیجیتلی

دانش آموزان نظر به اطلاعات در (درک استفاده از معلومات دیجیتلی برای اهداف مختلف) داده شد، یک نمونه اطلاعات جمع آوری کند از منابع مختلف مانند:

1. جمع آوری نمونه ها:
از منابع مختلف مثل:

- اینترنت
- رسانه‌ها
- تبلیغات
- وب‌سایت‌های دولتی
- نظرسنجی ها و افراد حاضر در محل اطلاعات

2. تحلیل (Reflection) انجام دهد
برای هر نمونه باید این سوال‌ها را پاسخ دهد:

- چرا این ماده ساخته شده؟
- هدف آن چیست؟
- برای چه مخاطبی است؟
- آیا موفق بوده یا نه؟

2. انواع نمونه‌ها

1. مواد برای قانع‌سازی(Persuasion)

تشویق مردم به خرید یا انجام یک کار بطور نمونه: نهال شانی در فصل بهار بخاطر سرسبزی شهر و جلوگیری از آلودگی هوا توزیع رایگان نهال های باردار و بی بار در سطح شهر و تشویق مردم بخاطر نگهداری و آبیاری مداویم آن.

هدف:
تشویق مردم به خرید یا انجام یک کار به نحوی وادار کردن به انجام کاری!

مثال:

- تبلیغ یک موبایل جدید
- اعلان تخفیف فروشگاه
- ثبت نام کارهای رضاکارانه در قابل بورسیه‌های رایگان
- ... وغیره

تحلیل:

- هدف: فروش محصول، بدست نتایج مطلوب
- مخاطب: مشتریان، شهروندان
- روش: استفاده از تصویر جذاب و متن قوی، معافیت از فیس دوره های تحصیلی

2. معلومات دولتی(Government Information)

اطلاعات دولتی شامل تمام آمارها و معلوماتی است که در مورد بخش‌های مختلف و موضوعات مهم و حساس یک کشور جمع‌آوری و نشر می‌شود. این معلومات می‌تواند شامل موارد ذیل باشد: آمار مبتلایان به ویروس کرونا، سرطان و بیماری توبرکلوز، سطح سواد مردم، میزان گرسنگی، درآمد سالانه، میزان بیکاری، واردات دوا و سایر موارد.
این نوع معلومات معمولاً به‌صورت منظم و دسته‌بندی‌شده ارائه می‌گردد و به محققین کمک می‌کند تا تحلیل‌ها و گزارش‌های دقیق‌تری تهیه نمایند. به همین دلیل، آمار و معلومات دولتی از اهمیت بسیار بالایی برخوردار است. البته اعتبار این معلومات تا حد زیادی به میزان شفافیت و دقت در همان کشور بستگی دارد. بطور مثال اگر یک نمونه را بررسی کنیم:

هدف:

آگاهی‌دهی یا هشدار به شهروندان همان کشور

مثال:

- کمپاین: استفاده نکردن از موبایل هنگام رانندگی
- اعلان‌های صحی

تحلیل:

- هدف: جلوگیری از خطر
- مخاطب: رانندگان
- روش: پیام واضح و هشداردهنده

3. مواد آموزشی

بصورت ویژه تقسیم اوقات، جزوه‌های درسی، سلایدها، کتابها، رهنمودها امتحانات همه را اگر ببنیم یک هدف ویژه دارد که آنها جامعه دانش آموزان میباشد.

هدف:

یاد دادن یک موضوع به دانش آموزان

مثال:

- ویدیوی آموزشی
- اسلاید درسی

تحلیل:

- هدف: آموزش
- مخاطب: دانش آموزان
- روش: توضیح ساده + تصویر

4. گزارش‌ها و تحقیقات

گزارشها

هدف:

ارائه معلومات دقیق و مستند

مثال:

- گزارش نتایج امتحان
- تحقیق علمی

تحلیل:

- هدف: اطلاع‌رسانی و اثبات
- مخاطب: مدیران یا استادان

5. اهمیت جمع‌آوری مثال‌های بیشتر

دانش آموزان مثالهای را با دقت مطالعه نموده و مثالهای بیشتر یاد داشت کند و تحلیل نمایند.

- مثال‌های بیشتری جمع کند
- تحلیل دقیق‌تر انجام دهد
- درک آنها عمیق‌تر می‌شود.

فعالیت عملی

فعالیت:

1. **سه نمونه پیدا کنید:**
   - یک تبلیغ
   - یک پیام دولتی
   - یک محتوای آموزشی
2. **برای هر کدام بنویسید:**
   - هدف چیست؟
   - مخاطب کیست؟
   - آیا موفق است؟ چرا؟

1.2 تأثیر معلومات دیجیتلی بر نتایج و برنامه‌ریزی

1. **مفهوم اساسی**

معلومات دیجیتلی فقط محتوا نیست، بلکه:

نحوه ذخیره شدن آن (File Type) تعیین می‌کند که:

- چگونه استفاده شود

- توسط چه نرم‌افزاری باز شود
- چقدر قابل تغییر یا اشتراک گذاری باشند.

نتیجه:

نوع فایل می‌تواند روی **تصمیم‌گیری، تحلیل و نتایج نهایی** تأثیر مستقیم داشته باشد. چون وقت فایل ها ذخیره میشود میتواند دیتابیس باشد و ممکن تصویر یا متنی باشد در این صورت تمام اقدام بعدی بستگی به نوعیت فایلها دارند.

2. چرا نوع فایل مهم است؟

مثال ساده:

- اگر گزارش به شکل PDF باشد → فقط خوانده می‌شود
- اگر همان گزارش به شکل Word باشد → هم خوانده میشود و هم قابل ویرایش است

پس:

نوع فایل = نوع استفاده

انواع فایل ها در جدول

دسته	نوع فایل	کاربرد
اسناد	.docx, .odt, .pdf, .txt, .rtf, .epub	نوشتن گزارش و متن
دیتا عددی	.xlsx, .ods, .csv	تحلیل اعداد و نمودار
ارائه	.pptx	ساخت پریزنتیشن
وب	.html, .htm, .xml, .php, .js	نشر در اینترنت
تصویر	.jpg, .png, .gif, .bmp, .svg	نمایش تصاویر
صدا	.mp3, .wav, mp4	فایل‌های صوتی
ویدیو	.MPEG, .MKV. AVI. . MOV .mp4, .3GP/3G2	ویدیوها
طراحی	.psd, .AI, . EPS, . TIFF	طراحی گرافیکی

دانش آموزان باید هر فرمت را با فایل واقعی کار کنند:

- ساخت یک فایل
- ذخیره با فرمت مربوطه
- دباره بازکرده و تغیر بیاورند و ذخیره کنند

3. مقایسه Open و Proprietary

نوع	مثال	مزایا	معایب
🔒 **Proprietary**	.docx, .xlsx	امکانات پیشرفته	نیاز به نرم‌افزار خاص
🌐 **Open**	.odt, .ods, .csv	رایگان و قابل استفاده در همه جا	امکانات محدود

4. تأثیر نوع فایل بر نتایج

نوع فایل	ویژگی	تأثیر بر نتیجه
Excel (.xlsx)	قابل تحلیل	تصمیم‌گیری دقیق
PDF	فقط خواندن	تحلیل محدود
JPG (کیفیت پایین)	جزئیات کم	احتمال اشتباه

5. انتخاب فایل مناسب (برای برنامه‌ریزی)

هدف	فایل مناسب
گزارش رسمی	PDF / Word
تحلیل دیتا	Excel
ارائه مطلب	PowerPoint
نشر آنلاین	HTML

2.2 نمایش معلومات دیجیتلی در چندین نرم‌افزار

فرض کنم ما یک لوگو داریم که در فوتوشاپ دیزاین میکنیم بعد در هر سند که میخواهم ترتیب بدهم لوگو را در بالایی صفحه برای مخاطبین نمایش میدهم. این روند نمایش معلومات دیجیتالی در چندین نرم افزار گفته میشود. یا جدول نمرات دانش آموزان میتواند در برنامه ها:

- ورد Word
- اکسل Excel
- پاورپوینت PowerPoint

نمایش داده شود و ما نتایج برای مخاطب مورد نظر نمایش داده میتوانیم.

1. تحلیل کلی موضوع

در دنیای دیجیتال، یک نوع دیتا می‌تواند:

- در **فرمت‌های مختلف** ذخیره شود
- در **نرم‌افزارهای مختلف** نمایش داده شود

- برای **مخاطبین مختلف** تغییر شکل دهد

یعنی:
یک دیتا ثابت، اما نمایش آن متفاوت است.
مثال ساده:
نمرات دانش آموزان:

- در Excel → جدول و نمودار
- در Word → گزارش
- در PowerPoint → اسلاید

هدف:
دانش آموزان بتواند یک دیتا را در چندین نرم افزار نمایش بدهند اما اشکال مختلف مفهوم یک چیز باشد. طوری باشد که ذهنیت مفهوم که در نرم افزار اولی بوده در دومی تغیر نکند و فقط نحوه نمایش آن تغیر کند.

2. استفاده از نرم‌افزارهای مختلف (مطابق بخش 1.4)
1.2 برنامه ورد Word

- نحوه ترتیب دیتا در برنامه
- دسته بندی و منظم بودن
- فهرست بندی مطالب به اساس عناوین مرتبط
- تشریح دیتا برای مخاطب قابل فهم

هدف: تشریحی و توضیح دیتا
مثال:

1. نوشتن گزارش نتایج امتحان
2. تحلیل عملکرد دانش آموزان در طول 9 ماه گذشته

2.2 برنامه اکسل:
گزارش که در برنامه ورد ترتیب شده است: حالا نتایج دانش آموزان در برنامه اکسل

- تحلیل
- محاسبه
- پیش بینی

هدف: نمایش دیتا بشکل جدول و نمودارها جذاب و قابل فهم
مثال:

- محاسبه میانگین نمرات
- رسم گراف پیشرفت دانش آموزان

PowerPoint 3.2 (پریزنتیشن)

در برنامه پاورپوینت به شکل پریزنتیشن نتایج دانش آموزان ارائه نموده با انمیشن و ترانزیشن قابل فهم ارائه میشود. یعنی دیتا طوری نمایش داده شود مقدار درک و جذب فهم موضوع نسبت به دو برنامه قبلی بیشتر باشد.

هدف:

ارائه معلومات به مخاطب

مثال:

- ارائه نتایج امتحان در صنف
- نمایش گراف‌ها و نکات مهم

Database 4.2 (دیتابیس)

برای ذخیره و جستجوی حجم زیاد دیتا شکل پیشرفته برنامه اکسل اما به امکانات وسیع تر و حرفه‌ای که میتواند باعث سرعت در جستجویی نمرات دانش آموزان شود.

هدف:

مدیریت و بازیابی دیتا

مثال:

- جستجوی دانش آموزان کامیاب
- مرتب‌سازی اطلاعات

5.2 وب سایت ها Websites

برای نشر معلومات به مخاطبین گسترده و یا بطور نمونه مثالهای قبلی: اعلان نتایج دانش آموزان بصورت وسیع یا خصوصی در اکوونت شخصی هر دانش آموز

هدف:

دسترسی عمومی به معلومات، دسترسی خصوصی

مثال:

- نشر نتایج در وب‌سایت
- نمایش اطلاعات آموزشی

Video / Image Applications 6.2 برنامه ایدیت ویدیو عکسها

برای جذاب‌تر ساختن معلومات، اعلانها و اطلاعیه یا معرفی مقام اول تا سوم دانش آموزان که بالاترین نمرات را در طول سال کسب کردند.

هدف:

ارائه بصری و تاثیرگذار، ماندگار

مثال:

- ویدیوی آموزشی
- تصویر گرافیکی (اعلان ها، پسترها تبلیغاتی)

3.2 کار با فرمت های مختلف فایلها (File Formats)

نوع فایل	کاربرد	نرم‌افزار
.docx	سند متنی	Word
.xlsx	دیتا عددی	Excel
.pptx	ارائه	PowerPoint
.html	وب	Browser
.jpg/.png	تصویر	Image Apps

4. کار با مخاطبین و اهداف مختلف

مخاطب	نوع نمایش مناسب
دانش آموزان	ساده + تصویر
استادان	دقیق + تحلیل
مدیران	خلاصه + نمودار
عموم مردم	واضح + جذاب

5. مفهوم Metadata

بعضی فایل‌ها (خصوصیات Proprietary) اطلاعات اضافی دارند که به آن Metadata گفته می‌شود.

Metadata یعنی:

اطلاعات درباره خود فایل، مثل:

- نام نویسنده
- تاریخ ایجاد
- تنظیمات فایل
- تاریخ انتشار
- رمزنگاری شده
- آخرین بار که تغیرات آورده شده کی بوده (Date Modified)

هدف:

درک اینکه چرا بعضی فایل‌ها:

- بزرگ‌تر هستند
- یا در نرم‌افزار دیگر درست کار نمی‌کنند

تأثیرMetadata

حالت	نتیجه
وجود Metadata زیاد	حجم فایل زیاد
انتقال به نرم‌افزار دیگر	ممکن است مشکل ایجاد شود

مثال:
یک فایلWord :
- در Word کامل باز می‌شود
- در نرم‌افزار دیگر ممکن است فونت یا ترتیب تغییر کند.

نوت:
به یاد داشته باشید که فونت طرح دیزاین و به نسخه نرم افزارها بستگی دارد قبل از بازکردن فایلها خود را مطمئن نمایید این فایل در نسخه فعلی این برنامه خراب نمیشود.

4.2 طراحی معلومات دیجیتلی برای استفاده در شرایط مختلف

وقتی ما یک دیتایی دیجیتلی ایجاد می‌کنیم (تصویر، سند، دیتا و...)، باید بدانیم: به چی مقصد و منظور طراحی میکنیم.

1. نوع طراحی و فرمت فایل (File Format) مستقیماً تعیین می‌کند:
- چگونه استفاده شود
- در کجا استفاده شود
- کیفیت آن چگونه باشد

یعنی:
انتخاب نادرست فایل → نتیجه ضعیف
انتخاب درست فایل → نتیجه حرفه‌ای

هدف:
دانش آموزان باید بتواند:
- نوع فایل مناسب را انتخاب کند
- درک کند که هر فرمت برای چه هدفی مناسب است
- تأثیر انتخاب خود را بر محصول نهایی توضیح دهد.

2. انتخاب نوع فایل در شرایط مختلف

2.1 طراحی لوگو (.png. vs .svg)

لوگو معمولاً در اندازه‌های مختلف استفاده می‌شود (کوچک و بزرگ)

هدف:
حفظ کیفیت در هر اندازه
مقایسه

نوع فایل	ویژگی	نتیجه
.svg	برداری(Vector)	کیفیت ثابت در هر اندازه
.png	پیکسلی(Raster)	با بزرگ شدن کیفیت کاهش می‌یابد

نوت:
برای استفاده در سطح وب فرمت SVG بهترین گزینه برای لوگوها میباشد است. اما برای نسخه های چاپی jpg. اما در صورت استفاده بصورت آفلاین لایه (png) باز باشد بهتر است.

2.2 تصاویر ویرایش‌شده (.jpg. vs .psd)
وقتی یک تصویر ویرایش می‌شود، لایه‌ها (Layers) مهم هستند. فایل که با پسوند psd ذخیره میشود میتوانیم بارها آنرا باز کرده و ویرایش کنیم. اما jpg لایه هایش بسته میشود قابل ویرایش نیستند.
هدف:
امکان ویرایش مجدد

مقایسه

نوع فایل	ویژگی	نتیجه
.psd	**دارای لایه‌ها**	**قابل ویرایش کامل**
.jpg	**فشرده و ساده**	**غیرقابل ویرایش دقیق**

برای کارهای طراحی → psd. مناسب‌تر است.

3.2 انتقال دیتا (.csv)
بعضی سیستم‌ها فقط فایل‌های ساده و قابل انتقال را قبول می‌کنند. این فرمت دقیقاً شبیه فایل اکسل است، اما به‌صورت گسترده توسط سیستم‌ها پشتیبانی می‌شود. اما اکسل به این اندازه پشتیبانی نمی‌شود، چون یک فرمت تجاری از محصولات مایکروسافت است. تعداد زیادی از سیستم‌ها فرمت اکسل (.xlsx) را قبول می‌کنند، اما به‌صورت عمومی پذیرفته نیست. لذا یکی از رایج‌ترین فرمت‌های دیتابیس در سطح وب، فرمت (.csv) می‌باشد.
هدف:
انتقال آسان دیتا بین سیستم‌ها

ویژگی‌ها:

نوع فایل	ویژگی	کاربرد
.csv	ساده و متنی	انتقال دیتا به دیتابیس
.xlsx	پیچیده‌تر	تحلیل و محاسبه

مثال:
لیست نام و رمز → تبدیل به → csv. انتقال به سیستم آنلاین

3. تأثیر طراحی بر محصول نهایی

انتخاب	نتیجه
انتخاب درست فایل	کیفیت بالا + استفاده آسان
انتخاب نادرست	مشکل در نمایش یا استفاده
عدم توجه به هدف	محصول غیرمؤثر

4. نکات مهم در طراحی معلومات دیجیتلی

همیشه قبل از ایجاد فایل فکر کنید:

- هدف چیست؟
- مخاطب کیست؟
- در کجا استفاده می‌شود؟

مثال:

- وب‌سایت → فایل سبک و سریع
- چاپ → کیفیت بالا
- ویرایش → فایل قابل تغییر

فعالیت عملی

تمرین:

برای هر مورد بهترین نوع فایل را انتخاب کنید:

انتخاب مناسب	حالت
.svg	طراحی لوگو
.jpg	عکس برای وب
.psd	فایل قابل ویرایش
.csv	انتقال دیتا

5.2 رابطه بین معلومات دیجیتلی که ایجاد می‌کنیم و نحوه استفاده آن

هر زمانی که شما یک معلومات دیجیتلی (دیتا) ایجاد می‌کنید (مثل: سند، جدول، تصویر یا ویدیو)، در واقع تعیین می‌کنید که:

این معلومات:

- چگونه استفاده شود
- توسط چه کسی استفاده شود
- در کجا استفاده شود

نکته بسیار مهم:

طریقه ایجاد معلومات دیجیتلی مستقیماً بر طریقه استفاده آن تأثیر می‌گذارد.

هدف:

دانش آموزان باید بتواند:

- معلومات دیجیتلی ایجاد کند
- آن را در چند نرم‌افزار استفاده کند
- توضیح دهد چرا آن نوع فایل یا نرم‌افزار را انتخاب کرده
- نشان دهد که چگونه این انتخاب‌ها بر نتیجه نهایی تأثیر گذاشته است!

تفسیرساده

اگر شما یک فایل را:

- درست طراحی کنید → استفاده آسان و موثر
- اشتباه طراحی کنید → استفاده مشکل و ضعیف

مثال ساده

حالت	نتیجه
نمرات درExcel	قابل تحلیل و نمودار
نمرات درPDF	فقط قابل دیدن
تصویر بی‌کیفیت	فهم دشوار
متن نامنظم	گیج‌کننده

کار عملی با نرم‌افزارها

1. Word (سند نوشتاری)

برای اسناد و الخصوص توضیح و تشریح معلومات استفاده می‌شود.

هدف:

ارائه معلومات به شکل رسمی، ساده و خصوصی

مثال:

یک دانش آموز نتایج امتحان را در Word می‌نویسد

رابطه:

اگر متن:

- منظم باشد → خواندن آسان
- نامنظم باشد → فهم مشکل

2. اکسل (Excel) دیتاها عددی

برای محاسبه و تحلیل دیتا

هدف:

تصمیم‌گیری دقیق

مثال:

- محاسبه میانگین نمرات
- ساخت نمودار پیشرفت

رابطه:

اگر فرمول اشتباه باشد → نتیجه غلط و بعضی وقت اصلاً کار نمیکند. فورمولهای اکسل بسیار حساس هستند باید دقیق با اسپیل همان لغت نوشته شود در غیر آنصور کار نمیکند.

برعلاوه برنامه ورد و اکسل ترتیب و منظم بودن اطلاعات در برنامه پاورپوینت و وب سایت نیز بسیار مهم است. اگر اطلاعات برای ارائه در برنامه پاورپوینت منظم نباشد مخاطب گیج و خسته میشود در نتیجه ارائه مفید نخواهد بود. همین در وب سایت ها اگر اطلاعات درست نمایش داده نشده باشد و چیدمان و فونت درست انتخاب نشده باشد و رنگ بدرستی ترکیب نشده باشند بننیدگان وب سایت افراد زیاد نخواهد بود.

کار با انواع فایل ها

نوع فایل	کاربرد	تأثیر در استفاده
.docx	نوشتن	قابل ویرایش
.pdf	نشر	فقط خواندن
.xlsx	تحلیل	محاسبه و نمودار
.csv	انتقال	ساده و سریع
.jpg/.png	تصویر	نمایش بصری
.mp4	ویدیو	آموزشی، تفریحی و تبلیغاتی

تأثیر مخاطب بر طراحی

طراحی دیتاها بستگی به طبقه‌بندی مخاطبان دارد، زیرا باید با سطح دانش و اولویت‌های هر طبقه همخوانی داشته باشد.

مخاطب	چگونه طراحی کنیم
دانش آموزان	ساده + تصویر
استادان	دقیق + تحلیل
مدیران	خلاصه + مهم

اشتباهات رایج

باید هنگام طراحی به نکات کوچک توجه داشته باشیم، مانند: مخاطب کیست؟ هدف چیست؟ نتیجه چیست؟ در ترکیب طراحی نیز به رنگ‌ها، اندازه فونت و ترکیب رنگ و اشکال توجه شود. هنگام ذخیره نمودن نیز باید در نظر داشته باشیم که فایل در کدام دستگاه نمایش داده می‌شود، زیرا بعضی دستگاه‌ها فقط از فرمت‌های خاص پشتیبانی می‌کنند. اگر شما اسلاید را با فرمت pptx. طراحی کنید اما دستگاه فقط PDF را نمایش دهد، در این صورت کار شما نادرست است. این موضوع در مورد ویدیوها، تصاویر و فایل‌های وب نیز صدق می‌کند.

3. تحلیل و ارزیابی کنترول مواد دیجیتلی

1.3 ارزیابی نیاز به کنترول استفاده از معلومات دیجیتلی

در عصر دیجیتال، هر فرد مقدار زیادی از **دیتا شخصی** خود را در دستگاه‌ها و اینترنت ذخیره می‌کند، مانند:

- نام و مشخصات
- شماره تماس
- حساب‌های شبکه‌های اجتماعی
- معلومات بانکی
- جستجو کردن در مرورگرها و اطلاعات از انترنت میگیرند

اگر این دیتا بدون کنترول باقی بماند:

- ممکن است دزدیده شود
- یا به‌صورت نادرست استفاده گردد

بنابراین:

کنترول معلومات دیجیتلی یک ضرورت بسیار مهم است، نه یک انتخاب. در سطح 1 ما دانستم که چطور وقت در دستگاه عمومی حساب کاربری خود باز میکنم از آن محافظت کنیم لذا از همین باید تمام نکات که قبلاً مطالعه نمودید را رعایت نمایید.

هدف

دانش آموزان باید بتواند:

- اهمیت محافظت از دیتا را درک کند
- روش‌های جلوگیری از سوءاستفاده را توضیح دهد
- در زندگی روزمره از این روش‌ها استفاده کند

روش‌های مهم برای محافظت از دیتا

1. استفاده از انتی‌ویروس (Antivirus)

توضیح:

انتی‌ویروس یک نرم‌افزار است که:

- ویروس‌ها و برنامه‌های خطرناک را شناسایی می‌کند
- از سیستم محافظت می‌کند

نکته مهم:

آنتی ویروس ها و سیستم باید **همیشه آپدیت (Updated)** باشد اگر آنتی‌ویروس به‌روز نشود، سیستم در برابر تهدیدات جدید آسیب‌پذیر می‌شود. دلیل آن این است که ویروس‌ها و بدافزارها نیز به‌طور مداوم در حال پیشرفت و هوشمندتر شدن هستند.

زمانی که یک ویروس جدید ظاهر می‌شود، علائم و رفتار آن در سیستم‌های مختلف شناسایی شده و توسط کاربران و متخصصان به شرکت‌های سازنده آنتی‌ویروس گزارش داده می‌شود. این شرکت‌ها با تحلیل این اطلاعات، نسخه‌های جدیدی از آنتی‌ویروس را منتشر می‌کنند تا بتوانند تهدیدات تازه را شناسایی و از بین ببرند. بنابراین، به‌روزرسانی منظم آنتی‌ویروس یک ضرورت اساسی در سیستم‌های

دیجیتال است و نقش مهمی در حفظ امنیت اطلاعات و جلوگیری از حملات سایبری دارد. لذا دانش آموزان ملزم هستند این نکات را رعایت نمایند.

2. استفاده از فایروال (Firewall)

فایروال مانند یک دیوار امنیتی عمل می‌کند که ورود و خروج داده‌ها و کاربران را در سیستم‌های دیجیتالی بررسی و کنترل می‌نماید. این ابزار از دسترسی افراد غیرمجاز به سیستم جلوگیری می‌کند و نقش مهمی در حفظ امنیت اطلاعات دارد. فایروال‌ها معمولاً به‌صورت پیش‌فرض در سیستم‌عامل‌هایی مانند Microsoft Windowsوجود دارند و به‌طور رایگان در اختیار کاربران قرار می‌گیرند. با این حال، این نوع فایروال‌ها ممکن است برای نیازهای ساده مناسب باشند، اما در برابر تهدیدات پیشرفته چندان قدرتمند نیستند.

در سازمان‌ها و نهادهایی که دیتاهای بسیار حساس و مهم دارند مانند: بانک‌ها یا ادارات دولتی استفاده از فایروال‌های پیشرفته و چندلایه ضروری است. این نوع فایروال‌ها امنیت بالاتری فراهم کرده و از اطلاعات حیاتی در برابر حملات سایبری محافظت می‌کنند.

3. استفاده از رمز قوی (Strong Password)

رمزعبور (Password) یکی از مهم‌ترین لایه‌های امنیتی در سیستم‌های دیجیتال است و معمولاً در کنار احراز هویت دو مرحله‌ای (2FA) استفاده می‌شود. اگر این لایه امنیتی به‌درستی تنظیم نشود، بدون شک راه برای نفوذ به سیستم فراهم می‌گردد.

بنابراین، یک رمزعبور باید حداقل ۸ کاراکتر یا بیشتر طول داشته باشند و ترکیبی از موارد زیر را شامل شود:

- حروف بزرگ(A–Z)
- حروف کوچک(a–z)
- اعداد(0–9)
- نمادها (! @ # $ % و غیره)

همچنین، بهتر است رمزعبور:

- قابل حدس نباشد (مثل نام یا تاریخ تولد نباشد)
- برای هر حساب متفاوت باشد
- به‌صورت منظم تغییر داده شود

در ادامه، مرور کوتاهی بر ویژگی‌های یک رمزعبور قوی خواهیم داشت تا بتوانیم امنیت حساب‌های خود را به‌طور مؤثر افزایش دهیم.

نکته مهم:

- استفاده از یک رمز برای همه حساب‌ها (کاراشتباه است)
- استفاده از رمزهای مختلف (کار درست است)
- رمزعبور فقط هویت شخصی حساب های دیجیتلی شماست نباید با کسی گفته شود.

4. تنظیمات حریم خصوصی (Privacy Settings)

حریم خصوصی به معنای تعیین میزان دسترسی دیگران به اطلاعات شخصی شما است. به‌عبارت ساده، شما مشخص می‌کنید چه کسانی بتوانند اطلاعات، تصاویر و فعالیت‌های شما را ببینند یا با آن‌ها تعامل داشته باشند. برای مثال، در شبکه‌های اجتماعی مانند Facebook یا Instagram، شما می‌توانید تنظیم کنید که چه افرادی بتوانند پُست‌های شما را مشاهده کنند یا آن‌ها را لایک، کامنت و یا به اشتراک بگذارند.

این به این معنا نیست که همیشه اختیار کامل دارید، بلکه باید آگاهانه تنظیمات حریم خصوصی را مدیریت کنید. بنابراین، تعیین دقیق و محتاطانه میزان اشتراک‌گذاری اطلاعات می‌تواند نقش مهمی در حفظ امنیت شخصی شما داشته باشد.

5. عدم شریک‌سازی معلومات شخصی

معلومات شخصی شما مانند کلید ورود به زندگی دیجیتالی‌تان است. اگر این معلومات به دست افراد نادرست بیفتد، ممکن است از آن برای سوءاستفاده، سرقت هویت یا دسترسی غیرمجاز به حساب‌های شما استفاده شود.

بنابراین، هرگز نباید اطلاعات حساس خود را با دیگران افرادی که به آن‌ها اعتماد دارید شریک سازید. این اطلاعات شامل موارد زیر می‌شود:

- رمز عبور(Password)
- معلومات بانکی (مانند شماره کارت یا حساب)
- اطلاعات شخصی مهم (مانند شماره تذکره، آدرس، یا شماره تماس)

برای مثال، اگر کسی از طریق ایمیل یا شبکه‌های اجتماعی مانند WhatsApp یا Telegram از شما درخواست چنین اطلاعاتی کند، به احتمال زیاد یک تلاش برای کلاهبرداری (Phishing) است.

در نتیجه، حفظ و عدم اشتراک‌گذاری معلومات شخصی یکی از مهم‌ترین اصول امنیت دیجیتال است و می‌تواند شما را از بسیاری خطرات محافظت کند.

6. آگاهی از مراکز گزارش‌دهی

مرکزهای گزارش‌دهی مانند **CEOP**[1] و دیگر نهادهای معتبر، مکان‌هایی هستند که افراد می‌توانند سوءاستفاده‌ها و رفتارهای خطرناک آنلاین را به صورت امن گزارش دهند. این مراکز به بررسی گزارش‌ها، پیگیری متخلفان و محافظت از قربانیان کمک می‌کنند.

اگر شما یا کسی که می‌شناسید، مورد سوءاستفاده، تهدید یا هر رفتار آنلاین مشکوک قرار گرفت، مهم است که موضوع را سریعاً گزارش کنید. عدم اقدام می‌تواند باعث ادامه یا تشدید سوءاستفاده شود.

مزایای گزارش‌دهی عبارت‌اند از:

- جلوگیری از آسیب بیشتر به شما یا دیگران

[1] **CEOP** (Child Exploitation and Online Protection Command)

- شناسایی و پیگرد قانونی افراد مجرم
- افزایش آگاهی عمومی و امنیت آنلاین برای همه
- دریافت راهنمایی و پشتیبانی از متخصصان امنیت

برای مثال، اگر کسی از طریق شبکه‌های اجتماعی یا ایمیل تهدید، کلاهبرداری یا درخواست اطلاعات شخصی داشت، می‌توانید مستقیماً آن را به مرکز گزارش‌دهی مربوطه اطلاع دهید. این اقدام نه تنها شما را محافظت می‌کند، بلکه به جلوگیری از قربانی شدن دیگران نیز کمک می‌کند. حفظ آگاهی از مراکز گزارش‌دهی و اقدام به موقع، یکی از اصول کلیدی امنیت دیجیتال است و می‌تواند شما را از بسیاری خطرات آنلاین مصون نگه دارد.

2.3 سوءاستفاده از معلومات دیجیتلی

معلومات دیجیتلی شما شامل هر دیتایی است که در فضای آنلاین یا روی دستگاه‌های دیجیتالی ذخیره می‌شود، مانند پیام‌ها، عکس‌ها، و اطلاعات شخصی. این اطلاعات همیشه برای اهداف مثبت استفاده نمی‌شوند و گاهی افراد یا گروه‌های نادرست از آن‌ها برای اهداف خطرناک سوءاستفاده می‌کنند.
نمونه‌های سوءاستفاده عبارت‌اند از:

- **سرقت هویت :**استفاده از اطلاعات شخصی شما برای باز کردن حساب‌های بانکی، درخواست وام یا انجام کلاهبرداری
- **کلاهبرداری آنلاین :**استفاده از اطلاعات شما برای فریب دادن خود یا دیگران و دریافت پول یا اطلاعات بیشتر
- **نظارت و جاسوسی :**جمع‌آوری و تحلیل اطلاعات شما بدون اجازه برای کنترل یا دسترسی به زندگی شخصی

بنابراین، شناخت این خطرات بسیار مهم است. اقدامات پیشگیرانه شامل موارد زیر می‌شود:

- محافظت از اطلاعات شخصی و حساس
- عدم اشتراک‌گذاری اطلاعات با افراد یا سایت‌های نامعتبر
- استفاده از رمزهای قوی و ابزارهای امنیتی مانند احراز هویت دو مرحله‌ای 2FA
- آگاهی از روش‌های گزارش‌دهی سوءاستفاده و اقدام سریع در صورت مواجهه با تهدید

در نتیجه، درک و آگاهی از نحوه سوءاستفاده از معلومات دیجیتلی، کلید حفظ امنیت و محافظت از خود در فضای دیجیتال است و می‌تواند شما را از بسیاری آسیب‌ها مصون نگه دارد.

انواع مهم سوءاستفاده از دیتا

1. فیشینگ و فارمینگ(Phishing & Pharming)

فریب افراد برای گرفتن دیتاهای شخصی مانند رمز عبور، شماره کارت یا اطلاعات حساب.
مثال:

- ایمیل جعلی از بانک

- لینک تقلبی شبیه سایت اصلی

خطر :سرقت حساب‌ها و دیتاهای حساس یا موجودی حساب شما.

2. ترولینگ و آزار آنلاین(Cyberbullying)

ارسال پیام‌های توهین‌آمیز، تهدید یا اذیت افراد آنلاین برای آسیب رساندن روانی.

مثال:

- پیام‌های توهین‌آمیز در شبکه‌های اجتماعی
- مسخره کردن افراد آنلاین

خطر :آسیب روانی و کاهش اعتماد به نفس

3. هک کردن(Hacking)

دسترسی غیرمجاز به سیستم‌ها، حساب‌ها یا دستگاه‌های دیجیتالی شما.

شامل:

- هک موبایل یا کامپیوتر
- شنود تماس‌ها و پیام‌ها

خطر :سرقت دیتا و سوءاستفاده از حساب‌ها

4. سوءاستفاده از شبکه‌های اجتماعی

شامل:

- **فریب دادن افراد :(Grooming)** ایجاد رابطه با هدف سوءاستفاده
- **ارسال محتوای نامناسب :(Sexting)** مجبور کردن افراد به ارسال محتوا
- **استفاده از حساب دیگران :(Frapping)** ورود و پست گذاشتن بدون اجازه

مثال :کسی بدون اجازه وارد حساب شما شده و پست می‌گذارد.

خطر :سرقت دیتا شخصی و آسیب به امنیت دیجیتالی

5. سایر تهدیدهای مهم

- **بدافزارها و ویروس‌ها :**برنامه‌هایی که به صورت مخفیانه به سیستم شما نفوذ کرده و دیتا را می‌دزدند یا خراب می‌کنند
- **اسپم و هرزنامه :**پیام‌ها و ایمیل‌های غیرضروری که ممکن است حاوی لینک‌های خطرناک باشند
- **ربات‌ها و تله‌های آنلاین :**جمع‌آوری دیتاهای شما بدون اجازه برای تبلیغات یا سوءاستفاده

اقدامات پیشگیرانه:

- نصب آنتی‌ویروس و بروزرسانی مداوم
- اجتناب از باز کردن لینک‌ها یا فایل‌های ناشناس

- تنظیمات حریم خصوصی و محدود کردن دسترسی‌ها

3.3 راهنمای جامع قوانین و استفاده صحیح از دیتا دیجیتلی

در دنیای دیجیتال، استفاده از دیتا کاملاً آزاد نیست؛ بلکه توسط قوانین و مقررات مختلف کنترل می‌شود. این قوانین برای:

- محافظت از افراد
- جلوگیری از سوءاستفاده
- ایجاد نظم در استفاده از دیتا وضع شده‌اند.

نکته مهم:

استفاده نادرست از دیتا می‌تواند پیامدهای قانونی جدی داشته باشد و باعث مشکلات مالی، تحصیلی یا اجتماعی شود.

هدف آموزشی:

- شناخت قوانین مهم و ضروری
- توضیح تأثیر آن‌ها بر استفاده از دیتا
- رعایت قوانین در زندگی دیجیتال

انواع قوانین و محدودیت‌ها

1. پالیسی استفاده قابل قبول (AUP)

AUP یا **Acceptable Use Policy** مجموعه قوانینی است که توسط مدارس، دانشگاه‌ها یا اداره‌ها وضع می‌شود تا رفتار کاربران را در محیط دیجیتال کنترل کند. این قوانین مشخص می‌کنند که چه نوع استفاده‌ای از اینترنت، کامپیوتر یا شبکه داخلی مجاز است و چه نوع فعالیت‌هایی ممنوع است.

هدف:

کنترل رفتار کاربران و حفظ امنیت محیط آموزشی

مثال عملی:

- استفاده از اینترنت فقط برای اهداف درسی یا تحقیقاتی
- ممنوعیت دانلود برنامه‌های غیرمجاز یا بازی

پیامد:

عدم رعایت → محرومیت از کامپیوتر یا اینترنت مدرسه، تنبیه یا هشدار رسمی

چرا مهم است؟
این قانون کمک می‌کند دانش آموزان یاد بگیرند اینترنت را به شکل مسئولانه استفاده کنند و از وقت و منابع آموزشی بهینه بهره ببرند.

2. حق نشر(Copyright)

حق نشر یا **Copyright** به آثار خلاقانه افراد مانند کتاب، تصویر، ویدیو یا موسیقی محافظت قانونی می‌دهد. این قانون به افراد و شرکت‌ها اجازه می‌دهد کنترل کنند که چگونه اثرشان استفاده شود. شما هم اگر محتوایی در انترنت نشر میکند باید این قوانین را رعایت کنید.
هدف:
جلوگیری از کپی و استفاده غیرقانونی از آثار دیگران
مثال عملی:
- کپی کردن یک کتاب بدون اجازه
- استفاده از تصویر یا متن با ذکر منبع یا پرداخت هزینه در قابل استفاده با مجوز همان منبع

پیامد:
نقض حق نشر → ممکن است با جریمه یا مشکلات قانونی مواجه شوید
چرا مهم است؟
رعایت حقوق نشر احترام به خلاقیت دیگران است و نشان می‌دهد شما یک کاربر مسئول دیجیتال هستید.

3. قانون سوءاستفاده از کمپیوتر(Computer Misuse)

این قانون به منظور جلوگیری از جرایم سایبری وضع شده است و شامل هک، دسترسی غیرمجاز، خرابکاری یا سرقت دیتا می‌شود.
هدف:
محافظت از سیستم‌ها و دیتاهای کاربران
مثال عملی:
- هک کردن سیستم مدرسه یا ایمیل دیگران
- دسترسی به حساب کاربری بدون اجازه

پیامد:
این کار جرم محسوب می‌شود و مجازات قانونی دارد
چرا مهم است؟
این قانون تضمین می‌کند که فضای دیجیتال امن باقی بماند و هیچ‌کس بدون اجازه به اطلاعات دیگران دسترسی نداشته باشد.

4. حفاظت از دیتا(Data Protection)

قانون حفاظت از دیتا یا **Data Protection** برای حفظ اطلاعات شخصی افراد مانند شماره تماس، آدرس یا نتایج تحصیلی یا هر دیتا سودمند وضع شده است. این قانون از سوءاستفاده و انتشار غیرمجاز دیتا جلوگیری می‌کند.

هدف:

افزایش امنیت و اعتماد کاربران

مثال عملی:

- نگهداری امن دیتاهای دانش آموزان و کارکنان مدرسه
- عدم انتشار اطلاعات شخصی بدون اجازه

پیامد:

رعایت این قانون → امنیت بیشتر، اعتماد بالاتر

عدم رعایت → مشکلات قانونی و اخلاقی

چرا مهم است؟

دانش آموزان یاد می‌گیرند احترام به حریم خصوصی دیگران چیست و چرا محافظت از دیتا شخصی ضروری است.

5. قانون ارتباطات(Communication Act)

این قانون نحوه استفاده از ابزارهای ارتباط دیجیتالی مانند ایمیل، پیام‌رسان‌ها و شبکه‌های اجتماعی را کنترل می‌کند. هدف جلوگیری از ارسال پیام‌های تهدیدآمیز، انتشار اطلاعات نادرست و آزار آنلاین است.

هدف:

حفظ امنیت، اخلاق و سلامت روان کاربران

مثال عملی:

- ارسال پیام تهدیدآمیز
- انتشار شایعات یا اطلاعات نادرست

پیامد:

رعایت قانون → فضای دیجیتال امن و اخلاقی

عدم رعایت → تنبیه قانونی یا حذف حساب کاربری

چرا مهم است؟

این قانون به دانش آموزان یاد می‌دهد چگونه مسئولانه با دیگران در فضای آنلاین تعامل کنند.

تأثیر این قوانین بر استفاده از دیتا

قانون	تأثیر بر کاربر
AUP	محدودیت و کنترل استفاده از اینترنت و کامپیوتر در مدرسه یا محیط کاری
Copyright	جلوگیری از استفاده غیرقانونی از آثار دیگران
Data Protection	حفاظت از حریم خصوصی و امنیت دیتا
Computer Misuse	جلوگیری از هک و دسترسی غیرمجاز
Communication Act	پیشگیری از سوءاستفاده و پیام‌های مضر

6. مثال عملی

وضعیت:

یک دانش آموز:

- تصویر از اینترنت می‌گیرد
- در پروژه خود استفاده می‌کند

اگر:

- منبع ذکر نشود ❌ → نقض Copyright
- استفاده درست باشد ✅ → قانونی

چرا این مثال مهم است؟

دانش آموزان یاد می‌گیرند هر دیتا یا اثر دیجیتال دارای حقوق و قوانین است و رعایت آن‌ها بخشی از رفتار مسئولانه دیجیتالی است. بعضی شرکت ها بعضی محتوا را رایگان در اختیار کاربران به اشتراک میگذارد که این محتوا بدون ذکر منبع هم اشکال ندارد بهتر منبع آن ذکر شود.

4.3 بررسی و تشریح استندردهای باز (Open Standards)

در دنیای دیجیتال، تمام فایل‌ها و دیتاها در قالب‌های مشخصی ذخیره می‌شوند که به آن‌ها «فرمت» یا «استندرد» گفته می‌شود. این فرمت‌ها تعیین می‌کنند که یک فایل چگونه ذخیره شود و چگونه توسط نرم‌افزارها خوانده شود.

اما نکته مهم این است که همه فرمت‌ها یکسان نیستند. بعضی از آن‌ها:

- **باز (Open)** هستند → همه می‌توانند آزادانه استفاده کنند
- **بسته یا اختصاصی (Proprietary)** هستند → فقط توسط یک شرکت یا نرم‌افزار خاص قابل استفاده‌اند

تعریف استندرد باز:
استندرد باز نوعی فرمت یا تکنالوژی است که:
- برای همه قابل دسترسی و استفاده است
- وابسته به یک شرکت خاص نیست
- معمولاً رایگان یا کم‌هزینه است
- مستندات آن در دسترس عموم قرار دارد

چرا این موضوع مهم است؟
اگر شما فایلی را در یک فرمت بسته ذخیره کنید، ممکن است در آینده نتوانید آن را باز کنید یا مجبور شوید نرم‌افزار خاصی خریداری کنید. اما استندردهای باز این مشکل را حل می‌کنند و باعث آزادی و انعطاف بیشتر در استفاده از دیتا می‌شوند.

ویژگی‌های استندردهای باز

استندردهای باز دارای ویژگی‌های مهمی هستند که آن‌ها را از سایر فرمت‌ها متمایز می‌کند:
- **رایگان بودن :**بیشتر این فرمت‌ها بدون نیاز به پرداخت قابل استفاده‌اند
- **سازگاری بالا :**در نرم‌افزارهای مختلف (حتی از شرکت‌های مختلف) کار می‌کنند
- **مناسب برای اشتراک‌گذاری :**به راحتی بین افراد و سیستم‌ها تبادل می‌شوند
- **عدم وابستگی :**شما مجبور نیستید از یک نرم‌افزار خاص استفاده کنید

مثال قابل فهم:
اگر یک فایل در فرمت باز باشد، شما می‌توانید آن را در چندین برنامه مختلف باز کنید. اما اگر فرمت بسته باشد، شاید فقط در یک برنامه خاص باز شود.

نتیجه:
استفاده از استندردهای باز یعنی آزادی بیشتر، هزینه کمتر و دسترسی آسان‌تر به دیتا.

فرمت‌های تصویری مهم(Open Standards)

تصاویر بخش مهمی از وب‌سایت‌ها، پروژه‌های درسی و شبکه‌های اجتماعی هستند. انتخاب فرمت مناسب تصویر بسیار مهم است، زیرا بر کیفیت، حجم و سرعت بارگذاری تأثیر می‌گذارد.

فرمت‌های مهم:

- **SVG (Scabble Vector Graphics):**
  - نوع: برداری (Vector)
  - ویژگی: بدون کم شدن کیفیت در هر اندازه
    کاربرد: لوگو، آیکن، طراحی گرافیکی

دلیل: چون بزرگ یا کوچک شود، کیفیت خراب نمی‌شود

- **JPG, JPEG (Joint Photographic Experts Group):**

- نوع: فشرده
- ویژگی: حجم کم
- کاربرد: عکس‌ها

دلیل: مناسب برای ذخیره تصاویر زیاد بدون مصرف زیاد اینترنت

- **PNG (Portable Network Graphics):**
  - ویژگی: کیفیت بالا + شفافیت (Transparent)
  - کاربرد: تصاویر وب، طراحی

دلیل: برای تصاویر با پس‌زمینه شفاف بسیار مناسب است

نتیجه:

این فرمت‌ها در تمام مرورگرها (Browser) ها پشتیبانی می‌شوند، به همین دلیل بهترین انتخاب برای وب هستند.

استندردهای مهم در وب Web

وب‌سایت‌ها بدون این استندردها کار نمی‌کنند. این‌ها مانند یک «زبان مشترک» بین کامپیوترها، سرورها و مرورگرها هستند که باعث می‌شوند همه چیز به‌درستی نمایش و تبادل شود. که در ذیل بصورت فشرده به آن اشاره میکنیم.

جدول مهم استندردها وب

استندرد	وظیفه اصلی	توضیح ساده و قابل فهم	مثال کاربردی
HTML	ساختار صفحه وب	مانند اسکلت بدن است؛ تعیین می‌کند چه چیزهایی (متن، تصویر، لینک) در صفحه باشد	ایجاد عنوان، پاراگراف، دکمه
CSS	طراحی و ظاهر	ظاهر صفحه را زیبا می‌کند؛ رنگ، فونت و چیدمان را تنظیم می‌کند	تغییر رنگ متن، طراحی دکمه
XML	ذخیره و انتقال دیتا	برای ذخیره و تبادل دیتا بین سیستم‌ها استفاده می‌شود	ارسال دیتا بین دو سیستم مختلف
SQL	مدیریت دیتابیس	برای ذخیره، جستجو و مدیریت دیتا در پایگاه داده	ذخیره اطلاعات کاربران در وب‌سایت
RSS	نشر محتوا	برای دریافت خودکار اخبار و به‌روزرسانی‌ها	دنبال کردن اخبار یک سایت
HTTPS	انتقال دیتا	ارتباط بین کاربر و وب‌سایت را برقرار می‌کند	باز کردن یک وب‌سایت در مرورگر

نتیجه مهم:

اگر این استندردها وجود نداشتند، هیچ ویب‌سایتی کار نمی‌کرد و اینترنت به شکل امروزی وجود نداشت.

تفاوت Open وProprietary

در دنیای دیجیتال، فایل‌ها و نرم‌افزارها یا بر اساس **استندردهای باز (Open)** ساخته می‌شوند یا **بسته و اختصاصی** .**(Proprietary)** انتخاب بین این دو نوع، تأثیر مستقیم بر دسترسی، هزینه، و آزادی شما در استفاده از دیتا دارد.

استانداردهای باز (Open Standards)

ویژگی‌ها:

- معمولاً رایگان و در دسترس همه
- در نرم‌افزارهای مختلف باز می‌شوند
- وابسته به یک شرکت خاص نیستند
- مناسب برای اشتراک‌گذاری و همکاری

وقتی از استندرد باز استفاده می‌کنید، شما مالک واقعی دیتای خود هستید. یعنی هر زمان، در هر سیستم و با هر نرم‌افزاری می‌توانید به فایل‌های خود دسترسی داشته باشید. این موضوع به‌خصوص در آموزش، کار تیمی و اشتراک‌گذاری بسیار مهم است.

مثال:

فایل‌های html. یا png. تقریباً در تمام سیستم‌ها و برنامه‌ها باز می‌شوند، بدون نیاز به نرم‌افزار خاص یا پرداخت هزینه.

نتیجه:

آزادی، دسترسی آسان، و انعطاف‌پذیری بالا در همه بخش ها

بسته یا اختصاصی (Proprietary)

ویژگی‌ها:

- وابسته به یک شرکت یا نرم‌افزار خاص
- گاهی نیاز به خرید یا لایسنس دارد
- ممکن است در همه برنامه‌ها باز نشود
- محدود در اشتراک‌گذاری و استفاده

در فرمت‌های بسته، شما کاملاً وابسته به یک شرکت می‌شوید. اگر آن نرم‌افزار را نداشته باشید یا نسخه آن تغییر کند، ممکن است دیگر نتوانید فایل خود را باز کنید. این یعنی کنترل کامل روی دیتای شما در اختیار شما نیست.

مثال:

فایل psd. فقط در نرم‌افزار Adobe Photoshop به‌خوبی باز می‌شود، یا فایل docx. وابسته به Microsoft Word است.

نتیجه:
محدودیت، وابستگی، و گاهی هزینه و بدون انعطاف پذیری.
مثال واقعی و قانع‌کننده برای دانش آموزان
فرض کنید شما یک پروژه مهم درسی دارید:

- اگر آن را در فرمت باز ذخیره کنید :
  - می‌توانید در هر کامپیوتر، حتی بدون نرم‌افزار خاص، آن را باز و ویرایش کنید
- اما اگر در فرمت بسته ذخیره کنید:
  - فقط در یک برنامه خاص باز می‌شود و اگر آن برنامه را نداشته باشید، فایل شما عملاً بی‌استفاده می‌شود.

این یعنی انتخاب فرمت، می‌تواند موفقیت یا مشکل شما را در طراحی و کارهای دیجیتلی تعیین کند.

جدول مقایسه (درک بهتر)

ویژگی	Open Standards	Proprietary
دسترسی	آزاد و عمومی	محدود
هزینه	رایگان یا کم	گاهی پولی
سازگاری	بالا (چندین نرم‌افزار)	محدود
وابستگی	ندارد	به شرکت خاص
اشتراک‌گذاری	آسان	دشوارتر

لایسنسCreative Commons

بعضی از محتواها (مثل عکس، ویدیو، موسیقی، متن و ...) دارای جواز استفاده (License) هستند که مشخص می‌کند دیگران چگونه می‌توانند از آن استفاده کنند. یکی از معروف‌ترین این جوازها، **Creative Commons** است که به صاحب اثر اجازه می‌دهد شرایط استفاده از اثرش را خودش تعیین کند و شما مجبور هستید از آن شرایط تبعیت کنید.

Creative Commons یعنی:
نوعی لایسنس (جواز) که به دیگران اجازه می‌دهد از محتوا استفاده کنند، اما با **شرایط مشخص** مثل:

- ذکر نام صاحب اثر
- استفاده غیرتجاری
- عدم تغییر محتوا
- یا اشتراک‌گذاری با همان شرایط

به یاد داشته باشید License در اثرهای دیجیتلی و فزیکی مانند کتاب نقاشی ها رویی دیوار... شرایط و ضوابط آنها کمی با همدیگر تفاوت دارد.

انواع مهم لایسنسCreative Commons

نوع لایسنس	توضیح ساده
CC BY	فقط ذکر نام صاحب اثر کافی است
CC BY-NC	فقط استفاده غیرتجاری مجاز است
CC BY-SA	باید با همان لایسنس دوباره نشر شود
CC BY-ND	اجازه تغییر در محتوا داده نمی‌شود

اهداف

مورد	توضیح
استفاده قانونی	استفاده بدون مشکل حقوقی از آثار دیگران
حمایت از تولیدکننده	حفظ حقوق صاحب اثر
اشتراک‌گذاری آسان	کمک به نشر دانش و محتوا

مقایسه

وضعیت استفاده	نوع لایسنس
استفاده تقریباً ممنوع	Copyright کامل
استفاده آزاد اما با شرایط	Creative Commons
استفاده کاملاً آزاد بدون شرط	Public Domain

تأثیر استانداردهای باز بر استفاده از دیتا

استانداردهای باز (Open Standards) باعث می‌شوند داده‌ها به‌راحتی بین سیستم‌های مختلف قابل استفاده و انتقال باشند، در حالی‌که فرمت‌های اختصاصی (Proprietary) محدودیت ایجاد می‌کنند. همچنین رعایت لایسنس نقش مهمی در قانونی بودن استفاده از داده دارد.

جدول تأثیرات

حالت	نتیجه	توضیح کامل
Open استفاده از (استاندارد باز)	اشتراک آسان	داده‌ها به‌راحتی بین سیستم‌ها، نرم‌افزارها و کاربران مختلف قابل انتقال و استفاده هستند

Proprietary استفاده از (اختصاصی)	محدودیت	داده‌ها فقط در نرم‌افزار یا سیستم خاص باز می‌شوند و انتقال یا استفاده در سایر سیستم‌ها دشوار است
رعایت لایسنس	استفاده قانونی	استفاده از داده‌ها بدون مشکل حقوقی انجام می‌شود و حقوق صاحب اثر حفظ می‌گردد
عدم رعایت لایسنس	مشکل قانونی	ممکن است باعث نقض قانون، جریمه یا محدودیت در استفاده از داده‌ها شود

جدول اصطلاحات مهم پلتفورم‌های باز

اصطلاح انگلیسی	مخفف	معنی به دری	کاربرد / توضیح
Open Standards	—	استانداردهای باز	فرمت‌ها و تکنالوژی‌هایی که برای همه قابل استفاده است
Scalable Vector Graphics	SVG	گرافیک برداری مقیاس‌پذیر	برای طراحی لوگو و تصاویر بدون افت کیفیت
Joint Photographic Experts Group	JPG / JPEG	فرمت تصاویر فشرده	برای عکس‌ها با حجم کم
Portable Network Graphics	PNG	گرافیک شبکه قابل حمل	تصاویر با کیفیت و پس‌زمینه شفاف
HyperText Markup Language	HTML	زبان نشانه‌گذاری ابرمتن	ساختار صفحات ویب
Cascading Style Sheets	CSS	صفحات سبک آبشاری	طراحی و زیباسازی صفحات ویب
Extensible Markup Language	XML	زبان نشانه‌گذاری قابل گسترش	ذخیره و انتقال دیتا
Structured Query Language	SQL	زبان پرس‌وجوی ساختاریافته	مدیریت دیتابیس
Really Simple Syndication	RSS	انتشار ساده محتوا	دریافت اخبار و بروزرسانی‌ها
HyperText Transfer Protocol	HTTP	پروتوکول انتقال ابرمتن	انتقال دیتا در اینترنت
Creative Commons	CC	جواز استفاده عمومی	اجازه استفاده از محتوا با شرایط
Open Document Format	ODF	فرمت اسناد باز	برای فایل‌های متنی آزاد(.odt)
Comma Separated Values	CSV	مقادیر جدا شده با کاما	انتقال ساده دیتا

Portable Document Format	PDF	فرمت سند قابل حمل	نمایش اسناد بدون تغییر
Plain Text File	TXT	فایل متن ساده	ذخیره متن بدون فرمت
HyperText Markup Language 5	HTML5	نسخه جدیدHTML	ساخت صفحات پیشرفته ویب
Attribution	CC BY	ذکر منبع	می‌توانید استفاده کنید، فقط باید نام صاحب اثر را ذکر کنید
Attribution-NonCommercial	CC BY-NC	ذکر منبع + غیرتجاری	استفاده مجاز است، اما برای کار تجارتی نه
Attribution-ShareAlike	CC BY-SA	ذکر منبع + اشتراک مشابه	استفاده مجاز است، اما باید با همان جواز دوباره نشر شود
Attribution-NoDerivatives	CC BY-ND	ذکر منبع + بدون تغییر	استفاده مجاز است، اما نباید تغییر داده شود

جدول بالا شامل اصطلاحات کاربردی در بخش Open Standards بود که لازم است آنها یاد داشته باشید.

منابع

شماره	عنوان	لینک
1	Open Standards and Open Source (مهم‌ترین مقاله)	لینک دانلود
2	Open Standards in Digital Systems (Whitepaper دولتی)	آدرس مقاله
3	Digital Cultural Standards (Springer)	آدرس مقاله
4	Open Standards and the Digital Age	کتاب آدرس خرید
5	Open standards, open formats, and open source	آدرس مقاله
6	Digital Health & Open Standards	آدرس مقاله

فصل دوم

مدیریت پلتفرم های دیجیتلی
(Managing Digital Platforms Applying Digital Skills)

شرایط بخش دوم:

- **ساعت های درسی:** 25 ساعت
- **ساعت های اصافی:** 3 ساعت
- **مجموع ساعت های درسی:** 28 ساعت

در این فصل دانش آموزان خواهند آموخت:

Strand 1

دانش آموزان یاد می‌گیرند دیتایی که تولید می‌کنند باید به‌صورت منظم مدیریت شود و بدانند چگونه آن را در جای‌های مختلف درست نگهداری کنند.

Strand 2

دانش آموزان می‌فهمند که دیتا چگونه از یک سیستم به سیستم دیگر تبدیل می‌شود و چگونه می‌توانند از این تبدیل‌ها در کارهای عملی استفاده کنند.

Strand 3

دانش آموزان اهمیت استانداردهای باز را در دنیای امروز درک می‌کنند و می‌فهمند که این موضوع چگونه باعث کار کردن اینترنت و سایر تکنالوژی‌ها شده است.

Strand 4

دانش آموزان انواع ذخیره‌سازی (محلی و ابری) را می‌شناسند و می‌فهمند که هرکدام چه خوبی‌ها و مشکل‌ها دارند و در کجا استفاده می‌شوند.

Strand 5

دانش آموزان روش‌های مختلف کار گروهی دیجیتلی را یاد می‌گیرند و می‌فهمند که کدام روش برای کدام کار مناسب‌تر است.

Strand 6

دانش آموزان یاد می‌گیرند کار خود را بررسی کنند، خوبی‌ها و ضعف‌ها را پیدا کنند و نتایج کار خود را به دیگران ارائه دهند و از نظر دیگران استفاده کنید.

1. درک ضرورت مدیریت مواد دیجیتلی

در دنیای امروزی، مقدار بسیار زیادی دیتا به‌صورت پیوسته تولید و جمع‌آوری می‌شود. این دیتا شامل معلوماتی است که خود افراد ایجاد می‌کنند، مانند عکس‌ها، اسناد و فعالیت‌های آنلاین، و همچنان معلوماتی که درباره آن‌ها توسط سیستم‌ها بدون اطلاع‌شان جمع‌آوری می‌شود، مانند موقعیت مکانی، استفاده از اینترنت و تصاویر کمره‌های امنیتی. با توجه به افزایش سریع این دیتا، اگر مدیریت درست انجام نشود، باعث بی‌نظمی، مشکل در دسترسی و حتی خطرات امنیتی می‌گردد. بنابراین، دانستن اینکه چه نوع دیتا جمع می‌شود و چگونه باید آن را تنظیم، نگهداری و محافظت کرد، برای هر فرد ضروری است.

- مقدار دیتا در حال افزایش بسیار سریع است
- دیتا هم توسط خود افراد تولید می‌شود و هم درباره آن‌ها جمع‌آوری می‌شود
- بسیاری از دیتاها بدون اطلاع کاربر جمع‌آوری می‌شود
- دیتا در اشکال مختلف مانند تصویر، موقعیت، متن و ویدیو وجود دارد
- دستگاه‌ها و سیستم‌ها (موبایل، اینترنت،CCTV) نقش مهم در جمع‌آوری دیتا دارند
- عدم مدیریت دیتا باعث بی‌نظمی و خطرات امنیتی می‌شود
- مدیریت درست دیتا باعث امنیت و استفاده بهتر می‌گردد

دیتای که جمع آوری میشود شامل کدام موارد میشود؟
همانطوریکه در فصل اول دانستید دیتا مواد خام دیجیتلی مانند:

- نام
- عکس
- موقعیت
- فعالیت ها
- ... وغیره

و این دیتا خام تحلیل و پروسس شود به معلومات یا Information تبدیل میشود.

انواع دیتا که توسط دستگاه و ابزارهای دیجیتلی جمع آوری میشوند:

نوع دیتا	مثال ساده	چگونه جمع می‌شود؟
📍 **موقعیت**	مکان شما	موبایل(GPS)
🏫 **تعلیمی**	راپور مکتب	سیستم مکتب
📺 **عادت‌ها**	دیدن تلویزیون	Smart TV
🌐 **اینترنت**	سایت‌ها	WiFi / ISP
🎥 **امنیتی**	تصویر شما	CCTV
🛂 **سفر**	پاسپورت	میدان هوایی

ترانسپورت	مسیر رفت و آمد	کارت سفر
اجتماعی	عکس، چت	شبکه‌های اجتماعی

مثالهای جمع آوری دیتا

وسیله / سیستم	چه کار می‌کنید	چه دیتا جمع می‌شود	ابزار آن
موبایل	استفاده از نقشه	موقعیت(Location)	GPS
CCTV	عبور از جاده	تصویر شما	کمره امنیتی
اینترنت	باز کردن سایت	فعالیت آنلاین	ISP / Browser
تلویزیون هوشمند	دیدن برنامه	عادت‌های دیدن	Smart System
میدان هوایی	سفر خارجی	پاسپورت + چهره	سیستم امنیتی
ترانسپورت	استفاده از کارت	مسیر رفت و آمد	سیستم بلیط
شبکه اجتماعی	چت و پست	عکس، پیام	App

تحلیل بیشتر به موضوعات بررسی شده:

دیتا منظم و پاک‌کاری آن

دیتا باید همیشه منظم نگهداری شود و فایل‌های غیرضروری حذف گردد تا سیستم بهتر کار کند. اگر دیتا زیاد و نامنظم باشد، هم حافظه پر می‌شود و هم سرعت سیستم کاهش می‌یابد. برای مثال، اگر در موبایل عکس‌های تکراری زیاد ذخیره شود، حافظه پر می‌شود، اما با پاک کردن آن‌ها، فضا آزاد شده و کارکرد بهتر می‌شود.

حقایق در مورد دیتا

امروزه مقدار دیتا به‌سرعت در حال افزایش است و بخش زیادی از آن بدون اطلاع افراد جمع‌آوری می‌شود. دستگاه‌ها و سیستم‌های مختلف مانند موبایل، اینترنت و کمره‌های امنیتی به‌صورت دوامدار معلومات را ثبت می‌کنند. برای مثال، در شهرها کمره‌های CCTV تصاویر افراد را ثبت می‌کنند و موبایل‌ها موقعیت کاربران را ذخیره می‌کنند.

دیتا که خود ما ایجاد می‌کنیم vs دیتا که درباره ما جمع می‌شود

دیتا به دو نوع تقسیم می‌شود: دیتایی که خود ما ایجاد می‌کنیم و دیتایی که درباره ما جمع‌آوری می‌شود. دیتای تولیدی شامل عکس‌ها، ویدیوها و فایل‌هایی است که خود ما می‌سازیم، اما دیتای جمع‌شده شامل معلوماتی مانند موقعیت مکانی یا تصاویر کمره‌ها است که توسط سیستم‌ها بدون

دخالت مستقیم ما ثبت می‌شود. برای مثال، گرفتن عکس توسط خود شما یک دیتای تولیدی است، اما ثبت تصویر شما توسط CCTV یک دیتای جمع‌شده است.

جدول مقایسه کلی

موضوع	توضیح کوتاه	مثال
مدیریت دیتا	تنظیم و نگهداری درست	فولدر بندی فایل‌ها
دلیل جمع‌آوری	بهبود خدمات و امنیت	Google Maps
محافظت دیتا	جلوگیری از دسترسی غیرمجاز	رمز قوی
نظم و پاک‌کاری	حذف فایل‌های اضافی	دیتاهای تکراری و غیر ضروری باید حذف شود
حقایق دیتا	افزایش سریع و جمع‌آوری دائم	CCTV
دیتا تولیدی	توسط خود ما ایجاد می‌شود	عکس گرفتن
دیتا جمع‌شده	توسط سیستم‌ها جمع می‌شود	ثبت موقعیت

روش‌های مدیریت و ذخیره‌سازی مواد دیجیتلی

مدیریت و ذخیره‌سازی دیتا

دیتا می‌تواند به روش‌های مختلف مدیریت و ذخیره شود و این روش‌ها تعیین می‌کنند که دیتا چگونه استفاده، محافظت و دسترسی شود. برخی دیتاها به‌صورت شخصی (Private) نگهداری می‌شوند که فقط خود فرد به آن دسترسی دارد، در حالی که بعضی دیگر به‌صورت عمومی (Public) در اختیار دیگران قرار می‌گیرد. همچنان دیتا می‌تواند در سیستم شخصی (Local) ذخیره شود یا در اینترنت .(Cloud) هر روش مزایا و مشکلات خاص خود را دارد و انتخاب درست آن بستگی به نوع دیتا و هدف استفاده دارد. برای مثال، ذخیره فایل‌های مهم در کمپیوتر شخصی امنیت بیشتری دارد، اما ذخیره در Cloud باعث می‌شود از هرجا به آن دسترسی داشته باشیم.

روش‌های مختلف مدیریت دیتا

دیتا به شکل‌های مختلف مدیریت می‌شود تا هم قابل استفاده باشد و هم محفوظ بماند. یکی از این روش‌ها استفاده از فولدرهای مشترک (Shared) و محافظت‌شده (Protected) است. فولدرهای مشترک برای کار گروهی استفاده می‌شود، اما فولدرهای محافظت‌شده فقط برای افراد مشخص قابل دسترسی است. همچنان دیتا می‌تواند فشرده (Compressed) یا غیر فشرده (Uncompressed) باشد. فایل‌های فشرده حجم کم‌تری دارند و انتقال آن‌ها آسان است، اما ممکن است کیفیت یا سرعت دسترسی کاهش یابد. برای مثال، یک فایل ZIP حجم کم دارد و سریع ارسال می‌شود.

محل ذخیره دیتا(Location of Data)

محل ذخیره دیتا بسیار مهم است، زیرا قوانین کشورها روی آن تأثیر دارد. اگر دیتا در یک کشور خاص ذخیره شود، باید مطابق قوانین همان کشور مدیریت شود. بعضی شرکت‌ها دیتا را در سرورهای کشورهای دیگر ذخیره می‌کنند که ممکن است امنیت یا حریم خصوصی را تحت تأثیر قرار دهد. برای مثال، اگر معلومات شما در یک سرور خارجی ذخیره شود، ممکن است قوانین کشور شما از آن محافظت نکند.

تنظیمات حساب‌های آنلاین

در شبکه‌های اجتماعی، کاربران می‌توانند تعیین کنند که چه کسی به معلومات آن‌ها دسترسی داشته باشد. این تنظیمات شامل عمومی (Public) یا خصوصی (Private) بودن حساب است. اگر حساب عمومی باشد، همه می‌توانند محتوا را ببینند، اما اگر خصوصی باشد، فقط افراد مشخص دسترسی دارند. برای مثال، یک حساب فیسبوک که روی Private تنظیم شده باشد، فقط دوستان می‌توانند پُست‌ها را ببینند.

Big Data و نقش آن

Big Dataبه مقدار بسیار زیاد دیتا گفته می‌شود که توسط سیستم‌ها جمع‌آوری و تحلیل می‌شود. این دیتا برای تصمیم‌گیری‌های مهم استفاده می‌شود، مانند تحلیل رفتار کاربران یا پیش‌بینی آینده. برای مثال، شرکت‌ها از Big Data استفاده می‌کنند تا بدانند مردم بیشتر چه چیز را می‌خرند.

نیاز به HPC (قدرت پردازش بالا)

برای تحلیل Big Data ، سیستم‌های قوی به نام (High Performance Computing) **HPC** استفاده می‌شود. این سیستم‌ها توانایی پردازش مقدار زیاد دیتا را در زمان کوتاه دارند. برای مثال، در پیش‌بینی آب‌وهوا یا تحقیقات علمی از این سیستم‌ها استفاده می‌شود.

نکته بسیار مهم

دانش آموزان باید بدانند:

- دیتایی آن‌ها کجا ذخیره می‌شود
- چه کسی به آن دسترسی دارد

همچنان باید قبل از کلیک کردن روی گزینه‌ها یا قبول شرایط(Terms) ، دقت کنند، زیرا ممکن است اجازه دسترسی به دیتا خود را بدهند بدون اینکه متوجه شوند.

جدول خلاصه و مقایسه

موضوع	توضیح کوتاه	مثال
Private / Public	خصوصی یا عمومی بودن دیتا	حساب Private در فیسبوک
Local / Cloud	ذخیره در دستگاه یا اینترنت	هارد دیسکvs Google Drive
Shared / Protected	اشتراکی یا محافظت‌شده	فولدر مشترک صنف
Compressed	حجم کم‌تر	فایلZIP
Location Laws	قوانین کشور	سرور خارجی
Big Data	دیتای بسیار زیاد	تحلیل خرید کاربران
HPC	سیستم قوی پردازش	پیش‌بینی هوا

مشکلات مربوط به افزایش مقدار دیتا

امروزه مقدار دیتا به‌صورت بسیار سریع در حال افزایش است و این موضوع مشکلات زیادی را ایجاد کرده است. هر روز افراد، شرکت‌ها و سیستم‌ها مقدار زیادی دیتا تولید و ذخیره می‌کنند که مدیریت آن دشوار می‌شود. این افزایش باعث شده که ذخیره‌سازی، کنترول و محافظت از دیتا به یک چالش بزرگ تبدیل شود. برای مثال، شبکه‌های اجتماعی روزانه میلیون‌ها عکس و ویدیو ذخیره می‌کنند که مدیریت آن نیاز به سیستم‌های بسیار قوی دارد.

مصرف انرژی دیتا سنترها

ذخیره‌سازی این مقدار زیاد دیتا نیاز به دیتا سنترهای بزرگ دارد که انرژی بسیار زیاد مصرف می‌کنند. این مراکز مانند شهرهای بزرگ برق مصرف می‌کنند و تأثیر منفی بر محیط زیست دارند. برای مثال، در گذشته گفته شده که سیستم‌های IT حدود 10٪ برق جهان را مصرف می‌کردند و شرکت‌هایی مانند Google برق بسیار زیادی برای دیتا سنترهای خود استفاده می‌کنند.

دیتا از بین نمی‌رود

یکی از مشکلات مهم این است که دیتا پس از ایجاد شدن تقریباً هیچ‌وقت کاملاً از بین نمی‌رود. هر چیزی که در اینترنت نشر شود، ممکن است برای همیشه باقی بماند. این موضوع می‌تواند در آینده برای افراد مشکل ایجاد کند. برای مثال، اگر یک دانش آموز یک عکس یا پیام نامناسب نشر کند، ممکن است سال‌ها بعد هم در اینترنت موجود باشد.

محل ذخیره دیتا) مانند(Iceland

برای کاهش مصرف انرژی، بعضی کشورها مانند آیسلند از شرایط طبیعی خود استفاده می‌کنند. به دلیل هوای سرد، مصرف انرژی برای خنک‌سازی دیتا سنترها کم‌تر می‌شود و این کار از نظر محیط زیستی بهتر است. برای مثال، شرکت‌ها دیتا سنترهای خود را در مناطق سرد می‌سازند تا هزینه و انرژی کاهش یابد.

نشت دیتا(Data Leaks)

نشت دیتا زمانی اتفاق می‌افتد که معلومات به‌صورت غیرمجاز منتشر شود. این موضوع می‌تواند هم تأثیر مثبت و هم منفی داشته باشد، اما بیشتر باعث مشکلات امنیتی می‌شود. برای مثال، اگر معلومات شخصی کاربران یک سایت افشا شود، ممکن است افراد مورد سوءاستفاده قرار گیرند.

تأثیرات کلی بر جهان

افزایش مقدار دیتا تأثیرات زیادی بر جهان دارد، مانند:

- افزایش مصرف انرژی
- خطرات امنیتی
- مشکلات حریم خصوصی

در عین حال، این دیتا می‌تواند برای پیشرفت تکنالوژی و تصمیم‌گیری‌های بهتر نیز استفاده شود. برای مثال، تحلیل دیتا می‌تواند به بهبود خدمات صحی یا پیش‌بینی وضعیت هوا کمک کند. نمونه خوب استفاده از دیتا در ساخت ChatBot های هوش مصنوعی و آمارگیری و جلوگیری از تخریب فجایع طبیعی.

جدول مقایسه کلی مشکلات دیتا

موضوع	مشکل اصلی	مثال
افزایش دیتا	مدیریت دشوار	حجم زیاد ویدیوها
مصرف انرژی	برق زیاد	دیتا سنترهای بزرگ
ماندگاری دیتا	حذف سخت	پست‌های قدیمی
محل ذخیره	نیاز به شرایط خاص	دیتا سنتر در آیسلند
نشت دیتا	خطر امنیتی	افشای معلومات کاربران
تأثیر جهانی	محیط زیست و امنیت	مصرف 10٪ برق جهان

نیاز به استانداردهای باز(Open Standards)

استانداردهای باز به قوانینی گفته می‌شود که استفاده از آن‌ها برای همه آزاد است و باعث می‌شود سیستم‌ها و برنامه‌های مختلف بتوانند با هم کار کنند. در دنیای دیجیتال، اگر این استانداردها وجود نداشته باشد، تبادل معلومات بسیار مشکل می‌شود. یعنی یک فایل یا دیتا ممکن است در یک سیستم

باز شود، اما در سیستم دیگر کار نکند. برای مثال، وقتی شما یک صفحه ویب را باز می‌کنید، این کار به کمک استانداردهای باز انجام می‌شود که همه مرورگرها آن را پشتیبانی می‌کنند.

چرا استانداردهای باز مهم است؟

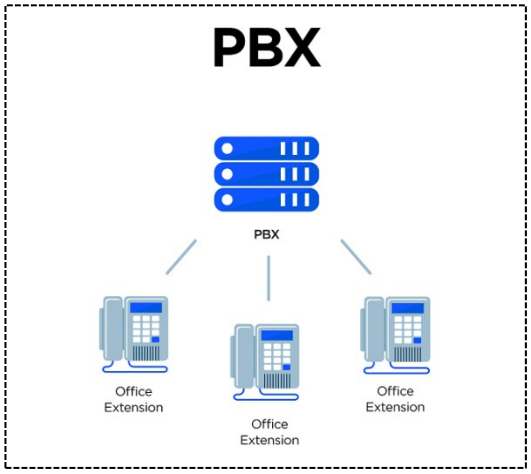
استانداردهای باز باعث می‌شوند که معلومات به‌راحتی بین سیستم‌های مختلف شریک شود. این کار باعث همکاری بهتر، کاهش محدودیت و استفاده آسان‌تر از دیتا می‌شود. اگر هر شرکت از روش خاص خود استفاده کند، تبادل دیتا مشکل می‌شود. برای مثال، یک فایل که در یک برنامه خاص ساخته شده، اگر استاندارد باز نداشته باشد، ممکن است در برنامه دیگر باز نشود.

مثال از استانداردهای مهم

در اینترنت چندین استاندارد باز استفاده می‌شود که هرکدام وظیفه خاص دارند. برای مثال، HTTP برای انتقال صفحات ویب، SMTP برای ارسال ایمیل و FTP برای انتقال فایل‌ها، PBX مدیریت تماس ها استفاده می‌شود. این استانداردها باعث می‌شوند که کاربران بتوانند به‌راحتی از خدمات مختلف اینترنت استفاده کنند.

نمونه ها:

- HTTP (Hyper Text Transfer Protocols)
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- PBX (Private Branch Exchange)



PBX (Private Branch Exchange)

نقش W3C

W3C (World Wide Web Consortium) یک سازمان جهانی است که استانداردهای ویب را تعیین می‌کند. این سازمان کمک می‌کند تا ویب‌سایت‌ها در همه مرورگرها به‌درستی کار کنند. اگر این استانداردها وجود نداشته باشد، ممکن است یک ویب‌سایت در یک مرورگر درست نمایش داده شود، اما در مرورگر دیگر مشکل داشته باشد.

همکاری بین سیستم‌ها Interoperability

Interoperability یعنی توانایی سیستم‌های مختلف برای کار کردن با یکدیگر. استانداردهای باز این امکان را فراهم می‌کنند که دیتا بدون مشکل بین سیستم‌ها انتقال یابد. برای مثال، یک فایل تصویری PNG در اکثر برنامه‌ها و دستگاه‌ها باز می‌شود، زیرا یک استاندارد باز است.

تفاوت Open و Closed Standards

استانداردهای باز برای همه قابل استفاده هستند، اما استانداردهای بسته (Closed) معمولاً متعلق به یک شرکت خاص هستند و محدودیت دارند. این موضوع بر نحوه اشتراک و استفاده از دیتا تأثیر می‌گذارد. برای مثال، بعضی فایل‌ها فقط در یک نرم‌افزار خاص باز می‌شوند. مانند فایل PSD شرکت ادوبی که فقط در برنامه های ادوبی قابل استفاده میباشد.

جدول مقایسهOpen vs Closed

نوع	ویژگی	مثال
Open Standards	آزاد و قابل استفاده در همه سیستم‌ها	HTTP, PNG
Closed Standards	محدود به شرکت خاص	PSD برخی نرم‌افزارها

جدول استانداردهای مهم

استاندارد	کاربرد	مثال
HTTP	انتقال صفحات ویب	باز کردن سایت
SMTP	ارسال ایمیل	Gmail
FTP	انتقال فایل	آپلود فایل
PBX	مدیریت تماس	سیستم تلفن

تفاوت ذخیره‌سازی محلی و دور(Local vs Remote)

ذخیره‌سازی محلی (Local Storage) به معنی نگهداری دیتا در دستگاه شخصی مانند کمپیوتر یا هارد دیسک است، در حالی که ذخیره‌سازی دور یا ابری (Remote/Cloud Storage) به معنی نگهداری دیتا در سرورهای آنلاین است که از طریق اینترنت قابل دسترسی می‌باشد. در سال‌های اخیر، استفاده از ذخیره‌سازی ابری افزایش یافته است، زیرا دسترسی آسان‌تری فراهم می‌کند. برای مثال، ذخیره فایل در هارد کمپیوتر یک نوع Local است، اما ذخیره آن در Google Drive یک نوع Cloud محسوب می‌شود.

انواع وسایل ذخیره‌سازی

وسایل مختلفی برای ذخیره دیتا وجود دارد که هرکدام ویژگی خاص دارند. هارد دیسک (HDD) ظرفیت زیاد دارد اما سرعت آن نسبتاً کم است، در حالی که SSD سرعت بسیار بالا دارد اما قیمت آن بیشتر است. همچنان Tape Drive برای ذخیره‌سازی طولانی‌مدت استفاده می‌شود. برای مثال، یک کمپیوتر جدید معمولاً از SSD برای سرعت بهتر استفاده می‌کند.

نوت: معلومات کلی در مورد حافظه ها و تفاوت های آنها در سطح 1 شما اطلاعات کامل را مطالعه نمودید.

هزینه‌ها(Cost)

هزینه ذخیره‌سازی یکی از عوامل مهم در انتخاب نوع آن است. ذخیره‌سازی محلی نیاز به خرید دستگاه دارد، اما بعد از آن هزینه اضافی کم است. در مقابل، ذخیره‌سازی ابری معمولاً به‌صورت اشتراک ماهانه یا سالانه است. برای مثال، خرید یک هارد دیسک یک‌بار هزینه دارد، اما استفاده از فضای ابری ممکن است هر ماه هزینه داشته باشد.

سرعت دسترسی و انتقال

در ذخیره‌سازی محلی، سرعت دسترسی معمولاً بالا است زیرا دیتا مستقیماً از دستگاه خوانده می‌شود. اما در ذخیره‌سازی ابری، سرعت بستگی به اینترنت دارد. اگر اینترنت ضعیف باشد، دسترسی به دیتا کند می‌شود. برای مثال، باز کردن یک فایل از کمپیوتر سریع‌تر از دانلود آن از اینترنت است.

امنیت و محافظت دیتا(Encryption)

برای محافظت از دیتا، از روش‌های امنیتی مانند رمزگذاری (Encryption) استفاده می‌شود. در این روش، دیتا به شکل رمز تبدیل می‌شود تا افراد غیرمجاز نتوانند آن را بخوانند. وقتی دوباره به حالت اصلی برگردد، به آن Decryption گفته می‌شود. برای مثال، وقتی شما رمز عبور برای فایل یا حساب خود تعیین می‌کنید، این یک نوع محافظت از دیتا است.

تفاوت ها Local Server vs Cloud

سرور محلی در داخل یک اداره یا سازمان قرار دارد و کنترول کامل در دست خودشان است، اما Cloud توسط شرکت‌های بزرگ مدیریت می‌شود و دسترسی از هرجا ممکن است. برای مثال، یک مکتب ممکن است سرور داخلی داشته باشد، اما از Google Drive برای ذخیره آنلاین هم استفاده کند.

محافظت از دیتا RAiD[1] (Research Activity Identifier)

RAID یک روش برای نگهداری دیتا در چند هارد دیسک است تا در صورت خراب شدن یکی، دیتا از بین نرود. این روش برای افزایش امنیت و اطمینان استفاده می‌شود. برای مثال، در شرکت‌ها از چند هارد استفاده می‌شود تا اگر یکی خراب شد، دیتا محفوظ بماند.

مثال عملی

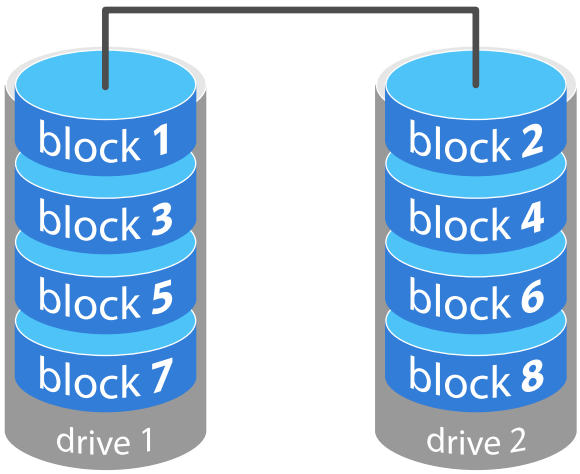
دانش آموزان می‌توانند:

[1] For More information (**Topic**)

- یک فایل را در کمپیوتر ذخیره کنند(Local)
- همان فایل را در Cloud آپلود کنند

سپس سرعت، دسترسی و تفاوت را مقایسه کنند.

این تکنالوژی معمولاً در شرکت ها که دیتا بسیار ارزشمند داشته باشند استفاده میشود. دلیلش این است که ما و شما دیتاها که در گوگل درایف، درایف مایکروساتف ذخیره میکنم و هرگز حذف نمیشود میتواند استفاده همین تکنالوژی در سرورهای این شرکت ها باشد.



RAiD (Research Activity Identifier)

جدول مقایسهLocal vs Remote

ویژگی	Local Storage	Remote / Cloud Storage
محل ذخیره	دستگاه شخصی	اینترنت / سرور
دسترسی	فقط همان دستگاه	از هرجا
سرعت	سریع	وابسته به اینترنت
هزینه	یک‌بار	اشتراک
امنیت	در دست کاربر	وابسته به شرکت
خطر از دست رفتن	در صورت خرابی دستگاه	کمتر (Backup دارد)

جدول انواع ذخیره‌سازی

نوع	ویژگی	مثال
HDD	ظرفیت زیاد، سرعت کم	هارد قدیمی
SSD	سرعت بالا، قیمت بیشتر	لپ‌تاپ جدید
Tape	ذخیره طولانی	آرشیف شرکت
RAID	محافظت دیتا	سرور شرکت

پیشنهاد دادن سیستم ذخیره‌سازی(Storage Recommendation)

دانش آموزان باید بتوانند با استفاده از دانشی که دارند، بهترین نوع ذخیره‌سازی را برای یک کار یا پروژه انتخاب کنند. این انتخاب بستگی به نیاز، مقدار دیتا، بودجه و نوع استفاده دارد. یعنی همیشه یک راه‌حل ثابت وجود ندارد، بلکه باید شرایط بررسی شود. برای مثال، یک شرکت کوچک ممکن است به Cloud نیاز داشته باشد، اما یک اداره بزرگ ممکن است از سرور محلی استفاده کند.

شناخت نیازها(Requirements)

برای انتخاب درست، ابتدا باید نیازها مشخص شود. این کار می‌تواند از طریق پرسیدن سوال، مصاحبه یا دیدن محل انجام شود. باید بدانیم:

- چه مقدار دیتا وجود دارد
- چند نفر استفاده می‌کنند
- امنیت چقدر مهم است

برای مثال، اگر یک مکتب فقط فایل‌های درسی ذخیره می‌کند، نیاز آن ساده است، اما یک بانک نیاز به امنیت بسیار بالا دارد.

آینده‌نگری(Future Proofing)

در انتخاب ذخیره‌سازی باید آینده را نیز در نظر گرفت. اگر امروز مقدار دیتا کم است، ممکن است در آینده زیاد شود. بنابراین باید سیستمی انتخاب شود که قابل گسترش باشد. برای مثال، اگر یک شرکت اکنون 500 GBدیتا دارد، باید سیستمی انتخاب کند که در چند سال آینده بتواند چند ترابایت دیتا را نیز ذخیره کند.

هزینه کلی(TCO)

هزینه فقط خرید اولیه نیست، بلکه باید تمام هزینه‌ها در نظر گرفته شود، مانند:

- نگهداری
- برق
- ارتقا

برای مثال، خرید یک سرور محلی شاید ارزان به نظر برسد، اما هزینه برق و نگهداری آن در طول زمان زیاد می‌شود، در حالی که Cloud ممکن است هزینه ماهانه داشته باشد.

مقایسه انواع ذخیره‌سازی

انواع ذخیره‌سازی مانند HDD و SSD هرکدام مزایا و معایب دارند .HDD ارزان‌تر و دارای ظرفیت بیشتر است، اما سرعت آن کم‌تر است SSD .سریع‌تر است، اما قیمت بالاتر دارد. برای مثال، برای کارهای سریع مانند اجرای برنامه‌ها، SSDبهتر است.

Cloud یا Local ؟

انتخاب بین Cloud و Local بسیار مهم است Cloud .دسترسی آسان از هرجا را فراهم می‌کند، اما نیاز به اینترنت دارد Local .سرعت بالا دارد و کنترول کامل در دست کاربر است، اما در صورت خرابی دستگاه، خطر از بین رفتن دیتا وجود دارد. برای مثال، یک اداره که کارمندان از راه دور کار می‌کنند، Cloud برای آن مناسب‌تر است.

مثال واقعی(Case Study)

فرض کنید یک مؤسسه خیریه می‌خواهد سیستم خود را به Cloud انتقال دهد.

دانش آموز باید:

- نیازهای آن را بررسی کند (حجم دیتا، تعداد کارمندان)
- هزینه‌ها را مقایسه کند
- امنیت را در نظر بگیرد
- پیشنهاد بدهد که Cloud مناسب است یاLocal

نتیجه: اگر دسترسی از راه دور مهم باشد Cloud → بهتر است

جدول راهنمای انتخاب ذخیره‌سازی

شرایط	بهترین انتخاب	دلیل
دسترسی از هرجا	Cloud	آنلاین است
سرعت بالا	Local / SSD	سریع‌تر
هزینه کم اولیه	Cloud	نیاز به خرید ندارد
کنترول کامل	Local	در دست خود
رشد آینده	Cloud	قابل گسترش
امنیت بسیار بالا	Local + Backup	کنترول بیشتر

جدول مقایسه سرعت و ظرفیت

نوع	مزایا	معایب	مثال
HDD	ارزان، ظرفیت زیاد	سرعت کم	آرشیف
SSD	سریع	قیمت بالا	لپ‌تاپ
Local	کنترول کامل	خطر خرابی	کمپیوتر
Cloud	دسترسی آسان	وابسته به اینترنت	Google Drive

2. برنامه‌ریزی، ایجاد و مدیریت مواد دیجیتلی

امروزه ساختن و شریک‌سازی مواد دیجیتلی بسیار آسان شده است. افراد می‌توانند به‌سادگی عکس، ویدیو، بلاگ و سایر محتواها را ایجاد کرده و در شبکه‌های اجتماعی نشر کنند. اما این آسانی باعث شده که بعضی افراد بدون فکر کردن محتوا نشر کنند که ممکن است پیام نادرست یا مشکل‌ساز داشته باشد. بنابراین، قبل از نشر هر محتوا باید فکر شود که این معلومات چه تأثیری بر دیگران دارد. برای مثال، اگر یک دانش آموز یک پُست نامناسب نشر کند، ممکن است اعتبار او در آینده آسیب ببیند.

اهمیت برنامه‌ریزی قبل از ایجاد محتوا

قبل از ساختن مواد دیجیتلی باید برنامه‌ریزی صورت گیرد تا محتوا هدف مشخص داشته باشد. باید مشخص شود:

- مخاطب کیست
- هدف چیست
- چه نوع محتوا مناسب است

اگر بدون برنامه‌ریزی کار شود، ممکن است پیام درست منتقل نشود. برای مثال، اگر یک ویدیو آموزشی بدون ترتیب ساخته شود، دانش آموزان آن را درست درک نمی‌کنند.

مدیریت مواد دیجیتلی

بعد از ایجاد محتوا، باید آن را به‌صورت درست مدیریت کرد. این شامل:

- ذخیره‌سازی مناسب
- نام‌گذاری درست
- شریک‌سازی کنترل‌شده

اگر مدیریت درست نباشد، محتوا گم می‌شود یا به‌صورت نادرست استفاده می‌شود. برای مثال، اگر فایل‌ها بدون نام درست ذخیره شوند، پیدا کردن آن‌ها مشکل می‌شود.

کار گروهی با استفاده ازCloud

خدمات Cloud این امکان را فراهم کرده که افراد از مکان‌های مختلف با هم کار کنند. این موضوع باعث شده که همکاری سریع‌تر و آسان‌تر شود. برای مثال، چند دانش آموز می‌توانند روی یک پروژه در Google Doce به‌صورت همزمان کار کنند.

مزایا استفاده ازCloud

استفاده از Cloud مزایای زیادی دارد، مانند:

- دسترسی از هرجا
- کار گروهی آسان

- ذخیره‌سازی امن‌تر

برای مثال، یک دانش آموز می‌تواند از خانه یا مکتب به فایل‌های خود دسترسی داشته باشد.

مشکلات و چالش‌ها

با وجود مزایا، Cloud بعضی مشکلات نیز دارد:

- وابسته بودن به اینترنت
- خطرات امنیتی
- امکان نشر معلومات نادرست

برای مثال، اگر اینترنت قطع شود، دسترسی به فایل‌ها ممکن نیست یا اگر تنظیمات امنیتی ضعیف باشد، دیگران می‌توانند به دیتا دسترسی پیدا کنند.

جدول مقایسه مزایا و مشکلات

بخش	مزایا	مشکلات
ایجاد محتوا	آسان و سریع	احتمال اشتباه
اشتراک‌گذاری	دسترسی وسیع	نشر معلومات نادرست
Cloud	همکاری آسان	نیاز به اینترنت
مدیریت	نظم بهتر	نیاز به مهارت

دانش آموزان عزیز شما در فصل اول در مورد این بخش جزئیات فشرده را کسب نموده در این فصل جزئیات بیشتر برایتان ارائه شد. در کنار این معلومات اشتراگ گذاری فایل و تمرین بصورت عملی نیز شامل این بسته آموزشی میشود.

ایجاد اشکال مختلف معلومات دیجیتلی برای هدف مشخص

دانش آموزان باید بتوانند انواع مختلف معلومات دیجیتلی را بر اساس هدف مشخص ایجاد کنند. این به این معنی است که هر نوع محتوا باید مطابق نیاز و نوع مخاطب ساخته شود. مثلاً اگر هدف آموزش باشد، استفاده از پریزنتیشن یا ویدیو مناسب است، اما اگر هدف ذخیره معلومات باشد، دیتابیس یا Spreadsheet بهتر است. همچنان دانش آموزان باید در ساخت محتوا به نحوه نمایش(Layout) ، شکل (Form) و تأثیرگذاری (Impact) توجه کنند تا پیام به‌صورت واضح و مؤثر منتقل شود.

- در برنامه اسناد مانند Word
- برنامه محسابه مانند اکسل و گوگل شیت
- برنامه های دیزاین مانند فتوشاب و کانوا
- برنامه سلاید مانند PowerPoint و Google Solid

- و سایر ابزارهای دیجتیالی شما میتوانید قوانین که برای مخاطب تأثیرگذار باشد را رعایت کند.

انواع مواد دیجیتلی

دانش آموزان باید با انواع مختلف مواد دیجیتلی کار کنند و بتوانند هرکدام را در جای مناسب استفاده نمایند. این مواد شامل اسناد(Documents) ، صفحات ویب(Web Pages) ، پادکست‌ها(Podcasts) ، ویدیوها، پریزنتیشن‌ها، Spreadsheets و دیتابیس‌ها می‌باشد. هرکدام از این ابزارها برای هدف خاصی استفاده می‌شود. برای مثال، یک Spreadsheets برای محاسبه اعداد مناسب است، در حالی که یک ویدیو برای توضیح یک موضوع به‌صورت بصری بهتر عمل می‌کند.

ارزیابی مواد دیجیتلی

دانش آموزان نه تنها باید محتوا ایجاد کنند، بلکه باید بتوانند آن را ارزیابی نیز نمایند. این ارزیابی شامل بررسی این است که:

- آیا محتوا هدف خود را برآورده کرده است
- از چه ابزار و فرمت استفاده شده است
- آیا برای مخاطب مناسب است یا نه

برای مثال، اگر یک دانش آموز یک پریزنتیشن بسازد، باید بررسی کند که آیا اسلایدها واضح هستند و پیام را به‌خوبی منتقل می‌کنند یا خیر.

استفاده در سایر مضامین

بسیاری از این مواد دیجیتلی در سایر مضامین درسی نیز استفاده می‌شود. دانش آموزان می‌توانند مهارت‌های IT خود را در مضامین دیگر به‌کار ببرند و کیفیت کار خود را بهتر بسازند. همچنان می‌توانند مواد دیجیتلی شرکت‌ها یا سازمان‌های محلی را بررسی کرده و از آن‌ها یاد بگیرند. برای مثال، بررسی یک ویب‌سایت شرکت می‌تواند به دانش آموز کمک کند تا نحوه طراحی و ارائه معلومات را بهتر درک کند.

ساخت پورتفولیو دیجیتلی(Electronic Portfolio)

تمام این کارها و پروژه‌ها می‌تواند در یک پورتفولیو دیجیتلی جمع‌آوری شود. این پورتفولیو نشان‌دهنده مهارت‌ها و توانایی‌های دانش آموز است و می‌تواند در پروژه‌های بزرگ‌تر یا حتی در آینده شغلی بسیار مفید باشد. برای مثال، یک دانش آموز می‌تواند تمام پروژه‌های خود را در یک فولدر یا ویب‌سایت ذخیره کند و به دیگران نشان دهد.

خلاصه موضوعات

موضوع	توضیح کوتاه	مثال
ایجاد محتوا	ساخت مواد بر اساس هدف	پریزنتیشن آموزشی
انواع مواد	ابزارهای مختلف دیجیتلی	ویدیو، ویب‌سایت
ارزیابی	بررسی کیفیت محتوا	وضاحت اسلایدها
استفاده در مضامین	کاربرد در سایر درس‌ها	پروژه علمی
پورتفولیو	جمع‌آوری کارها	فولدر پروژه‌ها

تشریح فرمت فایل‌ها و استانداردهای مورد نیاز

دانش آموزان باید بتوانند فرمت‌های مختلف فایل را بشناسند و بدانند که برای هر نوع کار کدام فرمت مناسب‌تر است. هر فایل دیجیتلی در یک فرمت خاص ذخیره می‌شود و این فرمت تعیین می‌کند که فایل چگونه باز شود، چه امکاناتی داشته باشد و در کدام برنامه‌ها قابل استفاده باشد. برای مثال، فایل‌های docx. برای نوشتن اسناد استفاده می‌شود، در حالی که pdf. برای خواندن و شریک‌سازی مناسب‌تر است.

تفاوت استانداردهای باز و بسته

فرمت‌های فایل به دو نوع تقسیم می‌شوند: استانداردهای باز (Open) و استانداردهای بسته یا اختصاصی .(Proprietary) فرمت‌های باز برای همه قابل استفاده هستند و در برنامه‌های مختلف باز می‌شوند، اما فرمت‌های بسته معمولاً مربوط به یک نرم‌افزار خاص هستند و ممکن است در برنامه‌های دیگر به‌خوبی کار نکنند. برای مثال، فایل odt. یک فرمت باز است، اما docx. بیشتر مربوط به یک نرم‌افزار خاص می‌باشد.

اهمیت انتخاب فرمت مناسب

انتخاب فرمت مناسب بسیار مهم است، زیرا این انتخاب بر نحوه استفاده، شریک‌سازی و ذخیره فایل تأثیر دارد. اگر فرمت درست انتخاب نشود، ممکن است دیگران نتوانند فایل را باز کنند یا اطلاعات آن به‌درستی نمایش داده نشود. برای مثال، اگر یک پروژه را به‌صورت PDF ذخیره کنید، همه می‌توانند آن را ببینند، اما اگر به‌صورت یک فرمت خاص باشد، ممکن است نیاز به نرم‌افزار خاص داشته باشد.

مزایا و محدودیت‌های استانداردهای باز:
استانداردهای باز مزایای زیادی دارند، مانند:

- قابل استفاده در برنامه‌های مختلف
- مناسب برای شریک‌سازی

اما ممکن است بعضی امکانات پیشرفته را نداشته باشند. برای مثال، یک فایل csv. ساده است و در همه برنامه‌ها باز می‌شود، اما امکانات پیشرفته Excel را ندارد.

ارتباط با پروژه عملی
دانش آموزان باید بتوانند بر اساس نیاز پروژه خود، فرمت مناسب را انتخاب کنند. این کار نشان می‌دهد که آن‌ها درک درستی از کاربرد فرمت‌ها دارند. برای مثال، در یک پروژه تحقیقاتی، استفاده از PDF برای ارائه نهایی مناسب است، اما برای تحلیل داده‌ها استفاده از xlsx. بهتر است.

جدول مقایسه فرمت‌ها

نوع فرمت	ویژگی	مثال	کاربرد
Open Standard	آزاد و قابل استفاده	.odt, .csv	شریک‌سازی
Proprietary	وابسته به نرم‌افزار	.docx, .psd	کار تخصصی

جدول انتخاب فرمت مناسب

نوع کار	فرمت مناسب	دلیل
نوشتن متن	.docx / .odt	ویرایش آسان
ارائه	.pdf	نمایش ثابت
محاسبه	.xlsx / .csv	کار با اعداد
تصویر	.png / .jpg	نمایش تصویر

وارد کردن (Import) و صادر کردن (Export) مواد دیجیتلی
دانش آموزان باید بتوانند فایل‌ها را از یک برنامه به برنامه دیگر وارد (Import) و صادر (Export) کنند. این کار باعث می‌شود که بتوانند از دیتا در نرم‌افزارهای مختلف استفاده کنند Import یعنی آوردن فایل به داخل یک برنامه و Export یعنی ذخیره کردن فایل در یک فرمت دیگر برای استفاده در جای دیگر. برای مثال، یک دانش آموز می‌تواند یک فایل Excel را به PDF تبدیل کند تا دیگران بتوانند آن را بدون تغییر ببینند.

انتخاب فرمت مناسب در Import وExport

انتخاب فرمت مناسب بسیار مهم است، زیرا هر فرمت برای هدف خاصی مناسب است. اگر فرمت اشتباه انتخاب شود، ممکن است دیتا از بین برود یا به‌درستی نمایش داده نشود. دانش آموزان باید بدانند که در هر مرحله از کار، کدام فرمت بهتر است. برای مثال، برای شریک‌سازی ساده از PDF استفاده می‌شود، اما برای ویرایش از DOCX یا XLSX استفاده می‌شود.

ترکیب (Merge) مواد دیجیتلی

دانش آموزان باید بتوانند چند نوع دیتا را با هم ترکیب کنند و یک نتیجه نهایی بسازند. این کار در پروژه‌ها بسیار مهم است، زیرا معمولاً اطلاعات از منابع مختلف جمع‌آوری می‌شود. برای مثال، یک دانش آموز می‌تواند متن، تصویر و نمودار را در یک پریزنتیشن یا گزارش ترکیب کند.

درک چرخه کامل دیتا(Lifecycle)

دانش آموزان باید درک کنند که دیتا از ایجاد تا استفاده نهایی چند مرحله دارد:

- ایجاد
- ویرایش
- ذخیره
- شریک‌سازی

این درک کمک می‌کند تا در هر مرحله بهترین تصمیم گرفته شود. برای مثال، در مرحله اول ممکن است از یک فرمت قابل ویرایش استفاده شود، اما در مرحله آخر از PDF برای ارائه استفاده گردد.

اهمیت فرمت‌های انعطاف‌پذیر مانند (SVG)

بعضی فرمت‌ها مانند SVG قابلیت ویرایش بیشتر دارند و برای کارهای طراحی مناسب‌تر هستند. این فرمت‌ها اجازه می‌دهند که تصویر بدون از دست دادن کیفیت تغییر داده شود. برای مثال، یک لوگو اگر به‌صورت SVG باشد، می‌توان آن را به هر اندازه تغییر داد بدون اینکه کیفیت آن کم شود.

همکاری و استفاده از استانداردهای باز

در کارهای گروهی، استفاده از فرمت‌های باز بسیار مهم است، زیرا همه افراد می‌توانند بدون مشکل به فایل‌ها دسترسی داشته باشند. اگر از فرمت‌های بسته استفاده شود، ممکن است دیگران مجبور شوند نرم‌افزار خاصی نصب کنند. برای مثال، استفاده از فرمت PDF یا CSV در کار گروهی آسان‌تر از فرمت‌های خاص است.

جدول مقایسه Import / Export / Merge

عملیه	توضیح	مثال
Import	وارد کردن فایل	آوردن عکس به Word
Export	تبدیل و ذخیره	تبدیل Excel به PDF
Merge	ترکیب چند فایل	ساخت پریزنتیشن

جدول انتخاب فرمت در مراحل کار

مرحله	فرمت مناسب	دلیل
ایجاد	.psd / .docx	قابل ویرایش
ویرایش	.xlsx / .svg	انعطاف بیشتر
اشتراک	.csv / .pdf	سازگاری بالا
نهایی	.pdf	ثابت و قابل نمایش

همکاری در پروژه‌های معلومات دیجیتلی

دانش آموزان باید بتوانند در پروژه‌های دیجیتلی با دیگران همکاری کنند. کار گروهی به این معنی است که چند نفر با هم یک هدف مشترک را دنبال کنند و هرکدام نقش مشخص داشته باشند. در دنیای امروز، بسیاری از کارها به‌صورت گروهی انجام می‌شود، مخصوصاً با استفاده از ابزارهای دیجیتلی. برای مثال، چند دانش آموز می‌توانند روی یک پروژه درسی به‌صورت مشترک کار کنند و هرکدام یک بخش آن را آماده نمایند.

اهمیت مهارت‌های نرم(Soft Skills)

کار گروهی فقط به مهارت تخنیکی نیاز ندارد، بلکه مهارت‌های رفتاری نیز بسیار مهم است. دانش آموزان باید یاد بگیرند که چگونه با دیگران به‌صورت درست برخورد کنند. این مهارت‌ها شامل ادب، احترام، درک دیگران و همکاری است. بدون این مهارت‌ها، حتی اگر کار تخنیکی خوب باشد، پروژه موفق نمی‌شود.

رفتار مناسب در کار گروهی

در همکاری باید چند اصل مهم رعایت شود. ادب و احترام باعث می‌شود محیط کار دوستانه باشد. قدردانی از کار دیگران باعث انگیزه می‌شود. همچنان باید نظر اصلاحی داده شود، نه انتقاد منفی. درک تفاوت‌ها نیز مهم است، زیرا افراد از نظر زبان، فرهنگ و شخصیت با هم فرق دارند. برای مثال، اگر یکی از اعضای گروه اشتباه کند، به‌جای سرزنش باید راه درست نشان داده شود.

استفاده از ابزارهای دیجیتلی برای همکاری

ابزارهای دیجیتلی مانند Cloud این امکان را فراهم می‌کنند که افراد از مکان‌های مختلف با هم کار کنند. این ابزارها کمک می‌کنند تا فایل‌ها شریک شود، تغییرات ثبت شود و همه اعضا بتوانند مشارکت داشته باشند. برای مثال، استفاده از Google Docs باعث می‌شود چند نفر همزمان روی یک سند کار کنند.

مثال واقعی

فرض کنید یک گروه دانش آموزان باید یک پروژه پریزنتیشن آماده کنند:

- یک نفر تحقیق می‌کند
- یک نفر اسلاید می‌سازد
- یک نفر طراحی را انجام می‌دهد

اگر این افراد با احترام و همکاری کار کنند، پروژه موفق می‌شود، اما اگر همکاری نداشته باشند، نتیجه ضعیف خواهد بود.

جدول مهارت‌های همکاری

مهارت	توضیح	مثال
ادب	برخورد محترمانه	صحبت آرام
قدردانی	تشکر از دیگران	گفتن "تشکر"
نظر اصلاحی	کمک به بهبود	پیشنهاد دادن
درک تفاوت‌ها	احترام به دیگران	پذیرش نظر متفاوت

تنظیم معلومات دیجیتلی مشترک برای همکاری بهتر

دانش آموزان باید بتوانند معلومات دیجیتلی مشترک را به‌گونه‌ای تنظیم کنند که کار گروهی آسان‌تر و مؤثرتر شود. وقتی چند نفر روی یک پروژه کار می‌کنند، اگر فایل‌ها منظم نباشد، باعث سردرگمی و اتلاف وقت می‌شود. بنابراین، تنظیم درست فایل‌ها و ساختار مناسب بسیار مهم است. برای مثال، اگر یک گروه تمام فایل‌ها را در یک فولدر نامشخص ذخیره کند، پیدا کردن آن مشکل می‌شود، اما اگر فولدرها بر اساس موضوع یا بخش پروژه ساخته شود، کار بسیار آسان می‌شود.

اهمیت نام‌گذاری واضح فایل‌ها

نام‌گذاری درست فایل‌ها باعث می‌شود که اعضای گروه به‌راحتی فایل مورد نظر خود را پیدا کنند. نام‌ها باید واضح، کوتاه و قابل فهم باشد. اگر نام فایل‌ها مبهم باشد، افراد نمی‌دانند کدام فایل جدید یا مهم است. برای مثال، به‌جای "file1" بهتر است از "Report_Final" استفاده شود.

ساختار منظم فولدرها

ایجاد یک ساختار منظم از فولدرها باعث می‌شود که پروژه به‌صورت منظم پیش برود. هر بخش پروژه باید فولدر جدا داشته باشد تا فایل‌ها به‌درستی دسته‌بندی شوند. برای مثال:

- فولدر تحقیق
- فولدر تصاویر
- فولدر پریزنتیشن

این کار باعث می‌شود هر عضو گروه سریع به بخش خود دسترسی داشته باشد.

استفاده از کامنت‌ها(Comments)

در پروژه‌های بزرگ، استفاده از کامنت‌ها بسیار مهم است. اعضای گروه می‌توانند توضیحات یا پیشنهادات خود را در داخل فایل بنویسند تا دیگران آن را ببینند. این کار باعث می‌شود ارتباط بهتر شود و اشتباهات کاهش یابد. برای مثال، یک دانش آموز می‌تواند در کنار متن بنویسد: "این بخش نیاز به اصلاح دارد."

افزایش سرعت و کارایی(Efficiency)

وقتی معلومات دیجیتلی به‌صورت درست تنظیم شود:

- وقت ضایع نمی‌شود
- کار سریع‌تر انجام می‌شود
- همکاری بهتر می‌شود

برای مثال، در یک پروژه گروهی اگر همه فایل‌ها منظم باشد، اعضا می‌توانند بدون مشکل کار خود را ادامه دهند.

مثال واقعی

فرض کنید یک گروه دانش آموزان پروژه دارند:
اگر:

- فایل‌ها نام درست نداشته باشد
- فولدرها منظم نباشد

اعضا گیج می‌شوند
اما اگر:

- فولدرها دسته‌بندی شود
- فایل‌ها واضح نام‌گذاری شود

کار سریع و آسان انجام می‌شود.

جدول نکات مهم برای تنظیم دیتا

بخش	کار درست	مثال
نام فایل	واضح و مشخص	Report_Final
فولدر	دسته‌بندی منظم	Images / Docs
کامنت	توضیح برای دیگران	اصلاح این بخش
نظم کلی	ساختار واضح	پروژه منظم

تعیین سطح دسترسی و اجازه‌ها(Permissions & Access Rights)

در کارهای گروهی دیجیتلی، بسیار مهم است که مشخص شود چه کسی به کدام فایل یا معلومات دسترسی دارد و چه کاری می‌تواند انجام دهد. به این موضوع "Permissions" یا سطح دسترسی گفته می‌شود. اگر این دسترسی‌ها درست تنظیم نشود، ممکن است بعضی افراد نتوانند کار کنند یا برعکس، افراد غیرمجاز تغییرات ایجاد کنند. برای مثال، اگر همه اعضا اجازه ویرایش داشته باشند، ممکن است فایل به‌اشتباه تغییر کند.

انواع سطح دسترسی در سیستم‌های دیجیتلی

در سیستم‌های مختلف مانند (Cloud) یا سرورهای محلی، سطوح مختلفی از دسترسی وجود دارد. این سطوح مشخص می‌کنند که کاربر فقط مشاهده کند یا بتواند تغییر هم بدهد. مهم‌ترین این سطوح عبارت‌اند از:

- **فقط دیدن Read Only:** کاربر فقط می‌تواند فایل را ببیند
- **ساختن فایل ها Write:** کاربر می‌تواند محتوا اضافه یا تغییر دهد
- **نظر دادن Comments:** کاربر می‌تواند نظر بدهد بدون تغییر اصلی
- **ویرایش Edite:** کاربر می‌تواند تغییر کامل ایجاد کند
- **کنترول کامل Full Control :** کاربر همه صلاحیت‌ها را دارد

اهمیت استفاده درست از دسترسی‌ها

تنظیم درست این سطوح باعث می‌شود:

- امنیت دیتا حفظ شود
- از اشتباهات جلوگیری شود
- هر فرد فقط در بخش مربوط به خود کار کند

برای مثال، اگر یک دانش آموز به اشتباه Full Control داشته باشد، ممکن است فایل مهم را حذف کند.

استفاده در سیستم‌های واقعی

در سیستم‌هایی مانند Google Drive یا شبکه‌های داخلی، این سطوح به‌صورت عملی استفاده می‌شود. دانش آموزان باید بتوانند این دسترسی‌ها را تنظیم کنند. برای مثال:

- استاد → فقط مشاهده(Read Only)
- دانش آموزان → ویرایش(Edit)

مثال واقعی

فرض کنید یک پروژه صنفی دارید:

- مدیر گروه → Full Control
- اعضا → Write / Edite
- سایر دانش آموزان → Read-Only

این کار باعث نظم و امنیت پروژه می‌شود

جدول کامل سطوح دسترسی

سطح دسترسی	توانایی‌ها	مزایا	محدودیت	مثال
Read Only	فقط مشاهده	امنیت بالا	بدون تغییر	دیدن گزارش
Comment	نظر دادن	همکاری بهتر	بدون تغییر مستقیم	پیشنهاد اصلاح
Write	اضافه کردن محتوا	کار گروهی	امکان اشتباه	نوشتن متن
Edit	ویرایش کامل	انعطاف بالا	خطر تغییر اشتباه	تغییر فایل
Full Control	کنترول کامل (حذف، تغییر، تنظیم دسترسی)	مدیریت کامل	خطر بالا اگر اشتباه باشد	مدیر پروژه

جدول انتخاب سطح دسترسی

نقش	سطح مناسب	دلیل
مدیر	Full Control	کنترول کامل
اعضای اصلی	Edit / Write	انجام کار
بازبین	Comment	اصلاح
دیگران	Read Only	جلوگیری از تغییر

انتخاب بهترین فرمت فایل برای یک پروژه

در هر پروژه دیجیتلی، انتخاب فرمت مناسب فایل بسیار مهم است، زیرا این انتخاب بر کیفیت، سرعت، اندازه فایل و قابلیت استفاده تأثیر مستقیم دارد. دانش آموزان باید بتوانند توضیح بدهند که چرا یک فرمت خاص را انتخاب کرده‌اند و این انتخاب چگونه نیاز پروژه را برآورده می‌کند. یعنی فقط انتخاب کافی نیست، بلکه باید دلیل آن هم واضح باشد. برای مثال، انتخاب PDF برای یک گزارش نهایی به این دلیل است که شکل فایل تغییر نمی‌کند.

در نظر گرفتن نیاز پروژه

قبل از انتخاب فرمت، باید نیاز پروژه مشخص شود. بعضی پروژه‌ها نیاز به کیفیت بالا دارند، بعضی به حجم کم، و بعضی به قابلیت ویرایش. این نیازها تعیین می‌کند که کدام فرمت مناسب‌تر است. برای مثال، اگر هدف اشتراک‌گذاری آسان باشد، فرمت سبک مانند PDF یا JPG مناسب است، اما اگر هدف ویرایش باشد، DOCXیا PSD بهتر است.

نقش Data Rate و حجم فایل

Data Rate (میزان انتقال دیتا) و حجم فایل از عوامل مهم در انتخاب فرمت است. فایل‌های با کیفیت بالا معمولاً حجم بیشتری دارند و انتقال آن‌ها زمان‌بر است. بنابراین گاهی لازم است بین کیفیت و حجم تعادل ایجاد شود. برای مثال، یک ویدیو با کیفیت بالا حجم زیادی دارد، اما اگر فشرده شود (MP4)، حجم کم می‌شود ولی ممکن است کیفیت کمی کاهش یابد.

انعطاف‌پذیری(Flexibility)

بعضی فرمت‌ها انعطاف‌پذیرتر هستند و امکان ویرایش بیشتری دارند. این نوع فرمت‌ها برای مراحل اولیه پروژه مناسب هستند. اما در مرحله نهایی، معمولاً از فرمت‌هایی استفاده می‌شود که ثابت باشند. برای مثال، فایل SVG برای طراحی بسیار انعطاف‌پذیر است، اما JPG انعطاف کم دارد.

سازش (Compromise) در انتخاب فرمت

در بعضی موارد، دانش آموزان مجبور می‌شوند بین چند گزینه یکی را انتخاب کنند و در یک بخش سازش انجام دهند. یعنی ممکن است کیفیت را کمی کاهش دهند تا حجم فایل کم شود یا برعکس. این تصمیم بستگی به هدف پروژه دارد. برای مثال:

- کیفیت بالا → حجم زیاد
- حجم کم → کیفیت کمتر

مثال واقعی

فرض کنید یک دانش آموز باید یک پروژه ویدیویی آماده کند:

- اگر کیفیت مهم باشد → استفاده از فرمت با کیفیت بالا

- اگر اشتراک‌گذاری مهم باشد → استفاده ازMP4

در اینجا دانش آموز باید توضیح بدهد که چرا این انتخاب را کرده است.

جدول انتخاب فرمت بر اساس نیاز

نیاز پروژه	فرمت مناسب	دلیل
گزارش نهایی	.pdf	نمایش ثابت
ویرایش متن	.docx	قابل تغییر
تصویر وب	.jpg / .png	حجم کم
طراحی	.svg / .psd	انعطاف بالا
ویدیو	.mp4	تعادل کیفیت و حجم

جدول مقایسه ویژگی‌ها

ویژگی	کیفیت بالا	حجم کم	انعطاف
PDF	متوسط	کم	کم
DOCX	متوسط	متوسط	زیاد
JPG	متوسط	کم	کم
SVG	بالا	کم	زیاد
MP4	متوسط/بالا	متوسط	کم

چرا یک نوع فایل در شرایط خاص مناسب‌تر است؟

در پروژه‌های دیجیتلی، همیشه یک فرمت فایل بهتر از بقیه نیست، بلکه هر فرمت در یک شرایط خاص مناسب‌تر است. دانش آموزان باید بتوانند توضیح دهند که چرا یک فرمت را انتخاب کرده‌اند و این انتخاب چه مزایا و معایبی دارد. این یعنی فقط انتخاب مهم نیست، بلکه دلیل انتخاب و تحلیل آن نیز اهمیت دارد. برای مثال، انتخاب PDF برای ارسال گزارش مناسب است، زیرا شکل فایل تغییر نمی‌کند، اما برای ویرایش مناسب نیست.

وابستگی انتخاب فرمت به شرایط

انتخاب فرمت فایل به شرایط مختلف بستگی دارد، مانند:

- هدف پروژه
- نوع مخاطب

- نوع استفاده (ویرایش یا فقط مشاهده)

برای مثال، اگر هدف چاپ باشد، کیفیت مهم است، اما اگر هدف ارسال آنلاین باشد، حجم کم مهم‌تر است.

تحلیل مزایا و معایب

هر فرمت دارای نقاط قوت و ضعف است و دانش آموزان باید بتوانند این موارد را تشخیص دهند. این تحلیل کمک می‌کند تصمیم بهتر گرفته شود. برای مثال:

- JPG → حجم کم، اما کیفیت پایین‌تر
- PNG → کیفیت بهتر، اما حجم بیشتر

مشکل در انتخاب نرم‌افزار و فرمت

گاهی دانش آموزان با یک نرم‌افزار راحت هستند، اما آن نرم‌افزار فرمت مورد نیاز پروژه را تولید نمی‌کند. در این حالت، باید یاد بگیرند که خود را با شرایط تطبیق دهند. برای مثال، یک دانش آموز ممکن است با یک برنامه طراحی کار کند، اما مشتری فایل SVG یا PDF بخواهد.

اهمیت شناخت فرمت‌های مختلف

هرچه دانش آموزان با فرمت‌های بیشتری آشنا باشند، بهتر می‌توانند تصمیم بگیرند و خود را با نیازهای مختلف تطبیق دهند. این مهارت در آینده کاری بسیار مهم است. برای مثال، یک طراح باید بداند که چه زمانی از PSD استفاده کند و چه زمانی از PNG یا.SVG

مثال واقعی

فرض کنید یک مشتری از شما یک لوگو می‌خواهد:

- برای چاپ → فرمت با کیفیت بالا(SVG)
- برای وب → فرمت سبک(PNG)

دانش آموز باید توضیح بدهد که چرا این انتخاب درست است.

جدول انتخاب فرمت در شرایط مختلف

شرایط	فرمت مناسب	دلیل
ارسال گزارش	.pdf	نمایش ثابت
ویرایش متن	.docx	قابل تغییر
تصویر وب	.jpg / .png	حجم مناسب
طراحی لوگو	.svg	کیفیت بالا

فایل کاری	.psd	قابل ویرایش

جدول مزایا و معایب

فرمت	مزایا	معایب
PDF	ثابت و قابل نمایش	ویرایش سخت
DOCX	قابل ویرایش	تغییر در نمایش
JPG	حجم کم	کیفیت کمتر
PNG	کیفیت بهتر	حجم بیشتر
SVG	انعطاف بالا	نیاز به دانش بیشتر

تحلیل و انتخاب بهترین ابزار برای کار گروهی

در پروژه‌های دیجیتلی، انتخاب ابزار مناسب برای همکاری بسیار مهم است، زیرا این ابزارها تعیین می‌کنند که کار گروهی چقدر سریع، منظم و موفق انجام شود. دانش آموزان باید بتوانند ابزارهای مختلف را بررسی کرده و بر اساس نیاز پروژه بهترین گزینه را انتخاب کنند. یعنی فقط استفاده از ابزار کافی نیست، بلکه باید بتوانند توضیح دهند که چرا آن ابزار را انتخاب کرده‌اند. برای مثال، برای نوشتن مشترک اسناد، ابزارهای آنلاین بهتر از نرم‌افزارهای آفلاین هستند.

معیارهای انتخاب ابزار مناسب

برای انتخاب بهترین ابزار همکاری، باید چند عامل مهم بررسی شود. این عوامل کمک می‌کنند تا ابزار مناسب برای پروژه انتخاب شود:

- **ابزارهای موجود :(Tools)** آیا امکانات کافی دارد؟
- **آسانی استفاده :(Ease of Use)** آیا استفاده از آن ساده است؟
- **قابلیت توسعه :(Add-ons)** آیا می‌توان امکانات جدید اضافه کرد؟
- **تنظیمات :(Customizations)** آیا ظاهر و تنظیمات قابل تغییر است؟
- **خودکارسازی :(Automation)** آیا کارها را خودکار انجام می‌دهد؟
- **همکاری با سیستم‌های دیگر :(Interoperability)** آیا با سایر برنامه‌ها کار می‌کند؟

انواع ابزارهای همکاری

ابزارهای مختلفی برای همکاری وجود دارد که هرکدام برای هدف خاصی مناسب هستند:

- ابزارهای نوشتاری (مانند اسناد آنلاین)
- ابزارهای ویدیویی (برای جلسات آنلاین)
- ابزارهای یادداشت‌برداری
- ابزارهای مدیریت پروژه

برای مثال، یک گروه می‌تواند از یک ابزار برای نوشتن گزارش و از ابزار دیگر برای جلسات آنلاین استفاده کند.

اهمیت انتخاب درست ابزار

اگر ابزار مناسب انتخاب نشود:

- کار کند می‌شود
- ارتباط ضعیف می‌شود
- اشتباهات بیشتر می‌شود

اما اگر ابزار درست انتخاب شود:

- کار سریع‌تر انجام می‌شود
- همکاری بهتر می‌شود
- نتیجه بهتر خواهد بود

مثال واقعی

فرض کنید یک گروه دانش آموزان پروژه دارند:

- برای نوشتن → اسناد آنلاین
- برای جلسه → تماس ویدیویی
- برای مدیریت کار → لیست وظایف

این ترکیب ابزارها باعث موفقیت پروژه می‌شود

جدول ارزیابی ابزارها

معیار	توضیح	اهمیت
Tools	امکانات موجود	بسیار مهم
Ease of Use	ساده بودن	مهم
Add-ons	قابلیت توسعه	متوسط
Customisation	تنظیم ظاهر	متوسط
Automation	انجام خودکار	مهم
Interoperability	سازگاری	بسیار مهم

جدول انتخاب ابزار بر اساس نیاز

نوع کار	ابزار مناسب	دلیل
نوشتن گروهی	اسناد آنلاین	همکاری همزمان
جلسه	ویدیو کنفرانس	ارتباط مستقیم
مدیریت پروژه	ابزار مدیریت کار	نظم بهتر
یادداشت	Note ابزار	ثبت معلومات

تحلیل نقاط قوت و ضعف ابزارهای همکاری

در کارهای گروهی دیجیتلی، استفاده از ابزارهای همکاری بسیار مهم است، اما هر ابزار مزایا و معایب خاص خود را دارد. دانش آموزان باید بتوانند این ابزارها را بررسی کرده و نقاط قوت و ضعف آن‌ها را مشخص کنند. این کار کمک می‌کند تا دیگران نیز بتوانند تصمیم درست بگیرند و ابزار مناسب را انتخاب کنند. برای مثال، یک ابزار ممکن است استفاده آسان داشته باشد، اما امکانات آن محدود باشد.

اهمیت شناخت مزایا و معایب

شناخت نقاط قوت و ضعف باعث می‌شود:

- انتخاب بهتر انجام شود
- مشکلات پیش‌بینی شود
- کار گروهی مؤثرتر گردد

برای مثال، اگر بدانیم یک ابزار نیاز به اینترنت قوی دارد، می‌توانیم از قبل آمادگی داشته باشیم.

نقاط قوت ابزارهای همکاری

ابزارهای همکاری معمولاً مزایای زیادی دارند، مانند:

- امکان کار همزمان چند نفر
- دسترسی از مکان‌های مختلف
- ذخیره خودکار اطلاعات
- افزایش سرعت کار

برای مثال، چند دانش آموز می‌توانند همزمان روی یک سند کار کنند بدون اینکه منتظر هم بمانند.

نقاط ضعف ابزارهای همکاری

در کنار مزایا، این ابزارها مشکلاتی نیز دارند:

- وابسته بودن به اینترنت

- مشکلات امنیتی
- احتمال اشتباه یا حذف معلومات
- نیاز به یادگیری ابزار

برای مثال، اگر اینترنت قطع شود، ممکن است دسترسی به فایل‌ها ممکن نباشد.

مثال واقعی

فرض کنید یک گروه از ابزار آنلاین استفاده می‌کند:

- مزیت: همه همزمان کار می‌کنند
- مشکل: اگر اینترنت ضعیف باشد، کار متوقف می‌شود

دانش آموز باید این موارد را تحلیل و بیان کند

جدول مقایسه ابزارها (نمونه)

نوع ابزار	مزایا	معایب	مثال استفاده
اسناد آنلاین	همکاری همزمان	نیاز اینترنت	نوشتن گزارش
ویدیو کنفرانس	ارتباط مستقیم	مصرف زیاد دیتا	جلسات
مدیریت پروژه	نظم کار	پیچیدگی	تقسیم وظایف
یادداشت آنلاین	ثبت سریع	محدودیت امکانات	یادداشت

منابع:

شماره	نام کتاب	دانلود کتاب
1	Cambridge IGCSE ICT (Coursebook)	دانلود PDF
2		

فصل سوم

حفاظت از پلتفورم‌های دیجیتلی

(و آماده ساختن آن‌ها برای استفاده در آینده)

شرایط بخش سوم:

- **ساعت های درسی:** 25 ساعت
- **ساعت های اصافی:** 3 ساعت
- **مجموع ساعت های درسی:** 28 ساعت

در این فصل خواهی آموخت:

Strand 1

دانش آموزان درک می‌کنند که دیتا ارزش مالی دارد و ممکن است برای اهداف مختلف استفاده یا فروخته شود. همچنان می‌فهمند که معلومات شخصی باید به‌صورت امن نگهداری شود و با روش‌های سخت‌افزاری از دسترسی غیرمجاز جلوگیری گردد.

Strand 2

دانش آموزان می‌آموزند که حفاظت دیتا از خود فرد شروع می‌شود. نشر معلومات در اینترنت خطرناک است و باید از رمزهای قوی، تنظیمات حریم خصوصی و رمزگذاری برای امنیت استفاده شود.

Strand 3

دانش آموزان با تهدیدات مختلف مانند سرقت و تخریب دیتا آشنا می‌شوند و درک می‌کنند که خطرات سایبری چقدر واقعی و نزدیک است.

Strand 4

دانش آموزان می‌فهمند که محافظت از دیتا نیاز به ترکیب ابزارهای مختلف دارد، مانند انتی‌ویروس، فایروال، رمزگذاری و استفاده از رمزهای قوی.

Strand 5

دانش آموزان درک می‌کنند که جرایم سایبری همیشه در حال تغییر و پیشرفت است و باید همیشه آگاه و آماده باشند.

Strand 6

دانش آموزان می‌توانند خطرات آنلاین را تشخیص دهند، مانند ایمیل‌های جعلی(Phishing) ، آزار اینترنتی و سوءاستفاده، و یاد می‌گیرند چگونه از خود محافظت کنند.

1. شناخت خطراتی که هنگام استفاده از معلومات و مواد دیجیتلی در اینترنت وجود دارد

درک ارزش مواد دیجیتلی(Digital Material Value)

مواد دیجیتلی در دنیای امروز تنها یک معلومات ساده نیست، بلکه یک دارایی (Asset) با ارزش بسیار بالا محسوب می‌شود. دلیل این ارزش این است که دیتا می‌تواند برای تصمیم‌گیری، تجارت، تبلیغات و حتی کنترول رفتار انسان‌ها استفاده شود. شرکت‌ها و سازمان‌ها از معلومات کاربران برای کسب درآمد استفاده می‌کنند، به همین دلیل این معلومات بسیار مهم و حساس است. هرچه دیتا دقیق‌تر و بیشتر باشد، ارزش آن نیز بالاتر می‌رود. به همین خاطر، سرقت دیتا (Data Theft) و تقلب (Fraud) به یک مشکل بزرگ جهانی تبدیل شده است.

چرا مواد دیجیتلی ارزش دارد؟

- دیتا می‌تواند **فروخته شود**
- برای **تبلیغات و تجارت** استفاده می‌شود
- به شرکت‌ها کمک می‌کند **تصمیم بهتر بگیرند**
- باعث **شناخت رفتار کاربران** می‌شود
- در بعضی موارد حتی **قدرت و کنترول ایجاد می‌کند**

اهمیت محافظت از دیتا

چون دیتا ارزشمند است، باید از آن محافظت شود. اگر دیتا به دست افراد نادرست برسد، می‌تواند باعث مشکلات جدی شود. برای مثال:

- سرقت هویت
- سوءاستفاده مالی
- آسیب به اعتبار شخص

به همین دلیل، قوانین و سیستم‌های امنیتی برای محافظت از دیتا ایجاد شده است.

ارزش دیتا در سطح جهانی

طبق گزارش‌ها، جرایم سایبری (Cybercrime) هزینه بسیار زیادی به کشورها وارد می‌کند. برای مثال، در یک گزارش گفته شده که در سال 2017، این جرایم حدود **27میلیارد پوند** به یک کشور خساره وارد کرده است. این نشان می‌دهد که دیتا چقدر ارزشمند است و چرا هدف حملات قرار می‌گیرد.

ارزش معلومات شخصی

معلومات شخصی هر فرد نیز ارزش دارد، حتی اگر خودش متوجه نباشد. این معلومات شامل:

- نام و مشخصات
- موقعیت(Location)
- علایق و رفتار آنلاین

شرکت‌ها از این معلومات برای تبلیغات استفاده می‌کنند. برای مثال، وقتی شما در اینترنت چیزی جستجو می‌کنید، بعداً تبلیغات مشابه آن را می‌بینید.

مثال واقعی

فرض کنید یک شخص در یک ویب‌سایت ثبت‌نام می‌کند و معلومات خود را وارد می‌کند:

- این معلومات ذخیره می‌شود
- ممکن است برای تبلیغات استفاده شود
- یا حتی به شرکت‌های دیگر فروخته شود

این نشان می‌دهد که معلومات شخصی نیز یک دارایی با ارزش است

پیام برای دانش آموزان

دانش آموزان باید بدانند:

- هر چیزی که آنلاین نشر می‌کنند ارزش دارد
- ممکن است دیگران از آن استفاده کنند
- باید محتاط باشند که چه چیزی را شریک می‌سازند

جدول خلاصه ارزش دیتا

نوع دیتا	چرا ارزش دارد	مثال
معلومات شخصی	قابل استفاده در تبلیغات	ایمیل، نام
رفتار آنلاین	تحلیل کاربران	جستجو در گوگل
معلومات مالی	هدف سرقت	حساب بانکی
دیتا شرکت	تصمیم‌گیری	آمار فروش

درک خطر سرقت مواد دیجیتلی(Data Theft)

مواد دیجیتلی اگر به‌درستی محافظت نشود یا به‌صورت ضعیف مدیریت گردد، به‌راحتی می‌تواند سرقت شود. امروزه بیشتر معلومات به‌صورت دیجیتلی ذخیره می‌شود و همین موضوع باعث شده که مجرمان

سایبری به‌راحتی به آن دسترسی پیدا کنند. وقتی دیتا بدون رمز، بدون تنظیمات امنیتی یا در سیستم‌های ضعیف نگهداری شود، خطر سرقت بسیار بالا می‌رود. بنابراین، دانش آموزان باید درک کنند که مدیریت درست و محافظت از دیتا یک ضرورت بسیار مهم است، نه یک انتخاب.

چرا دیتا سرقت می‌شود؟

- برای **سوءاستفاده مالی**
- برای **فروش به شرکت‌ها**
- برای **دسترسی به حساب‌ها**
- برای **فریب دیگران(Fraud)**
- برای **آسیب رساندن به افراد یا سازمان‌ها**

چگونه دیتا در خطر قرار می‌گیرد؟

دیتا معمولاً در این حالت‌ها بیشتر در خطر است:

- استفاده از **رمز ضعیف**
- ذخیره دیتا بدون محافظت
- کلیک روی لینک‌های مشکوک
- استفاده از شبکه‌های ناامن
- اشتراک‌گذاری بیش از حد معلومات

برای مثال، اگر یک دانش آموز رمز ساده مانند "12345" استفاده کند، حساب او به‌راحتی هک می‌شود.

اهمیت تحقیق و شواهد(Evidence)

دانش آموزان باید بتوانند با تحقیق خود، نمونه‌های واقعی از جرایم دیجیتلی پیدا کنند. این کار باعث می‌شود درک آن‌ها واقعی‌تر شود. منابع تحقیق می‌تواند شامل:

- اخبار محلی
- گزارش‌های آنلاین
- حوادث واقعی

برای مثال، خبرهایی که در آن حساب‌های بانکی هک شده یا معلومات کاربران افشا شده است.

مثال واقعی

فرض کنید یک شخص ایمیل جعلی دریافت می‌کند:

- روی لینک کلیک می‌کند
- معلومات خود را وارد می‌کند

نتیجه:

اطلاعات او سرقت می‌شود و ممکن است حساب بانکی‌اش خالی شود

نقش آگاهی در جلوگیری از سرقت

اگر افراد آگاه باشند:

- کمتر فریب می‌خورند
- بهتر از دیتا خود محافظت می‌کنند
- خطرات را زودتر تشخیص می‌دهند

برای مثال، اگر دانش آموز بداند که لینک مشکوک خطرناک است، روی آن کلیک نمی‌کند.

انواع سرقت دیتا

نوع جرم	توضیح	مثال
هک (Hacking)	دسترسی غیرمجاز	ورود به حساب
فیشینگ (Phishing)	فریب برای گرفتن معلومات	ایمیل جعلی
سرقت هویت	استفاده از معلومات شخصی	باز کردن حساب
نشت دیتا	افشای معلومات	لو رفتن دیتا

روش‌های محافظت

روش	توضیح	نتیجه
رمز قوی	استفاده از رمز پیچیده	امنیت بیشتر
عدم اشتراک	ندادن معلومات	کاهش خطر
آگاهی	شناخت خطرات	جلوگیری از سرقت
سیستم امن	استفاده از انتی‌ویروس	محافظت بهتر

روش‌هایی که مواد دیجیتلی تهدید می‌شود

مواد دیجیتلی همیشه در معرض تهدید قرار دارد، مخصوصاً زمانی که امنیت ضعیف باشد. امروزه با پیشرفت اینترنت، انجام جرایم دیجیتلی بسیار آسان‌تر شده است. افراد می‌توانند بدون حضور فیزیکی، از راه دور به دیتا دسترسی پیدا کنند یا آن را سرقت کنند. دانش آموزان باید درک کنند که بیشتر این تهدیدات به دلیل بی‌احتیاطی کاربران یا ضعف در سیستم‌های امنیتی به‌وجود می‌آید. همچنین، بعضی

از کارهایی که به‌نظر ساده می‌آید، مانند استفاده از نرم‌افزار غیرقانونی یا دانلود فلم و موسیقی غیرقانونی، خود نوعی جرم دیجیتلی محسوب می‌شود.

انواع تهدیدات

- **هک :(Hacking)** دسترسی غیرمجاز به سیستم‌ها
- **فیشینگ :(Phishing)** فریب کاربران برای گرفتن معلومات
- **ویروس و بدافزار :**تخریب یا سرقت دیتا
- **سرقت هویت :**استفاده از معلومات دیگران
- **دانلود غیرقانونی :(Piracy)** استفاده غیرمجاز از محتوا
- **Plagiarism:** کاپی کردن کار یا اثر دیگران بدون ذکر منبع و یا رضایت آنها

نقش امنیت ضعیف

بیشتر تهدیدات زمانی رخ می‌دهد که:

- رمزها ضعیف باشد
- سیستم محافظت نداشته باشد
- کاربر آگاهی نداشته باشد

برای مثال، اگر یک شخص از نرم‌افزار غیرقانونی استفاده کند، ممکن است آن نرم‌افزار دارای ویروس باشد.

تأثیر اینترنت در افزایش جرایم

اینترنت باعث شده:

- دسترسی به دیتا آسان شود
- مجرمان از راه دور فعالیت کنند
- تشخیص جرم سخت‌تر شود

برای مثال، یک هکر می‌تواند از یک کشور دیگر به سیستم شما حمله کند.

مالکیت فکری(Intellectual Property)

یکی از مهم‌ترین موضوعات، احترام به حقوق دیگران است. استفاده از کار دیگران بدون اجازه، مانند:

- دانلود فلم غیرقانونی
- استفاده از نرم‌افزار کرک‌شده
- کاپی پروژه دیگران

همه این‌ها نوعی سرقت دیجیتلی است.

مثال واقعی

فرض کنید یک دانش آموز:

- پروژه را از اینترنت کاپی می‌کند
- بدون تغییر به استاد می‌دهد

این عمل **Plagiarism** است و یک نوع سرقت علمی محسوب می‌شود.

جدول انواع تهدیدات

نوع تهدید	توضیح	مثال
هک	دسترسی غیرمجاز	ورود به حساب
فیشینگ	فریب کاربر	ایمیل جعلی
ویروس	آسیب به سیستم	فایل آلوده
Piracy	استفاده غیرقانونی	دانلود فلم
Plagiarism	کاپی بدون منبع	پروژه کاپی

جدول علت و نتیجه

علت	نتیجه
رمز ضعیف	هک شدن
نرم‌افزار غیرقانونی	ویروس
عدم آگاهی	سرقت دیتا
استفاده نادرست	مشکل قانونی

روش‌های محافظت از مواد دیجیتلی

مواد دیجیتلی به دلیل ارزش بالای خود، همیشه در معرض خطر سرقت، تخریب و سوءاستفاده قرار دارد. برای جلوگیری از این خطرات، نیاز است که از روش‌های مختلف محافظتی استفاده شود. این محافظت تنها مربوط به یک بخش نیست، بلکه شامل **افراد(Personal) ، نرم‌افزار(Software) ، سخت‌افزار (Hardware) و سازمان (Organization)** می‌شود. هرچه آگاهی و استفاده از این روش‌ها بیشتر باشد، خطرات کمتر می‌شود. دانش آموزان باید بتوانند این روش‌ها را شناسایی کرده و توضیح دهند که چگونه از دیتا محافظت می‌کند.

روش‌های محافظت

بخش فردی(Personal)

- آموزش دانش آموزان و کارمندان
- استفاده از رمز قوی

- عدم شریک‌سازی معلومات شخصی
- آگاهی از خطرات آنلاین

بخش نرم‌افزار(Software)

- استفاده از **HTTPS** به‌جایHTTP
- استفاده از **Encryption (رمزگذاری)**
- استفاده از **SSL** برای امنیت ویب‌سایت
- نصب و آپدیت انتی‌ویروس

بخش سخت‌افزار(Hardware)

- استفاده از **Firewall**
- استفاده از **IDS سیستم تشخیص نفوذ**
- محافظت از سرورها

بخش سازمانی(Organization)

- قوانین استفاده(AUP) Acceptable Use Policy
- پروتوکول‌های امنیتی
- کنترول دسترسی
- آموزش کارمندان

اهمیت آموزش(Training)

آموزش یکی از مهم‌ترین روش‌های محافظت است. اگر افراد بدانند:

- ایمیل جعلی چیست
- چگونه رمز قوی بسازند
- چگونه لینک مشکوک را تشخیص دهند

احتمال قربانی شدن بسیار کم می‌شود

نقش نرم‌افزار و سخت‌افزار

برای امنیت آنلاین، افراد باید آگاهی ابتدایی داشته باشند:

- فرق بین HTTP و HTTPS
- اهمیت رمزگذاری
- نقش Firewall

حتی استفاده ساده از این ابزارها می‌تواند امنیت را بسیار افزایش دهد.

نقش سازمان‌ها

سازمان‌ها مسئولیت بیشتری دارند و باید:

- سیستم‌های امنیتی قوی داشته باشند

- قوانین واضح ایجاد کنند
- دیتا کاربران را محافظت کنند

برای مثال، یک مکتب باید معلومات دانش آموزان را محفوظ نگه دارد.

مثال واقعی

فرض کنید یک دانش آموز:

- از ویب‌سایت HTTP استفاده می‌کند → معلومات او قابل سرقت است
- از HTTPS استفاده می‌کند → معلومات رمزگذاری می‌شود

این یک مثال ساده از اهمیت محافظت است.

روش‌های محافظت

بخش	روش	توضیح	نتیجه
Personal	آموزش	آگاهی افراد	کاهش خطر
Software	HTTPS / SSL	ارتباط امن	جلوگیری از سرقت
Software	Encryption	رمزگذاری دیتا	امنیت بیشتر
Hardware	Firewall	جلوگیری از حمله	محافظت سیستم
Hardware	IDS	تشخیص نفوذ	هشدار سریع
Organization	AUP	قوانین استفاده	نظم و امنیت

جدول آموزش مورد نیاز

نوع آموزش	هدف	مثال
امنیت آنلاین	جلوگیری از فریب	شناخت فیشینگ
رمزگذاری	محافظت دیتا	استفاده HTTPS
استفاده سیستم	کار درست	مدیریت فایل
آگاهی عمومی	شناخت خطر	عدم اشتراک معلومات

جدول کامل اصطلاحات(Digital Protection Terms)

اصطلاح انگلیسی	معنی دری	توضیح و کاربرد عملی

Digital Material	مواد دیجیتلی	معلومات که به شکل فایل ذخیره می‌شود مثل عکس، ویدیو، اسناد
Data Protection	محافظت دیتا	حفظ معلومات از دسترسی غیرمجاز
Security	امنیت	جلوگیری از دسترسی افراد غیرمجاز
Personal Security	امنیت شخصی	محافظت از معلومات شخصی خود
Training	آموزش	یادگیری روش‌های جلوگیری از جرم
Awareness	آگاهی	شناخت خطرات آنلاین
Password	رمز عبور	کلید ورود به حساب
Strong Password	رمز قوی	رمز پیچیده برای جلوگیری از هک
Authentication	تصدیق هویت	بررسی اینکه کاربر واقعی است
Encryption	رمزگذاری	تبدیل دیتا به شکل مخفی
Decryption	رمزگشایی	برگرداندن دیتا به حالت اصلی
HTTPs (Hyper Text Transfer Protocol Secure) Update Version	ارتباط امن ویب	انتقال دیتا به شکل رمزگذاری شده
HTTP (Hyper Text Transfer Protocol) Old Version	ارتباط عادی ویب	انتقال بدون امنیت
SSL (Secure Scout Layer)	گواهی امنیتی	ایجاد ارتباط امن در ویب‌سایت
Antivirus	انتی‌ویروس	نرم‌افزار برای جلوگیری از ویروس
Malware	بدافزار	برنامه مخرب برای آسیب رساندن
Virus	ویروس	نوعی بدافزار
Firewall	دیوار آتش	جلوگیری از دسترسی غیرمجاز به شبکه
IDS (Intrusion Detection System)	سیستم تشخیص نفوذ	شناسایی حملات
Network Security	امنیت شبکه	محافظت از شبکه‌ها
Server	سرور	سیستم ذخیره دیتا
Secure Server	سرور امن	سروری با محافظت بالا
Access Control	کنترول دسترسی	تعیین اینکه چه کسی دسترسی دارد
Permissions	سطح دسترسی	مشخص کردن نوع دسترسی کاربران
User Account	حساب کاربری	پروفایل کاربر
Privacy Settings	تنظیمات حریم خصوصی	کنترول نمایش معلومات
Data Breach	نشت دیتا	افشای معلومات
Cybercrime	جرایم سایبری	جرایم در فضای دیجیتال
Phishing	فیشینگ	فریب برای گرفتن معلومات

Hacking	هک	دسترسی غیرمجاز
Fraud	تقلب	استفاده نادرست از دیتا
AUP (Acceptable Use Policy)	قوانین استفاده	مقررات استفاده از سیستم
Security Protocols	پروتوکول‌های امنیتی	قوانین برای امنیت سیستم
Cloud Security	امنیت کلود	محافظت از دیتا در اینترنت
Backup	نسخه پشتیبان	ذخیره اضافی دیتا
Data Loss	از دست رفتن دیتا	حذف یا نابودی معلومات
Secure Connection	ارتباط امن	انتقال مطمئن دیتا
Login	ورود به سیستم	دسترسی به حساب
Logout	خروج از سیستم	پایان دسترسی
Two-Factor Authentication	تصدیق دو مرحله‌ای	امنیت بیشتر در ورود
Update	بروزرسانی	جدید ساختن سیستم
Patch	اصلاح امنیتی	رفع مشکلات امنیتی
Monitoring	نظارت	بررسی فعالیت‌ها
Threat	تهدید	خطر برای دیتا
Protection Mechanism	روش محافظت	ابزار یا راه جلوگیری از خطر

انواع تهدیدات فعلی در دنیای دیجیتال

در دنیای امروز، تهدیدات دیجیتلی بسیار گسترده و پیچیده شده‌اند با توسعه هوش مصنوعی رشد بخش های تکنالوژیکی هر روز در اخبار دیده می‌شوند. این تهدیدات نه تنها افراد، بلکه شرکت‌ها و حتی دولت‌ها را نیز هدف قرار می‌دهند. دانش آموزان باید درک کنند که این تهدیدات چگونه کار می‌کنند، چه ویژگی‌هایی دارند و چه خساراتی ایجاد می‌کنند. همچنان باید بدانند که بسیاری از این جرایم از طریق فریب(Deception) ، ضعف امنیتی یا بی‌احتیاطی افراد انجام می‌شود. شناخت این تهدیدات کمک می‌کند تا بتوان از آن‌ها جلوگیری کرد.

توضیح تهدیدات

Online Fraud

این نوع تهدید شامل استفاده از ایمیل، تماس یا ویب‌سایت جعلی برای فریب کاربران است تا معلومات مهم مانند معلومات بانکی خود را وارد کنند. معمولاً به شکل پیام‌های فوری یا پیشنهادهای جذاب ظاهر می‌شود.

Scareware

در این روش، پیام‌های ترسناک (مثلاً "سیستم شما ویروسی است") به کاربر نشان داده می‌شود تا او را مجبور به دانلود نرم‌افزار جعلی کند. این نرم‌افزار در واقع بدافزار است.

Identity Theft

در این تهدید، معلومات شخصی یک فرد (نام، شماره، ایمیل) دزدیده شده و برای انجام کارهای غیرقانونی استفاده می‌شود، مانند باز کردن حساب یا خرید.

IP Theft (Intellectual Property)

این نوع سرقت مربوط به آثار فکری است، مانند نرم‌افزار، طراحی، پروژه یا محتوا. استفاده بدون اجازه از این آثار، یک جرم دیجیتلی محسوب می‌شود.

Espionage

جاسوسی دیجیتلی است که در آن افراد یا سازمان‌ها تلاش می‌کنند معلومات مهم و محرمانه را به‌دست آورند، معمولاً برای اهداف سیاسی یا تجارتی.

Loss of Customer Data

در این حالت، معلومات مشتریان به دلیل بی‌احتیاطی یا ضعف امنیتی از دست می‌رود، مثلاً گم شدن لپتاپ یا هک شدن سیستم.

Online Theft from Companies

در این نوع تهدید، شرکت‌ها هدف قرار می‌گیرند و پول یا دیتا از آن‌ها سرقت می‌شود، معمولاً از طریق هک یا نفوذ به سیستم.

Extortion

در این روش، مجرمین با تهدید (مثلاً افشای معلومات) از افراد یا شرکت‌ها پول می‌خواهند. این کار معمولاً با بدافزار یا دسترسی به دیتا انجام می‌شود.

Fiscal Fraud

این نوع تقلب مربوط به امور مالی است، مانند دستکاری در حساب‌ها یا انتقال غیرقانونی پول از طریق سیستم‌های دیجیتلی.

جدول جامع تهدیدات دیجیتلی

Name of Threat	Main Characteristics	Prevention Techniques	Potential Damage
Online Fraud	استفاده از ایمیل، تماس یا ویب‌سایت جعلی برای گرفتن معلومات بانکی	بررسی منبع ایمیل، کلیک نکردن روی لینک مشکوک، استفاده از سایت معتبر	از دست دادن پول

Scareware	نمایش پیام‌های ترسناک (مثلاً ویروس جعلی) برای فریب کاربر	نصب انتی‌ویروس واقعی، نادیده گرفتن پیام‌های جعلی	نصب بدافزار، از دست رفتن دیتا
Identity Theft	استفاده از معلومات شخصی دیگران	عدم شریک‌سازی معلومات، رمز قوی	سوءاستفاده مالی، مشکلات قانونی
IP Theft (Intellectual Property)	سرقت آثار فکری مثل نرم‌افزار، طراحی، پروژه	استفاده قانونی، احترام به حق نشر	از دست رفتن حقوق مالک
Espionage	جاسوسی دیجیتلی برای گرفتن اطلاعات مهم	استفاده از سیستم‌های امنیتی قوی	افشای معلومات حساس
Loss of Customer Data	از دست رفتن معلومات مشتریان (مثلاً گم شدن لپتاپ)	دقت در نگهداری، قفل سیستم، Backup	آسیب به اعتبار شرکت
Online Theft from Companies	سرقت پول یا دیتا از شرکت‌ها	امنیت شبکه، Firewall	ضرر مالی
Extortion	تهدید برای گرفتن پول (مثلاً باج‌گیری)	محافظت از دیتا، عدم پاسخ به تهدید	از دست دادن پول
Fiscal Fraud	تقلب مالی از طریق سیستم‌های دیجیتال	بررسی تراکنش‌ها، استفاده از سیستم امن	ضرر مالی بزرگ

تهدیدات آنلاین بر امنیت شخصی

فعالیت در اینترنت علاوه بر مزایا، خطراتی نیز برای امنیت شخصی افراد دارد. این تهدیدات می‌تواند شامل سرقت معلومات، فریب، آزار و حتی سوءاستفاده باشد. دانش آموزان باید درک کنند که این خطرات چگونه به‌وجود می‌آید و کدام یک بیشتر احتمال وقوع دارد. همچنان باید بتوانند تصمیم بگیرند که برای کاهش این خطرات چه اقداماتی انجام دهند. این آگاهی باعث می‌شود که آن‌ها در استفاده از اینترنت محتاط‌تر و مسئولانه‌تر عمل کنند.

انواع تهدیدات شخصی

- **فیشینگ :(Phishing)** فریب برای گرفتن معلومات
- **سرقت هویت :(Identity Theft)** استفاده از معلومات شخصی
- **سایبر بولینگ :(Cyberbullying)** آزار آنلاین

- **گمراه‌سازی :(Grooming)** فریب برای سوءاستفاده
- **نشت معلومات :(Data Leak)** افشای اطلاعات
- **کلیک روی لینک‌های مشکوک**

تأثیر این تهدیدات بر فرد

این تهدیدات می‌تواند باعث:

- از دست دادن پول
- آسیب روحی
- از بین رفتن اعتبار
- خطرات جدی امنیتی

برای مثال، یک دانش آموز ممکن است با یک فرد ناشناس صحبت کند که هدف سوءاستفاده دارد.

مثال واقعی

فرض کنید یک دانش آموز:

- در شبکه اجتماعی با یک فرد ناشناس صحبت می‌کند
- معلومات شخصی خود را شریک می‌سازد

نتیجه:

ممکن است آن فرد از معلومات سوءاستفاده کند.

ارزیابی خطر(Likelihood & Action)

دانش آموزان باید بتوانند خطرات را ارزیابی کنند:

- کدام تهدید بیشتر اتفاق می‌افتد؟
- چگونه می‌توان آن را کاهش داد؟

جدول ارزیابی تهدیدات شخصی

نوع تهدید	احتمال وقوع	خطر	اقدام برای کاهش
Phishing	زیاد	بالا	کلیک نکردن لینک
Identity Theft	متوسط	بالا	عدم شریک‌سازی معلومات
Cyberbullying	متوسط	متوسط	بلاک و راپور
Grooming	کم/متوسط	بسیار بالا	عدم ارتباط با ناشناس
Data Leak	متوسط	بالا	Privacy تنظیم

اقدامات محافظتی

اقدام	توضیح	نتیجه
رمز قوی	جلوگیری از هک	امنیت بیشتر
Privacy Settings	محدود کردن دسترسی	محافظت معلومات
عدم اشتراک	حفظ اطلاعات	کاهش خطر
آگاهی	شناخت تهدید	تصمیم بهتر

طراحی و استفاده از پروسس‌ها برای محافظت از مواد دیجیتلی

برای محافظت از مواد دیجیتلی، فقط دانستن تهدیدات کافی نیست، بلکه باید یک سلسله پروسس (مراحل منظم) طراحی و استفاده شود. این پروسس‌ها کمک می‌کند که کاربر در هر مرحله از استفاده از اینترنت، امنیت خود را حفظ کند. دانش آموزان باید بتوانند توضیح دهند که در زندگی روزمره چگونه از این مراحل استفاده می‌کنند. این کار نشان می‌دهد که آن‌ها نه‌تنها دانش دارند، بلکه می‌توانند آن را در عمل نیز تطبیق کنند.

پروسس‌های محافظت

دانش آموزان می‌توانند این مراحل را در کار خود استفاده کنند:

- استفاده از **رمز قوی و متفاوت**
- فعال‌سازی **Privacy Settings**
- بررسی لینک‌ها قبل از کلیک
- استفاده از **HTTPS ویب‌سایت‌ها**
- نصب و آپدیت **Antivirus**
- گرفتن **Backup** از فایل‌ها
- خروج از حساب (Logout) بعد از استفاده نمودن

استفاده عملی از پروسس‌ها

هر پروسس باید در یک وضعیت واقعی استفاده شود. دانش آموزان باید بتوانند توضیح دهند که در هر مرحله چه کاری انجام می‌دهند و چرا. این کار نشان می‌دهد که امنیت فقط یک مفهوم نیست، بلکه یک عمل روزانه است.

مثال واقعی (سناریو)

فرض کنید یک دانش آموز می‌خواهد وارد ایمیل خود شود:

1. بررسی می‌کند که آدرس سایت **HTTPS** باشد
2. رمز قوی وارد می‌کند
3. بعد از استفاده، **Logout** می‌کند
4. روی لینک‌های مشکوک کلیک نمی‌کند

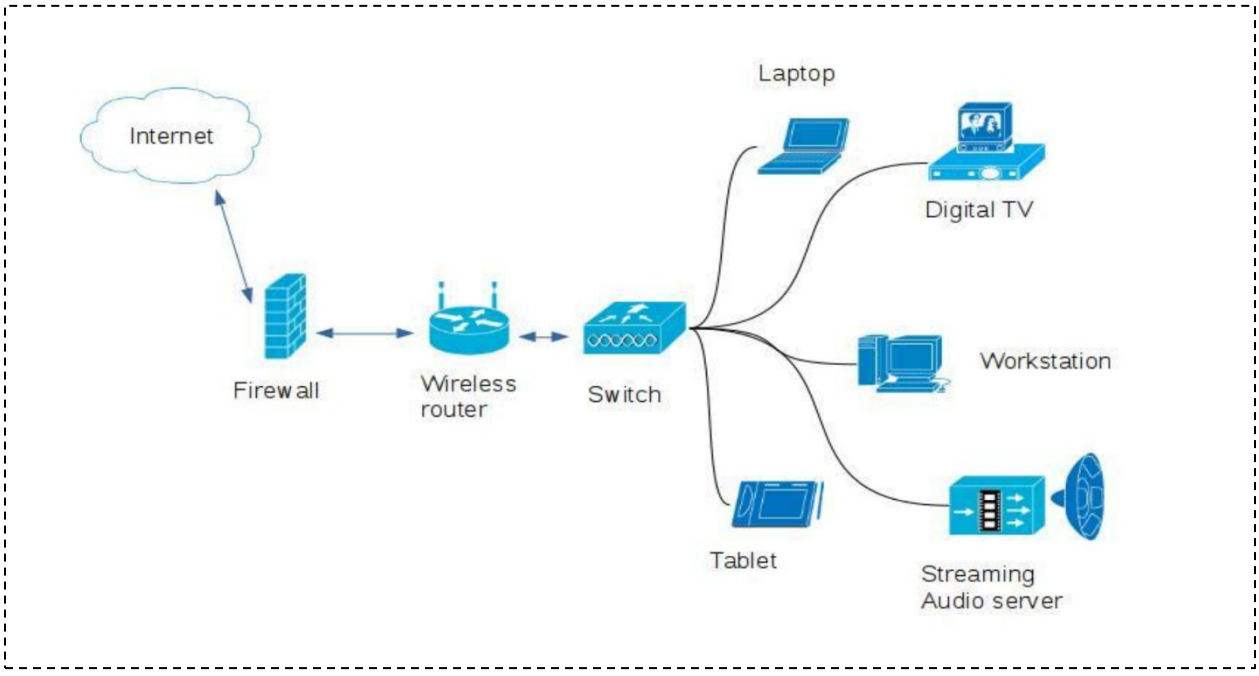
این یک پروسس کامل محافظتی است

استفاده از دیاگرام(Diagram)

دانش آموزان می‌توانند یک دیاگرام ساده رسم کنند که نشان دهد:

- انترنت → روتر → کمپیوتر
- Firewall → Antivirus → User

این کمک می‌کند که روند محافظت را بهتر درک کنند



جدول پروسس‌های محافظتی

مرحله	عمل	دلیل	نتیجه
ورود	استفاده از رمز قوی	جلوگیری از هک	امنیت حساب
استفاده	بررسی لینک	جلوگیری از فریب	کاهش خطر

اتصال	HTTPS استفاده از	ارتباط امن	محافظت دیتا
ذخیره	Backup	جلوگیری از از دست رفتن	حفظ معلومات
خروج	Logout	جلوگیری از دسترسی دیگران	امنیت بیشتر

سناریو محافظت

وضعیت	خطر	اقدام	نتیجه
استفاده از ایمیل	فیشینگ	بررسی لینک	جلوگیری از سرقت
دانلود فایل	ویروس	انتی‌ویروس	محافظت سیستم
استفاده از شبکه	هک	Firewall	امنیت شبکه

سیستم‌هایی که برای محافظت از مواد دیجیتلی استفاده می‌کنیم

برای محافظت از مواد دیجیتلی، استفاده از پروسس‌ها کافی نیست، بلکه باید از سیستم‌ها (Systems) نیز استفاده شود. این سیستم‌ها شامل نرم‌افزار، سخت‌افزار و پروتوکول‌های ارتباطی است. هرکدام از این بخش‌ها نقش مهمی در امنیت دارند. دانش آموزان باید بتوانند توضیح دهند که از چه ابزارهایی استفاده می‌کنند، این ابزارها چگونه کار می‌کند و چه نقاط ضعف (Vulnerabilities) دارد. شناخت این نقاط ضعف کمک می‌کند تا از خطرات جلوگیری شود.

سیستم‌های نرم‌افزاری(Software)

دانش آموزان معمولاً از این نرم‌افزارها استفاده می‌کنند:

- **Antivirus** → شناسایی و حذف ویروس
- **Firewall Software** → جلوگیری از دسترسی غیرمجاز
- **Browser Security Settings** → تنظیم امنیت در ویب
- **Encryption Tools** → رمزگذاری دیتا

این نرم‌افزارها کمک می‌کند که سیستم در برابر تهدیدات محافظت شود.

سیستم‌های سخت‌افزاری(Hardware)

مهم‌ترین وسیله سخت‌افزاری:

- **Router با Firewall داخلی**
- **Modem امن**
- **Device Lock** سیستم **قفل دستگاه**

برای مثال، Firewall در روتر خانه از ورود افراد غیرمجاز جلوگیری می‌کند.

Modern Router

پروتوکول‌های انتقال دیتا و خطرات آن

Protocol	معنی	خطر (Vulnerability)	روش محافظت
Bluetooth	انتقال نزدیک	دسترسی غیرمجاز	خاموش کردن وقتی نیاز نیست
SMS	پیام موبایل	فیشینگ (SMS Scam)	باز نکردن لینک
HTTP	وب غیرامن	قابل شنود	استفاده نکردن
HTTPS	وب امن	کم خطر	استفاده ترجیحی
Wireless (Wi-Fi)	شبکه بی‌سیم	هک شبکه	Wi-Fi رمز قوی
NFC	انتقال نزدیک	دسترسی سریع	استفاده محدود

دانش آموزان باید جدول بالا را بدقت مطالعه کند و نحوه انتقال دیتا از کدام مسیرها نا امن و کدام مسیرامن میباشد را تفکیک کنند.

نقاط ضعف(Vulnerabilities)

هر سیستم دارای ضعف است، برای مثال:

- Bluetooth روشن → امکان اتصال غیرمجاز
- Wi-Fi بدون رمز → دسترسی آسان
- HTTP → انتقال غیرامن

شناخت این ضعف‌ها بسیار مهم است

ویژگی‌های یک سیستم امن

یک سیستم محافظتی خوب باید:

- دسترسی را محدود کند

- فعالیت‌ها را نظارت کند
- هشدار بدهد
- دیتا را رمزگذاری کند

چگونه بفهمیم سیستم ما امن است؟

- دریافت هشدار از Antivirus
- بررسی فعالیت‌های مشکوک
- کند شدن غیرعادی سیستم (بررسی Task Manger در سیستم عامل ویندوز)
- پیام‌های امنیتی

مثال واقعی

فرض کنید یک دانش آموز:

- از Wi-Fi بدون رمز استفاده می‌کند

نتیجه:

- دیگران می‌توانند به شبکه وصل شوند
- معلومات او سرقت شود

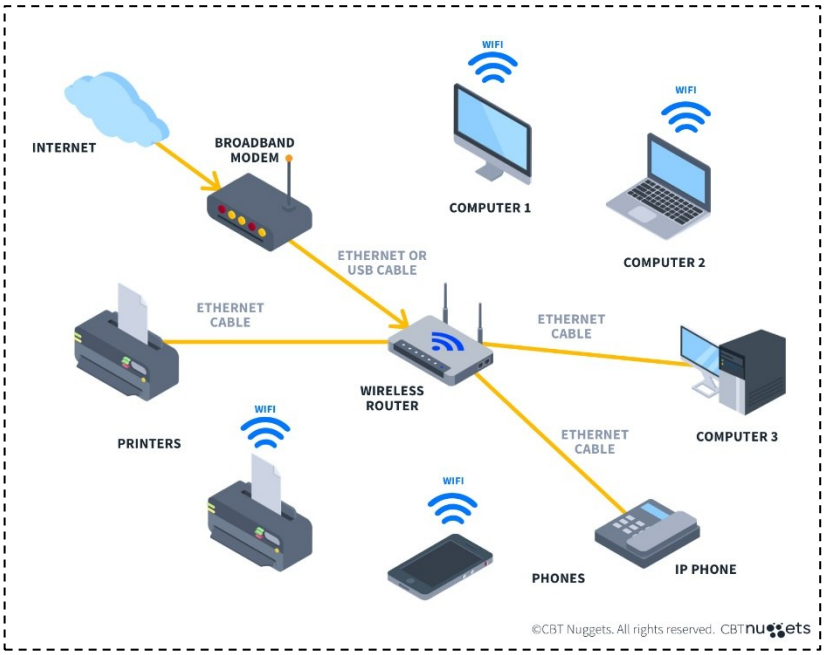
اما اگر:

- رمز قوی استفاده کند

امنیت افزایش می‌یابد

جدول سیستم‌های محافظتی

نوع سیستم	ابزار	وظیفه	نتیجه
Software	Antivirus	حذف ویروس	امنیت سیستم
Software	Firewall	جلوگیری از حمله	محافظت شبکه
Hardware	Router	کنترول اتصال	امنیت خانه
Protocol	HTTPS	انتقال امن	محافظت دیتا



ساختار شبکه در انترنت

برای معلومات کامل در مورد این دیاگرام میتوانید مقاله مربوطه را بخوانید بیشتر...

ماهیت (Nature) تهدیدات دیجیتلی

برای درک واقعی تهدیدات دیجیتلی، تنها شناخت نام آن‌ها کافی نیست؛ بلکه باید ماهیت (Nature) آن‌ها بررسی شود. یعنی بفهمیم که یک تهدید چگونه عمل می‌کند، چرا مؤثر است، و چه نقاط قوت و ضعف دارد. دانش آموزان باید بتوانند بین یک مزاحمت ساده (Annoyance) و یک تهدید واقعی (Threat)تفاوت قایل شوند. تهدید واقعی معمولاً باعث ضرر مالی، سرقت معلومات یا خطر امنیتی می‌شود، در حالی که مزاحمت فقط باعث ناراحتی موقت است.

تفاوت Threat و Annoyance

- **تهدید (Threat)**
  باعث ضرر واقعی (پول، معلومات، امنیت) می‌شود
- **مزاحمت (Annoyance):**
  فقط ناراحت‌کننده است (مثلاً تبلیغات زیاد)

مثال:
یک ایمیل تبلیغاتی = مزاحمت
یک ایمیل جعلی بانکی = تهدید

تحلیل چند تهدید مهم

تقلب آنلاین (Online Fraud)
این تهدید بر اساس فریب کاربر عمل می‌کند. مجرمین تلاش می‌کنند اعتماد فرد را جلب کنند و معلومات حساس را بگیرند.
قوت: بسیار واقعی و قانع‌کننده
ضعف: با دقت قابل تشخیص است

فیشینگ (Phishing)

ارسال ایمیل یا پیام جعلی برای گرفتن معلومات.
قوت: استفاده از لوگو و نام معتبر
ضعف: آدرس ایمیل جعلی قابل تشخیص است

سرقت هویت (Identity Theft)

استفاده از معلومات شخصی برای انجام جرم.
قوت: دسترسی کامل به هویت فرد
ضعف: نیاز به معلومات زیاد دارد

Scareware
ترساندن کاربر برای نصب نرم‌افزار.
قوت: ایجاد ترس فوری
ضعف: پیام‌ها اغلب غیرواقعی است
باج‌گیری (Extortion)

تهدید برای گرفتن پول.
قوت: فشار روانی بالا
ضعف: در صورت عدم پاسخ بی‌اثر می‌شود

چرا مردم فریب می‌خورند؟

- اعتماد به نام‌های مشهور (بانک، شرکت)
- عجله و ترس
- کمبود آگاهی
- ظاهر حرفه‌ای پیام‌ها

مثال:
ایمیل جعلی از "بانک" که می‌گوید: حساب شما بسته می‌شود

مثال واقعی

فرض کنید یک دانش آموز:

- ایمیل دریافت می‌کند که نوشته: "شما برنده شده‌اید "
- روی لینک کلیک می‌کند و معلومات خود را وارد می‌کند

نتیجه:

سرقت معلومات و حتی پول

نکات مهم در مؤثر بودن تهدیدات

- طراحی حرفه‌ای (لوگو، رنگ)
- استفاده از احساسات (ترس، خوشحالی)
- شباهت به منابع واقعی

جدول تحلیل تهدیدات

نوع تهدید	چگونه عمل می‌کند	چرا مؤثر است	نقطه ضعف
Online Fraud	فریب کاربر	اعتمادسازی	بررسی قابل تشخیص
Phishing	ایمیل جعلی	ظاهر واقعی	لینک مشکوک
Identity Theft	استفاده از معلومات	دسترسی کامل	نیاز به دیتا زیاد
Scareware	ترساندن	واکنش فوری	پیام غیرواقعی
Extortion	تهدید	فشار روانی	نادیده گرفتن

Threat vs Annoyance

نوع	ویژگی	مثال	نتیجه
Threat	خطر واقعی	فیشینگ	سرقت پول
Annoyance	ناراحتی ساده	تبلیغات	مشکل کم

سیستم عملی برای محافظت از مواد دیجیتلی

برای محافظت واقعی از مواد دیجیتلی، تنها دانستن ابزارها کافی نیست، بلکه باید یک سیستم کامل و عملی (Working System) طراحی شود. این سیستم شامل ترکیب انترنت، روتر، فایروال، انتی‌ویروس و رفتار کاربر است. دانش آموزان باید بتوانند توضیح دهند که هر بخش چگونه کار می‌کند و اگر درست تنظیم نشود، چه خطراتی ایجاد می‌کند. این نشان می‌دهد که امنیت یک سیستم هماهنگ است، نه یک ابزار جداگانه. همچنان شما در مورد ساختار انترنت و ابزارهای آن در صفحه 109 مطالعه

نمودید دقیقا شما باید تمام همان دیاگرام و ابزارهای که با هم ساختار را تشکیل میدهد لایه های امنیتی آنها را درست تخشیص داده و پیگیری نمایید.

اجزای سیستم محافظتی

یک سیستم ساده خانگی شامل:

- Internet (منبع اتصال)
- Router(کنترول کننده شبکه)
- Firewall (جلوگیری از نفوذ)
- Device (کمپیوتر/موبایل، تلویزیون...)
- Antivirus(محافظت نرم افزاری)
- User (کاربر)

طریقه کار سیستم

این سیستم به شکل زنجیره‌ای کار می‌کند:

1. Internet → دیتا وارد می‌شود
2. Router → ترافیک را کنترول می‌کند
3. Firewall → دسترسی مشکوک را بلاک می‌کند
4. Antivirus → فایل‌ها را بررسی می‌کند
5. User → تصمیم نهایی می‌گیرد

اگر یک بخش ضعیف باشد، کل سیستم آسیب‌پذیر می‌شود

نقاط خطر در سیستم

- Router بدون رمز → دسترسی آزاد
- Firewall خاموش → نفوذ آسان
- Antivirus آپدیت نشده → ویروس
- User بی‌احتیاط → کلیک روی لینک

مثال واقعی

فرض کنید:

- یک دانش آموز Wi-Fi بدون رمز دارد
- Firewall فعال نیست

نتیجه:

افراد دیگر می‌توانند وارد شبکه شوند و معلومات را سرقت کنند

اما اگر:

- رمز قوی Firewall + فعال

سیستم امن‌تر می‌شود.

بررسی روش‌های بدیل برای جلوگیری از حملات آینده

جمله مهم" :یک سیستم فقط به اندازه ضعیف‌ترین بخش خود قوی است "یعنی اگر یک بخش سیستم ضعیف باشد، کل سیستم در خطر است. دانش آموزان باید بتوانند روش‌های مختلف Software) و Hardware)را بررسی کنند و بفهمند که امنیت فقط به خرید ابزار گران وابسته نیست، بلکه به انتخاب درست، تنظیم صحیح و استفاده آگاهانه بستگی دارد. همچنان باید درک کنند که همیشه یک تعادل (Trade-off)بین امنیت و آسانی استفاده وجود دارد.

بررسی روش‌های بدیل(Alternative Methods)
دانش آموزان می‌توانند روش‌های مختلف را جایگزین یا ترکیب کنند:

- Antivirus معمولی ⟶ Advanced Security Software
- Password ساده ⟶ Two-Factor Authentication
- Wi-Fi عادی ⟶ Secure Wi-Fi (WPA3)
- Local Storage ⟶ Cloud Backup
- Firewall ساده ⟶ Smart Firewall

مفهوم Cost vs Benefit (هزینه و فایده)
همیشه سیستم گران‌تر = امنیت بیشتر نیست
- یک سیستم ارزان اما درست تنظیم‌شده → امن
- یک سیستم گران اما بدون تنظیم → خطرناک

مهم :دانش + استفاده درست >قیمت

Trade-off بین امنیت و انعطاف
اگر امنیت خیلی زیاد شود:
- استفاده سخت می‌شود
- سرعت کم می‌شود
- کاربران ناراضی می‌شوند

مثال:
- هر 5 دقیقه رمز خواستن ❌ (غیر عملی)
- استفاده از 2 FAبرای حساب مهم ✅ (متعادل)

چه زمانی سیستم غیرقابل استفاده می‌شود؟
سیستم بیش از حد امن زمانی مشکل‌ساز می‌شود که:
- کاربر نتواند به‌راحتی وارد شود

- کارها بسیار کند انجام شود
- دسترسی‌ها بیش از حد محدود شود

نتیجه: کاربران ممکن است امنیت را دور بزنند

مثال واقعی

فرض کنید:

حالت ضعیف:

- رمز ساده
- بدون Firewall

خطر زیاد

حالت متعادل:

- رمز قوی
- 2FA
- Firewallفعال

امنیت مناسب + استفاده آسان

اگر بودجه نامحدود باشد (سیستم ایده‌آل)

دانش آموزان می‌توانند چنین سیستم طراحی کنند:

- Router پیشرفته با Firewall قوی
- سیستم مانیتورینگ شبکه
- Cloud Backup خودکار
- Antivirus حرفه‌ای
- Encryption کامل دیتا
- 2FA برای تمام حساب‌ها

این یک سیستم بسیار امن است.

مقایسه روش‌های بدیل

روش	مزیت	ضعف	نتیجه
Password ساده	آسان	ضعیف	خطر بالا
2FA	امنیت بالا	نیاز مرحله اضافی	امنیت قوی
Antivirus عادی	ارزان	محدود	امنیت متوسط
Advanced Security	قوی	هزینه بالا	امنیت بهتر
Wi-Fi عادی	آسان	قابل هک	خطر

Secure Wi-Fi	امن	نیاز تنظیم	امنیت بالا

Cost vs Security

سطح هزینه	سطح امنیت	توضیح
کم	متوسط	اگر درست استفاده شود
متوسط	خوب	بهترین حالت
زیاد	عالی	اما ممکن پیچیده شود

نوت: تمام این نکات امنیتی را در دیاگرام صفحه 109 تمرین کنید و مطالب مربوط را بدقت با این ابزارهای انترنتی بررسی کنید.

تأثیر فعالیت‌های آنلاین بر امنیت و معلومات شخصی

هر فعالیت آنلاین که ما انجام می‌دهیم، با خود نوعی خطر برای معلومات شخصی و امنیت ما دارد. این خطرات بسته به نوع فعالیت متفاوت است. برای مثال، استفاده از شبکه‌های اجتماعی، خرید آنلاین یا دانلود فایل‌ها هرکدام سطح خطر مختلف دارند. دانش آموزان باید بتوانند این فعالیت‌ها را شناسایی کرده، خطر آن‌ها را ارزیابی کنند و توضیح دهند که در هر مرحله چه تهدیدی ممکن است به‌وجود آید. این مهارت کمک می‌کند تا آن‌ها تصمیم‌های آگاهانه و مصون بگیرند.

انواع فعالیت‌های آنلاین

- استفاده از شبکه‌های اجتماعی
- خرید آنلاین (Online Shopping)
- دانلود فایل‌ها
- استفاده از ایمیل
- بازی‌های آنلاین
- استفاده از Wi-Fi عمومی
- ساخت حساب در ویب‌سایت‌ها

تحلیل خطر در هر فعالیت

شبکه‌های اجتماعی

در این فعالیت، افراد معمولاً معلومات شخصی، عکس‌ها و ویدیوها را شریک می‌سازند. خطر اصلی شامل سرقت هویت و سوءاستفاده از معلومات است.

خرید آنلاین

در خرید آنلاین، معلومات بانکی وارد می‌شود. اگر سایت امن نباشد، خطر سرقت پول و معلومات مالی وجود دارد.

دانلود فایل‌ها

دانلود از منابع نامعتبر می‌تواند باعث ورود ویروس و بدافزار به سیستم شود.

ایمیل

ایمیل‌ها می‌توانند شامل پیام‌های جعلی (Phishing) باشند که هدف آن گرفتن معلومات است.

Wi-Fi عمومی

شبکه‌های عمومی معمولاً امنیت ضعیف دارند و امکان شنود و هک معلومات وجود دارد.مثال واقعی فرض کنید یک دانش آموز:

- در Wi-Fi عمومی وارد حساب ایمیل می‌شود

نتیجه:

ممکن است هکر معلومات او را سرقت کند

اما اگر:

- از HTTPS و VPN استفاده کند

خطر کاهش می‌یابد!

ارزیابی خطر فعالیت‌ها

فعالیت	نوع خطر	سطح خطر	اقدام محافظتی
شبکه اجتماعی	سرقت هویت	متوسط/زیاد	Privacy تنظیم
خرید آنلاین	سرقت پول	زیاد	HTTPS استفاده
دانلود فایل	ویروس	زیاد	انتی‌ویروس
ایمیل	فیشینگ	زیاد	بررسی لینک
عمومی Wi-Fi	هک	بسیار زیاد	VPN عدم استفاده یا
بازی آنلاین	دسترسی حساب	متوسط	رمز قوی

مراحل فعالیت و خطر

مرحله	فعالیت	خطر	راه حل
ورود	Login	سرقت رمز	2FA
استفاده	مرور	فیشینگ	دقت
دانلود	فایل	ویروس	Antivirus
خروج	Logout	دسترسی دیگران	خروج کامل

تحلیل تکنالوژی‌های سخت‌افزاری برای جلوگیری از حملات

با پیشرفت تکنالوژی، تهدیدات دیجیتلی نیز پیچیده‌تر شده است، بنابراین استفاده از سخت‌افزارهای امنیتی پیشرفته اهمیت زیادی پیدا کرده است. دانش آموزان باید بتوانند تجهیزات مختلف را بررسی کرده و قضاوت کنند که کدام برای یک خانه یا سازمان مناسب است. امروزه با افزایش استفاده از وسایل هوشمند(IoT) ، تنها یک روتر ساده کافی نیست و نیاز به سیستم‌های قوی‌تر مانند Firewall مستقل، سیستم‌های نظارتی و کنترول شبکه احساس می‌شود. هدف این است که دانش آموزان بتوانند بر اساس نیاز، هزینه و امنیت بهترین انتخاب را پیشنهاد دهند.

انواع تکنالوژی‌های سخت‌افزاری

- Router پیشرفته (Advanced Router)
- Hardware Firewall
- IDS / IPS (سیستم تشخیص و جلوگیری نفوذ)
- Network Monitoring Devices
- IoT Security Devices
- NAS (ذخیره‌سازی امن شبکه)

آیا روترهای ساده کافی است؟

در گذشته:

- روترهای ساده کافی بود

اما امروز:

- دستگاه‌های هوشمند زیاد شده (IoT ،Smart TV ،Camera)
- خطرات افزایش یافته

نتیجه:

روتر ساده همیشه کافی نیست

نقش [1](IoT) وسایل هوشمند

وسایل مانند:

- Smart TV
- Camera
- Smart devices

اگر امنیت نداشته باشد:

- هک می‌شود

NAS (ذخیره‌سازی امن شبکه)
برای مطالعه جزئیات بیشتر در گوگل:
NAS (Network Attached Storage)
جستجو کنید!

[1] IoT: Internet of Things انترنت اشیاء

- معلومات شخصی افشا می‌شود.

چگونه بفهمیم کسی به Wi-Fi وصل است؟

- بررسی لیست دستگاه‌ها در Router
- کند شدن اینترنت
- استفاده غیرعادی دیتا

باید دستگاه‌های ناشناس را بلاک کرد.

مفهوم

DMZ یک بخش جدا در شبکه است که:

- دستگاه‌های عمومی را از شبکه اصلی جدا می‌کند
- امنیت شبکه داخلی را افزایش می‌دهد

مثال:

Server در DMZ[1] قرار می‌گیرد تا اگر هک شود، شبکه اصلی محفوظ بماند.

Ports آسیب‌پذیر

Port ها دروازه‌های ارتباطی هستند:

- Port باز = خطر
- Port بسته = امنیت

اگر Port ها مدیریت نشود، هکرها می‌توانند وارد شوند.

آیا امنیت کامل ممکن است؟

حتی:

- بانک‌ها و شرکت‌های بزرگ هم هک می‌شوند

نتیجه:

- امنیت کامل وجود ندارد
- فقط می‌توان خطر را کاهش داد

مثال واقعی

فرض کنید یک خانه:

- فقط Router ساده دارد
- چندین دستگاه IoT وصل است

خطر:

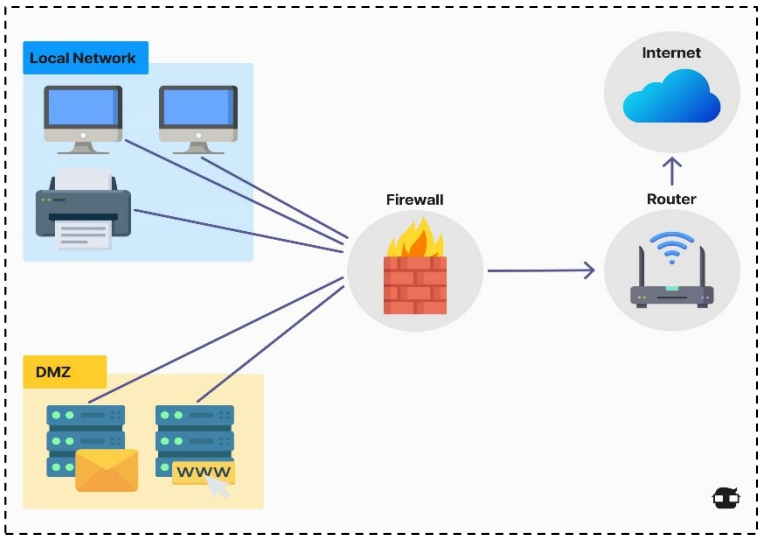
[1] DMZ (demilitarized zone)

- هک شدن Camera
- دسترسی به شبکه

اما اگر:

- Firewallجدا + Monitoring

امنیت بیشتر...



DMZ (demilitarized zone)

مقایسه سخت‌افزارها

نوع دستگاه	مزیت	ضعف	مناسب برای
ساده Router	ارزان	امنیت محدود	خانه کوچک
Advanced Router	امنیت بهتر	هزینه متوسط	خانه مدرن
Hardware Firewall	بسیار امن	هزینه بالا	شرکت‌ها
IDS/IPS	تشخیص حمله	پیچیده	شبکه پیشرفته
NAS	ذخیره امن	نیاز تنظیم	دیتا مهم

ویژگی‌ها و قیمت (نمونه)

دستگاه	امنیت	قیمت	توضیح
عادی Router	متوسط	کم	استفاده ساده
Firewall	بالا	زیاد	امنیت حرفه‌ای
Monitoring Tool	بالا	متوسط	نظارت شبکه

تحلیل تکنالوژی‌های نرم‌افزاری برای جلوگیری از حملات

در کنار سخت‌افزار، نرم‌افزارهای امنیتی نقش بسیار مهمی در محافظت از مواد دیجیتلی دارند. این نرم‌افزارها به‌صورت مداوم به‌روزرسانی می‌شوند تا در برابر تهدیدات جدید مقابله کنند. دانش آموزان باید بتوانند بررسی کنند که از چه نرم‌افزارهایی استفاده می‌کنند، این نرم‌افزارها چقدر مؤثر است و

چگونه می‌توان عملکرد آن‌ها را ارزیابی کرد. همچنان باید بدانند که بدون Update و Patch، حتی بهترین نرم‌افزار نیز ضعیف می‌شود.

انواع نرم‌افزارهای امنیتی

- Antivirus Software
- Anti-malware Tools
- Firewall Software
- Encryption Software
- Password Manager
- VPN (Virtual Private Network)
- System Monitoring Software

دانش آموزان باید بتوانند توضیح دهند که:

- از کدام استفاده می‌کنند
- چرا آن را انتخاب کرده‌اند
- چقدر مؤثر است

نقش Update وPatch

- نسخه جدید نرم‌افزار **Update**
- اصلاح مشکلات امنیتی **Patch**

اگر این‌ها انجام نشود:

- سیستم آسیب‌پذیر می‌شود
- هکرها از ضعف استفاده می‌کنند

چگونه عملکرد نرم‌افزار را ارزیابی کنیم؟

دانش آموزان باید این موارد را بررسی کنند:

- آیا نرم‌افزار **Update** است؟
- آیا **هشدار (Alert)** می‌دهد؟
- آیا **Scan Reports** دارد؟
- آیا سیستم را کند نمی‌کند؟

این‌ها نشان می‌دهد که نرم‌افزار درست کار می‌کند.

Exploits چیست؟

Exploitیعنی استفاده از یک ضعف در سیستم برای حمله

مثال:

اگر نرم‌افزار Update نشود → هکر از همان ضعف استفاده می‌کند.

خدمات(Internet Service Provider) ISP

بسیاری ازISP ها خدمات امنیتی ارائه می‌کنند:

- Firewall شبکه
- Spam Filtering
- Parental Control
- Monitoring ترافیک

این خدمات یک لایه امنیت اضافی ایجاد می‌کند.

- نبود ویروس یا فعالیت مشکوک
- آپدیت بودن نرم‌افزار

پیگیری تهدیدات جدید

برای امنیت بهتر باید:

- نرم‌افزار را همیشه Update کرد
- اخبار امنیتی را دنبال کرد
- ازPatch های جدید استفاده کرد

تهدیدات همیشه در حال تغییر است

مثال واقعی

فرض کنید:

Antivirus نصب است اما Update نشده

نتیجه: نمی‌تواند ویروس جدید را تشخیص دهد

Antivirus آپدیت شده

سیستم محافظت می‌شود.

ارزیابی نرم‌افزارها

دانش آموزان باید بتوانند بگویند:

- کدام نرم‌افزار بهتر است
- چرا مناسب است
- چه محدودیت دارد

NOD 32

Avast

KASPERSKY

McAffee

نوت:

آیکن های نرم افزارهای Antivirus را در سمت چپ صفحه می‌بنید تمام این نرم افزارها تجاری است نسخه رایگان آنها بصورت محدود در حدود یک هفته یا یکماه کار آمد دارد. در غیر آنصورت همین نرم افزارها بخاطر خریداری نسخه پولی تخینک ها را در بگروند استفاده میکنند که سیستم کند شده و شما را وارد کند بخاطر امنیت و سرعت سیستم نسخه پولی

را خریداری کنید. بهتر گزینه در سیستم عامل ویندوز همان Windows Defender خود سیستم میباشد.

مقایسه نرم‌افزارهای امنیتی

نرم‌افزار	وظیفه	مزیت	ضعف
Antivirus	حذف ویروس	ساده	Update نیاز
Anti-malware	شناسایی بدافزار	دقیق	گاهی کند
Firewall	کنترول شبکه	محافظت قوی	نیاز تنظیم
Encryption	رمزگذاری	امنیت بالا	پیچیده
VPN	مخفی کردن ارتباط	امنیت آنلاین	سرعت کمتر
Password Manager	مدیریت رمز	آسان	نیاز اعتماد

مقایسه نرم‌افزارها(Suitability + Cost)

نرم‌افزار	مناسب برای	ویژگی	هزینه	نتیجه
عادی Antivirus	کاربران خانگی	اسکن ویروس	کم	امنیت متوسط
Advanced Security Suite	کاربران حرفه‌ای	چندین ابزار	متوسط/زیاد	امنیت بالا
VPN	استفاده آنلاین	مخفی‌سازی	متوسط	امنیت اتصال
Password Manager	همه	مدیریت رمز	کم	امنیت حساب

ارزیابی تهدیدات فعلی برای مواد دیجیتلی شخصی

در این بخش، دانش آموزان باید بتوانند تهدیدات واقعی که به معلومات شخصی آن‌ها مربوط می‌شود را تحلیل و ارزیابی (Evaluate) کنند. این یعنی فقط شناخت تهدید کافی نیست، بلکه باید مشخص شود کدام تهدید خطرناک‌تر است و چرا. برای این کار، استفاده از Log Files (ثبت فعالیت‌ها) بسیار مهم است، زیرا این فایل‌ها نشان می‌دهند که چه نوع حملات یا فعالیت‌های مشکوک در سیستم رخ داده است. دانش آموزان باید بتوانند این معلومات را بررسی کرده و بر اساس آن تصمیم بگیرند که کدام تهدید بیشترین خطر را دارد.

Log Files چیست؟

Log Files فایل‌هایی هستند که تمام فعالیت‌های سیستم و شبکه را ثبت می‌کنند.

این فایل‌ها کمک می‌کند تا:

- حملات شناسایی شود
- رفتار مشکوک دیده شود
- امنیت سیستم ارزیابی گردد

مثال:
سیستم مانند **Fail2Ban** در لینوکس حملات مکرر را شناسایی کرده و IP را موقتاً بلاک می‌کند.

نقش سیستم‌عامل در امنیت
سیستم‌عامل‌ها (Operating Systems) خودشان ابزارهای امنیتی دارند:

- Firewall داخلی
- Security Logs
- Access Control

این‌ها یک لایه امنیت اضافی ایجاد می‌کند.

حملات شبکه(Network Attacks)
تلاش برای نفوذ به سیستم از طریق اینترنت
معمولاً در Log ثبت می‌شود

حملات رویWeb Server
اجرایScript های مخرب
هدف: دسترسی به سیستم

تهدیدات ناشی از عادت‌های بد
بعضی خطرات از خود کاربر است:

- باز گذاشتن حساب (Logged in)
- شریک‌سازی رمز
- استفاده از Wi-Fi عمومی

این‌ها بسیار خطرناک است

مثال واقعی
فرض کنید:

- در Log File دیده می‌شود که یک IP چند بار تلاش Login کرده

نتیجه:
حمله Brute Force
اگر Fail2Ban فعال باشد:
IP بلاک می‌شود

چگونه تهدیدات را ارزیابی کنیم؟

دانش آموزان باید بررسی کنند:

- چند بار حمله انجام شده؟
- از کجا آمده؟
- چه نوع حمله است؟
- آیا موفق بوده؟

ارزیابی تهدیدات

نوع تهدید	منبع	سطح خطر	دلیل
Brute Force	اینترنت	زیاد	تلاش مکرر
Phishing	ایمیل	زیاد	فریب کاربر
عمومی Wi-Fi	شبکه	بسیار زیاد	دسترسی آسان
اشتراک رمز	کاربر	بسیار زیاد	دسترسی مستقیم
ویروس	دانلود	زیاد	آسیب سیستم

Log Analysis

مورد	معنی	اقدام
Failed Login	تلاش ناموفق	بررسی
Multiple Attempts	حمله	بلاکIP
Unknown Access	دسترسی ناشناس	تغییر رمز
Suspicious Activity	فعالیت مشکوک	بررسی کامل

ارزیابی بهترین روش‌های محافظت و پیشنهاد پروتکل‌ها

در این بخش، دانش آموزان باید از تمام دانسته‌های قبلی خود استفاده کنند تا بهترین روش‌های محافظت (Protection Methods) را انتخاب و ارزیابی کنند. هدف فقط شناخت ابزارها نیست، بلکه ایجاد یک پروتکل (Protocol) یعنی مجموعه‌ای از قوانین و مراحل مشخص است که اگر رعایت شود، خطر حملات کاهش می‌یابد. دانش آموزان باید بتوانند تهدیدات را با روش‌های محافظتی مرتبط ساخته و یک سیستم عملی و قابل اجرا طراحی کنند.

پروتکل چیست؟

Protocolیعنی یک مجموعه از قوانین و دستورالعمل‌ها که برای رسیدن به یک هدف مشخص استفاده می‌شود.
در اینجا هدف :**محافظت از معلومات دیجیتلی**
مثال ساده:

- همیشه رمز قوی استفاده کن
- لینک ناشناس را باز نکن

روش‌های محافظتی مهم

- استفاده از HTTPS به‌جای HTTP
- استفاده از Firewall
- استفاده از Encryption
- فعال‌سازی Two-Factor Authentication
- استفاده از VPN
- Update منظم سیستم

نوت: دانش آموزان ویدیوها و رهنمایی های منتور را بصورت کامل تعقیب و تمرین کنند.

ارتباط تهدید و روش محافظتی
دانش آموزان باید نشان دهند که:
هر تهدید → یک روش محافظتی مناسب دارد.

جدول ذیل حملات و روش مقابله با آن مقایسه شده است.

تهدید	روش محافظتی	توضیح
Phishing	آموزش + دقت	کلیک نکردن لینک
Wi-Fi عمومی	VPN	مخفی‌سازی دیتا
Brute Force	2FA + رمز قوی	جلوگیری از ورود
ویروس	Antivirus	حذف بدافزار
Data Theft	Encryption	محافظت معلومات

طراحی پروتکل شخصی
دانش آموزان باید بتوانند یک پروتکل برای خود یا دیگران طراحی کنند. این پروتکل باید:

- ساده
- قابل اجرا
- موثر باشد

نمونه پروتکل امنیتی (برای خانه یا مکتب)

قوانین عمومی:

- استفاده از رمز قوی (حداقل 8 کاراکتر)
- عدم شریک‌سازی رمز
- فعال‌سازی 2FA

استفاده از اینترنت:

- فقط استفاده از HTTPS
- عدم استفاده از Wi-Fi عمومی بدون VPN
- بررسی لینک‌ها قبل از کلیک

سیستم و نرم‌افزار:

- Update منظم
- نصب Antivirus
- فعال بودن Firewall

مدیریت دیتا:

- Backup منظم
- استفاده از Cloud امن
- Encryption فایل‌های مهم

مثال واقعی

یک دانش آموز:

بدون پروتکل:

- رمز ساده
- بدون Update

نتیجه: هک شدن

با پروتکل:

- 2FA
- Antivirus
- VPN

نتیجه: امنیت بالا

به داشته باشید که شناسایی دو مرحله توسط گزینه های مختلف انجام میشود:

1. **از طریق پیامک که به شماره تلیفون انجام میشود خیلی معمول است**
2. **از طریق ایمیل نیز انجام میشود**
3. **از طریق اپلیکشن های Google Authenticator , Microsoft Auth**
4. **از طریق Passkey و جدول کدهای که ازپیش توسط اپلیکشن و شرکت به شما داده میشود دانلود یا چاپ میکند.**

پیشنهاد سیستم‌ها برای تقویت امنیت

در این مرحله، دانش آموزان باید تمام دانسته‌های قبلی خود را یکجا استفاده کنند تا بتوانند نقاط ضعف سیستم‌ها را شناسایی کرده و راه‌حل‌های عملی برای بهبود امنیت پیشنهاد دهند. هدف فقط شناخت مشکل نیست، بلکه ارائه پیشنهادهای دقیق و منطقی است. این پیشنهادها باید بر اساس تحلیل، شواهد (Findings) و تجربه عملی باشد. دانش آموزان باید مانند یک مشاور (Consultant) فکر کنند و برای یک خانه، مکتب یا شرکت راه‌حل مناسب ارائه دهند.

شناسایی نقاط ضعف

قبل از هر پیشنهاد، باید ضعف‌ها مشخص شود:

- رمزهای ضعیف
- نبود Firewall
- استفاده از Wi-Fi ناامن
- عدم Update سیستم
- نبود Backup

بدون شناخت مشکل، راه‌حل درست ممکن نیست

روش تحلیل سیستم

دانش آموزان باید بررسی کنند:

- چه تهدیداتی وجود دارد؟
- سیستم فعلی چه ضعف‌هایی دارد؟
- چه ابزارهایی استفاده شده؟
- آیا امنیت کافی است؟

پیشنهاد سیستم‌های امنیتی

بر اساس تحلیل، دانش آموزان باید سیستم‌های بهتر پیشنهاد دهند. این سیستم‌ها می‌تواند شامل:

- ارتقای Router به مدل پیشرفته
- استفاده از Hardware Firewall

- نصب Advanced Antivirus
- استفاده از Cloud Backup
- فعال‌سازی 2 FA

Firewall Devices

مثال واقعی

فرض کنید یک شرکت کوچک:

وضعیت فعلی:

- رمز ساده
- بدون Backup
- Wi-Fiمشترک

سرقت دیتا

پیشنهاد:

- رمز قوی 2 FA+
- Backup خودکار
- شبکه جدا برای کارمندان

نتیجه: امنیت بهتر

سیستم پیشنهادی

بخش	سیستم پیشنهادی	هدف
شبکه	Advanced Router	کنترول بهتر
امنیت	Firewall	جلوگیری از حمله
نرم‌افزار	Antivirus	حذف ویروس
دیتا	Cloud Backup	حفظ معلومات
دسترسی	2FA	امنیت حساب

نوت: به یاد داشت باشید این مورد بر فعالیت شخصی نیز صدق میکند همانطوریکه شما در تحت عنوان (تأثیر فعالیت‌های آنلاین بر امنیت و معلومات شخصی) مطالعه نمودند.

ارائه مشوره مؤثر برای امنیت آنلاین

در این مرحله، دانش آموزان باید نشان دهند که می‌توانند از تمام دانش خود استفاده کرده و به دیگران **مشوره واضح، منطقی و قابل اجرا (Cogent Advice)** بدهند. هدف این است که دانش آموز فقط برای

خود امنیت را رعایت نکند، بلکه بتواند دیگران (دوستان، خانواده، مکتب یا شرکت‌ها) را نیز راهنمایی کند. این مشوره باید ساده، عملی و بر اساس تهدیدات واقعی باشد، نه فقط معلومات نظری.

ویژگی‌های یک مشوره خوب

- واضح و قابل فهم
- عملی و قابل اجرا
- مرتبط با خطرات واقعی
- مختصر اما مفید

موضوعات مهم برای مشوره

دانش آموزان باید در مورد موضوعات مهم مانند:

- رمزهای قوی
- فیشینگ **(Phishing)**
- استفاده از **Wi-Fi** عمومی
- محافظت از معلومات شخصی
- استفاده از **Antivirus** و **Update**

مشوره بدهند تا دیگران بتوانند خود را محافظت کنند.

نمونه مشوره برای کاربران

امنیت حساب‌ها

- از رمز قوی استفاده کنید
- رمز را با کسی شریک نسازید
- **2FA** را فعال کنید

استفاده از اینترنت

- فقط سایت‌های **HTTPS** را استفاده کنید
- روی لینک ناشناس کلیک نکنید
- از **Wi-Fi** عمومی با احتیاط استفاده کنید

امنیت سیستم

- **Antivirus** نصب کنید
- سیستم را **Update** نگه دارید
- **Firewall** را فعال کنید

مثال واقعی

فرض کنید یک دانش آموز به دوست خود مشوره می‌دهد:

قبل:

- دوستش رمز ساده داشت
- روی هر لینک کلیک می‌کرد

بعد از مشوره:

- رمز قوی استفاده کرد
- لینک‌ها را بررسی می‌کند

نتیجه: امنیت بهتر

استفاده از Survey یا Questionnaire

دانش آموزان می‌توانند:

- یک پرسشنامه طراحی کنند
- از افراد یا شرکت‌ها سوال بپرسند
- وضعیت امنیت را ارزیابی کنند

مثال سوالات:

- آیا از 2 FA استفاده می‌کنید؟
- آیا سیستم خود را **Update** می‌کنید؟

جدول ارزیابی کاربران

سوال	بلی	نخیر	نتیجه
استفاده از رمز قوی	✓	✕	امنیت خوب
استفاده از 2FA	✓	✕	امنیت بالا
Update سیستم	✓	✕	محافظت بهتر
استفاده Wi-Fi عمومی	✓	✕	خطر

ارائه مشوره(Report / Video)

دانش آموزان می‌توانند:

- گزارش **(Report)** بنویسند
- ویدیو **(Video)** بسازند
- یا به‌صورت حضوری ارائه دهند

هدف: انتقال واضح معلومات

کمک به دیگران

دانش آموزان می‌توانند:

- به دوستان و خانواده کمک کنند
- به یک شرکت مشوره دهند
- منابع معتبر معرفی کنند

مثال:
معرفی سایت‌های امنیتی یا مراکز گزارش‌دهی
نکات مهم برای دانش آموزان

- مشوره باید ساده باشد
- همه مردم متخصص نیستند
- هدف: جلوگیری از مشکل

جدول لغات بخش امنیتی دیجیتالی

شماره	اصطلاح (English)	معنی دری	کاربرد عملی
1	Cybersecurity	امنیت سایبری	محافظت سیستم و دیتا
2	Data	دیتا	معلومات شخصی و کاری
3	Information Security	امنیت معلومات	محافظت از معلومات
4	Malware	بدافزار	تخریب یا سرقت دیتا
5	Virus	ویروس	آسیب سیستم
6	Worm	کرم (نرم افزاری)	انتشار خودکار در شبکه
7	Trojan	تروجان	نرم‌افزار مخفی مخرب
8	Ransomware	باج‌افزار	قفل کردن دیتا
9	Spyware	نرم‌افزار جاسوسی	نظارت مخفی
10	Antivirus	ضد ویروس	حذف ویروس
11	Firewall	دیوار آتش	جلوگیری از نفوذ
12	Encryption	رمزگذاری	محافظت دیتا
13	Decryption	رمزگشایی	باز کردن رمز
14	Password	رمز عبور	محافظت حساب
15	Strong Password	رمز قوی	جلوگیری از هک
16	2FA	تأیید دو مرحله‌ای	امنیت بیشتر
17	Authentication	تأیید هویت	شناسایی کاربر
18	Authorization	اجازه دسترسی	تعیین سطح دسترسی
19	Access Rights	سطح دسترسی	کنترول کاربران
20	Read Only	فقط خواندن	بدون تغییر
21	Write	نوشتن	امکان تغییر
22	Full Control	کنترول کامل	دسترسی کامل
23	Phishing	فیشینگ	فریب کاربر
24	Pharming	فارمینگ	هدایت به سایت جعلی
25	Hacking	هک	دسترسی غیرمجاز

26	Brute Force Attack	حمله حدس رمز	امتحان رمز
27	Social Engineering	مهندسی اجتماعی	فریب انسان
28	Identity Theft	سرقت هویت	سوءاستفاده معلومات
29	Data Breach	نشت دیتا	افشای معلومات
30	Online Fraud	تقلب آنلاین	سرقت پول
31	Cyberbullying	آزار آنلاین	اذیت اینترنتی
32	Spam	پیام ناخواسته	ایمیل اضافی
33	VPN	شبکه خصوصی	امنیت اتصال
34	Proxy	واسطه اینترنت	تغییر مسیر
35	HTTPS	پروتکل امن	ارتباط امن
36	HTTP	پروتکل عادی	بدون امنیت
37	SSL/TLS	رمزگذاری ویب	امنیت سایت
38	Patch	اصلاح امنیتی	رفع ضعف
39	Update	بروزرسانی	بهبود سیستم
40	Exploit	سوءاستفاده از ضعف	حمله
41	Vulnerability	آسیب‌پذیری	نقطه ضعف
42	Threat	تهدید	خطر
43	Risk	ریسک	احتمال خطر
44	Log File	ثبت فعالیت	بررسی حمله
45	Monitoring	نظارت	کنترول سیستم
46	IDS	تشخیص نفوذ	شناسایی حمله
47	IPS	جلوگیری نفوذ	توقف حمله
48	DMZ	منطقه جدا	امنیت شبکه
49	Port	دروازه ارتباط	مسیر دیتا
50	Router	روتر	مدیریت شبکه
51	IoT	دستگاه هوشمند	اینترنت اشیا
52	Backup	نسخه پشتیبان	جلوگیری از ضایع
53	Cloud Storage	ذخیره ابری	نگهداری آنلاین
54	Local Storage	ذخیره محلی	ذخیره در دستگاه
55	Public Wi-Fi	وای‌فای عمومی	خطر بالا
56	Private Network	شبکه خصوصی	امنیت بهتر
57	Secure Protocol	پروتکل امن	انتقال امن
58	Digital Footprint	ردپای دیجیتلی	آثار آنلاین
59	Privacy	حریم خصوصی	حفاظت معلومات
60	Acceptable Use Policy (AUP)	پالیسی استفاده	قوانین استفاده

61	Cybercrime	جرایم سایبری	جرم اینترنتی
62	Data Protection	محافظت دیتا	امنیت معلومات
63	Encryption Key	کلید رمز	باز کردن دیتا
64	Authentication Token	کُد تأیید	ورود امن

جدول منابع (کتاب‌ها و مقالات امنیت دیجیتلی)

#	نام کتاب / مقاله	دانلود
1	**Cybersecurity Essentials – Charles J. Brooks**	https://library.books24x7.com/resource/book/9781119362397
2	**Introduction to Computer Security – Michael Goodrich**	https://pdfcoffee.com/qdownload/introduction-to-computer-security-goodrich-tamassia-pearson-new-international-edition-pdfdrivecom-pdf-2-pdf-free.html
3	**Information Security Principles**	https://www.opentextbooks.org.hk/ditatopic/3551
4	**Data Protection and Privacy Issues**	https://www.sciencedirect.com/science/article/pii/S1877050919315533
4	**Phishing Attacks and Countermeasures**	https://www.researchgate.net/publication/220892354
6	**Security Issues in Cloud Computing**	https://arxiv.org/pdf/1303.4814.pdf

فصل چهارم

برنامه‌ریزی، تطبیق و ارزیابی سیستم‌های دیجیتلی

شرایط فصل چهارم:

- ساعت های درسی: 50 ساعت
- ساعت های اضافی: 5 ساعت
- مجموع ساعت های درسی: 50 ساعت

در این فصل خواهی آموخت:

Strand 1

دانش آموز درک می‌کند که یک پروفایل دیجیتلی چگونه باید ساخته شود تا مهارت‌ها و دانش خود را به مخاطبین مختلف نشان دهد. همچنین نیازها و توقعات مخاطب را می‌شناسد، ابزار و نوع فایل مناسب انتخاب می‌کند و خطرات امنیتی معلومات شخصی را درک می‌کند.

Strand 2

دانش آموز یک پلان منظم برای ساخت پروفایل دیجیتلی تهیه می‌کند که شامل انتخاب برنامه‌ها **(Applications)** و نوع فایل‌ها **(File Types)** باشد تا کار به‌صورت درست و امن پیش برود.

Strand 3

دانش آموز یک پروفایل دیجیتلی عملی می‌سازد که مطابق نیاز بازار کار باشد، مهارت‌های خود را نشان دهد و معلومات را به‌صورت امن و مناسب برای مخاطب نمایش ده

Strand 4

دانش آموز یک سیستم تست امنیت ایجاد می‌کند تا از امنیت و کارایی پروفایل خود مطمئن شود، مانند استفاده از رمز قوی، تغییر منظم رمز، عدم شریک‌سازی معلومات و شناخت حملات مثل **brute force.**

Strand 5

دانش آموز امنیت و کارایی پروفایل خود را تحلیل و ارزیابی می‌کند و می‌فهمد که چگونه سیستم‌ها مثل**Firewall** در مقابل حملات عمل می‌کنند و چگونه می‌تواند پروفایل خود را بهتر سازد.

Strand	خلاصه
1	درک پروفایل دیجیتلی و مخاطب
2	پلان‌سازی پروفایل
3	ساخت پروفایل عملی
4	تست امنیت پروفایل
5	ارزیابی و بهبود

1. دانستن این‌که یک پروفایل دیجیتالی چگونه باید باشد تا دانش و مهارت های مرا به شکل امن و مناسب به افراد مختلف نشان دهد.

درک ارائه مناسب خود در آنلاین

در این بخش، دانش آموز باید یاد بگیرد که چگونه خود را در یک پروفایل دیجیتلی مثل CV آنلاین، LinkedIn یا ePortfolio به‌صورت مناسب معرفی کند. مهم‌ترین نکته این است که بداند مخاطب (Audience)کی ها است، زیرا نوع ارائه (زبان، طراحی، محتوا) باید مطابق مخاطب تغییر کند. همچنین در فضای آنلاین، مخاطبین می‌توانند از فرهنگ‌ها، زبان‌ها و شرایط مختلف (مثل افراد دارای ناتوانی) باشند، بنابراین باید احترام، سادگی و دسترسی‌پذیری رعایت شود.

درک مخاطب (Audience)

دانش آموز باید بداند:

- آیا مخاطب استاد است یا کارفرما؟
- آیا مخاطب داخلی است یا بین‌المللی؟
- چه سطح دانش دارد؟

چون هر مخاطب توقع متفاوت دارد.

تفاوت مخاطب آنلاین و محلی

- مخاطب محلی → محدود و قابل شناخت
- مخاطب آنلاین → گسترده و ناشناخته

پس در آنلاین باید دقت بیشتر شود.

نکات کلیدی

دانش آموز باید موارد زیر را رعایت کند:

- انتخاب ابزار مناسب **(Presentation Tools)**
- استفاده از رنگ‌های مناسب
- استفاده از فونت واضح و ساده
- رعایت تفاوت‌های فرهنگی
- استفاده از زبان محترمانه و ساده
- در نظر گرفتن افراد دارای ناتوانی

دسترسی‌پذیری (Accessibility)

در طراحی پروفایل دیجیتلی باید به افرادی که:

- مشکل بینایی دارند
- مشکل شنوایی دارند توجه شود

مثال:
- استفاده از فونت بزرگ
- استفاده از رنگ‌های واضح
- اضافه کردن توضیح برای تصاویر

حساسیت فرهنگی و زبانی

دانش آموز باید:
- از کلمات مناسب استفاده کند
- از محتواهای حساس خودداری کند
- فرهنگ‌های مختلف را احترام کند

مثال واقعی

یک دانش آموز برای یک شرکت خارجی پروفایل می‌سازد:

اشتباه:
- استفاده از زبان محلی
- رنگ‌های نامناسب
- فونت پیچیده

درست:
- زبان ساده انگلیسی
- طراحی ساده
- فونت واضح

نتیجه: بهتر دیده می‌شود.

خلاصه نکات کلیدی:

بخش	نکته	هدف
مخاطب	شناخت مخاطب	ارائه بهتر قابل فهم مناسب مخاطب
ابزار	انتخاب درست	نمایش حرفه‌ای
رنگ	مناسب و ساده	خوانایی
فونت	واضح	فهم آسان
فرهنگ	احترام	جلوگیری از سوءتفاهم
دسترسی	کمک به همه	استفاده آسان

درک مشکلات آنلاین و نحوه بیان نمودن آن و از چی کسی کمک بگیریم؟

در این بخش، دانش آموز باید یاد بگیرد که وقتی در فضای آنلاین با مشکل یا سوال روبه‌رو می‌شود، **به چه منابع و افراد مراجعه کند .**مهم است که دانش آموز بداند اینترنت منابع زیادی دارد، اما همه آن‌ها قابل اعتماد نیستند.
بنابراین باید بتواند بین منابع مفید و منابع نادرست فرق بگذارد. همچنان باید بداند که فقط اینترنت کافی نیست و گاهی منابع واقعی **(Offline)** نیز بسیار مهم و قابل اعتماد هستند.

منابع آنلاین
دانش آموز می‌تواند از منابع آنلاین مانند:
- فورم‌های آموزشی
- گروه‌های تخصصی
- سایت‌های رسمی

استفاده کند، اما باید **با دقت و بررسی.**

نکته مهم: تشخیص منبع معتبر
دانش آموز باید:
- به هر معلومات باور نکند
- منبع را بررسی کند
- از سایت‌های معتبر استفاده کند

چون بعضی معلومات غلط یا خطرناک است. این خیلی مهم است که شما اطلاعات دقیق و اصلی را از هم تفکیک کنید. بطور نمونه شما باید وقت اطلاعات را از هوش مصنوعی میگیرد حتما منابع دیگر را همان موضوع را هوش مصنوعی داده بررسی کنید.

منابع غیرآنلاین (Offline)
دانش آموز باید بداند که منابع واقعی هم مهم است:
- مشاور شغلی **(Careers Officer)**
- کتابخانه مکتب
- فامیل و افراد با تجربه
- شرکت‌های محلی

این منابع معمولاً قابل اعتمادتر هستند
- استفاده از فورم‌های معتبر
- بررسی صحت معلومات
- سوال پرسیدن از افراد متخصص
- استفاده از منابع مختلف (آنلاین و حضوری)

مثال واقعی
یک دانش آموز مشکل نرم‌افزاری دارد:
اشتباه:
- اعتماد به یک سایت ناشناس
- دانلود فایل مشکوک

درست:
- پرسیدن در یک فورم معتبر
- سوال از استاد یا دوست با تجربه

نتیجه: حل مشکل بدون خطر

درک سیستم‌ها، برنامه‌ها و نوع فایل‌ها برای پروفایل دیجیتلی

در این بخش، دانش آموز باید بفهمد که برای ساخت یک پروفایل دیجیتلی موفق، فقط محتوا مهم نیست، بلکه انتخاب درست سیستم‌ها (**Systems**)، برنامه‌ها (**Applications**) و نوع فایل‌ها (**File Types**) نیز بسیار مهم است. هر پروژه یا هدف، نیاز به ابزار و فایل مناسب دارد. اگر انتخاب درست نباشد، ممکن است کیفیت کار پایین بیاید یا دیگران نتوانند آن را باز و استفاده کنند.

شناخت سیستم‌ها و برنامه‌ها
دانش آموز باید بداند که:
- برای نوشتن **Word** → یا **Google Docs**
- برای ارائه **PowerPoint** →
- برای طراحی **Photoshop** → یا **Canva**
- برای دیتا **Excel** → یا **Database**

انتخاب ابزار باید مطابق هدف باشد.

درک نوع فایل‌ها(File Types)
هر فایل خصوصیات خاص خود را دارد:
- **PDF** → مناسب برای اشتراک‌گذاری
- **JPG/PNG** → تصاویر
- **MP4** → ویدیو
- **MP3** → صدا

هر فایل برای یک کار خاص مناسب است و با برنامه خواص استفاده میشود.

مدیریت فایل‌ها
دانش آموز باید درک کند:
- فایل‌های مختلف مدیریت متفاوت دارند

- بعضی فایل‌ها حجم زیاد دارند
- بعضی نیاز به نرم‌افزار خاص دارند

مثال: فایل ویدیو بزرگ‌تر از فایل متن است

ارتباط با ذخیره‌سازی(Storage)

اگر فایل‌ها بزرگ باشد:

- نیاز به حافظه بیشتر **(GB)**
- استفاده از **Cloud Storage**
- انتخاب پلان ذخیره مناسب

نکات ذیل در انتخاب برنامه برای فایل های مخصوص باید مدنظر گرفته شود:

- انتخاب برنامه مناسب
- انتخاب فایل مناسب
- توجه به حجم فایل
- توجه به نرم‌افزار مورد نیاز
- انتخاب سیستم ذخیره مناسب

مثال واقعی

یک دانش آموز پروفایل می‌سازد:

اشتباه:

- استفاده از فایل‌های سنگین و غیرقابل باز شدن
- انتخاب فرمت نامناسب

درست:

- استفاده از **PDF** برای اسناد
- **JPG** برای تصاویر
- **MP4** برای ویدیو

نتیجه: پروفایل حرفه‌ای و قابل استفاده

جدول انواع فایل‌ها

نوع فایل	کاربرد	مزیت
PDF	اسناد	قابل باز شدن در همه جا
JPG / PNG	تصویر	حجم مناسب
MP4	ویدیو	کیفیت خوب
MP3	صدا	حجم کم
DOCX	متن قابل ویرایش	قابل تغییر

درک خطرات رایج برای معلومات شخصی در حضور آنلاین

در این بخش، دانش آموز باید به‌صورت جدی درک کند که داشتن یک حضور آنلاین **(Online Presence)** مثل استفاده از شبکه‌های اجتماعی، **ePortfolio** یا ارسال معلومات در **Cloud** ، فقط یک فرصت نیست بلکه یک مسئولیت امنیتی نیز است. هر معلوماتی که آنلاین نشر می‌شود، در واقع از کنترول فرد خارج می‌شود و ممکن است برای همیشه در اینترنت باقی بماند. علاوه بر این، اگر پروفایل یا فایل‌ها به‌درستی محافظت نشود، افراد دیگر می‌توانند به آن دسترسی پیدا کرده، آن را تغییر دهند یا حتی از آن سوءاستفاده کنند. بنابراین، دانش آموز باید یاد بگیرد که چگونه با استفاده از سطح دسترسی **(Permissions)** ، قفل‌سازی فایل‌ها و تنظیمات امنیتی از معلومات خود محافظت کند.

ماندگاری معلومات در اینترنت

یکی از مهم‌ترین خطرات این است که:

هر چیزی که آنلاین نشر شود:

- ممکن است توسط دیگران ذخیره **(Save)** شود
- ممکن است **Screenshot** گرفته شود
- ممکن است دوباره نشر شود

در دنیای دیجیتال، حتی اگر فایلی را حذف کنید، این به معنی از بین رفتن کامل آن نیست. در بسیاری از موارد، اطلاعات قابل بازیابی هستند و ممکن است دوباره به دست دیگران برسند. به‌طور کلی می‌توان گفت هر چیزی که در فضای دیجیتال تولید یا منتقل می‌شود، به‌صورت کامل از بین نمی‌رود؛ مگر این‌که منبع آن به‌طور کامل نابود شود. برای مثال، اگر عکسی را با موبایل خود بگیرید و آن را در انترنت منتشر نکنید، این عکس همچنان در حافظه **(Memory Card)** یا حافظه داخلی باقی می‌ماند. تنها در صورتی که آن حافظه به‌طور فیزیکی نابود شود، می‌توان گفت اطلاعات کاملاً از بین رفته است. یکی از اشتباهات رایج این است که برخی افراد تصاویر شخصی را در موبایل خود نگه‌داری می‌کنند، با این تصور که چون در انترنت منتشر نشده، امن است.

اما این تصور کاملاً درست نیست. برای مثال، اگر موبایل خود را بفروشید، شخص خریدار می‌تواند با استفاده از نرم‌افزارهای ریکاوری، فایل‌های حذف‌شده را بازیابی کرده و حتی آن‌ها را در انترنت منتشر کند.

بنابراین، اگر نگران حفظ حریم خصوصی خود هستید، بهتر است از ذخیره‌سازی اطلاعات حساس در حافظه‌های دیجیتال خودداری کنید یا اقدامات امنیتی لازم را انجام دهید.

خطر تغییر یا دسترسی غیرمجاز

اگر امنیت پروفایل یا فایل‌ها ضعیف باشد:

- افراد دیگر می‌توانند وارد حساب شوند
- فایل‌ها را تغییر دهند
- یا اطلاعات را حذف کنند

این خطر در سیستم‌های **Cloud** و کار گروهی بسیار بیشتر است.

درک اهمیت Permissions و Access Control

دانش آموزان همانطوریکه در فصول قبلی مطالعه کردند بدانند که:

- همه افراد نباید به همه چیز دسترسی داشته باشند
- باید مشخص شود چه کسی فقط ببیند **(Read Only)**
- چه کسی تغییر بدهد **(Edit)**

این کار از سوءاستفاده جلوگیری می‌کند.

محافظت از فایل‌ها در سیستم‌های اشتراکی(Cloud)

در سیستم‌های **Cloud:**

- می‌توان فایل را با لینک **(URL)** شریک کرد
- می‌توان مشخص کرد چه کسی دسترسی داشته باشد
- می‌توان اعلان **(Notification)** برای افراد فرستاد

مثال: ارسال **CV** به کارفرما به‌صورت امن

نکات کلیدی (دقیق مطابق موضوع)

- معلومات آنلاین ممکن است دائمی باشد
- پروفایل باید محافظت شود
- دسترسی‌ها باید محدود و کنترول شود
- نشر معلومات باید با دقت انجام شود

مثال واقعی (واضح‌تر)

یک دانش آموز فایل پروژه خود را در **Cloud** شریک می‌کند:

اشتباه:

- دسترسی را روی **"Public"** می‌گذارد
- همه می‌توانند تغییر بدهند

نتیجه: فایل خراب می‌شود بعضی ممکن بعضی موضوعات و جزئیات را تغییر بدهند.

✅ درست:

- فقط **"Read Only"** برای دیگران
- **Edit** فقط برای خودش

نتیجه: امنیت حفظ می‌شود.

جدول خطرات دیتا در فضایی دیجیتالی

خطر	چگونه اتفاق می‌افتد	نتیجه
ماندگاری دیتا	ذخیره توسط دیگران	حذف مشکل
تغییر غیرمجاز	دسترسی آزاد	تخریب کار

اشتراک اشتباه	لینک عمومی	افشا معلومات
سوءاستفاده	استفاده نادرست	خطر شخصی

روش‌های محافظت

روش	توضیح	کاربرد عملی
Permissions	تعیین سطح دسترسی	فقط دیدن یا ویرایش
Password	رمز قوی	جلوگیری از ورود
File Lock	قفل فایل	جلوگیری از تغییر
Private Setting	تنظیم خصوصی	محدود کردن دسترسی

این دو جدول خطرات و روشهای جلوگیری از نشت و نفوذ به دیتا در فضایی دیجیتالی را خلاصه بیان میکند دانش آموزان میتوانند این جدول را حفظ کنند.

درک محدودیت‌های محلی و عمومی در انجام پروژه دیجیتلی

در این بخش، دانش آموز باید درک کند که هنگام انجام یک پروژه دیجیتلی (مثل ساخت **ePortfolio**)، همیشه آزادی کامل ندارد و ممکن است با محدودیت‌ها (**Constraints**) روبه‌رو شود. این محدودیت‌ها می‌تواند از طرف مکتب، سیستم، قوانین یا حتی دسترسی به ابزارها باشد. دانش آموز باید بتواند این محدودیت‌ها را شناسایی کرده و راه‌حل مناسب را انتخاب کند. یعنی به‌جای اینکه کار متوقف شود، یاد بگیرد چگونه در چارچوب محدودیت‌ها کار کند.

محدودیت‌های محلی (Local Constraints)

در محیط مکتب یا کالج، دانش آموز ممکن است با محدودیت‌های زیر روبه‌رو شود:

- قوانین استفاده از سیستم
- محدود بودن نرم‌افزارها
- محدودیت اینترنت (در افغانستان این مورد بیشتر تجربه کردیم)

این‌ها روی انتخاب ابزار و روش کار تأثیر می‌گذارد.

محدودیت‌های عمومی (Wider Constraints)

محدودیت‌ها فقط محلی نیست، بلکه می‌تواند شامل:

- قوانین عمومی
- دسترسی به تکنالوژی
- هزینه نرم‌افزارها باشد

نمونه محدودیت‌ها

دانش آموز باید این موارد را درک کند:

- قوانین استفاده قابل قبول(**AUP**)
- نبود بعضی نرم‌افزارها
- محدود بودن سایت‌ها در اینترنت

کار در چارچوب محدودیت

دانش آموز باید یاد بگیرد:

- از ابزارهای موجود استفاده کند
- راه‌حل‌های بدیل **(Alternative)** پیدا کند
- قوانین مکتب را رعایت کند

این مهارت در دنیای واقعی بسیار مهم است.

استفاده از سیستم‌های آنلاین

در بسیاری موارد:

- بهتر است از سیستم‌هایی استفاده شود که مکتب اجازه داده
- مثل سیستم‌های **Cloud** تأیید شده
- یا سیستم داخلی مکتب

این کار امنیت و دسترسی را بهتر می‌کند.

نکات کلیدی

- شناخت محدودیت‌ها قبل از شروع کار
- رعایت قوانین مکتب **(AUP)**
- انتخاب ابزارهای در دسترس
- استفاده از راه‌حل‌های بدیل

مثال واقعی

یک دانش آموز می‌خواهد از یک نرم‌افزار خاص استفاده کند:

مشکل:

- نرم‌افزار در مکتب نصب نیست
- سایت آن بلاک است

راه‌حل:

- استفاده از نرم‌افزار مشابه
- استفاده از نسخه آنلاین مجاز

نتیجه: کار ادامه پیدا می‌کند

انواع محدودیت‌ها

نوع محدودیت	مثال	تأثیر
قانونی	AUP	محدود کردن استفاده
تکنیکی	نبود نرم‌افزار	تغییر ابزار
اینترنت	سایت‌های بسته	محدودیت دسترسی
مالی	هزینه نرم‌افزار	انتخاب رایگان

جدول راه‌حل‌ها

مشکل	راه‌حل
نبود نرم‌افزار	استفاده از بدیل
اینترنت محدود	استفاده آفلاین
قوانین مکتب	رعایتAUP
دسترسی کم	استفاده از سیستم تأیید شده

تهیه پلان کاری برای ساخت پروفایل دیجیتلی

در این بخش، دانش آموز باید بتواند یک **پلان کاری (Working Plan)** واضح و منظم برای ساخت پروفایل دیجیتلی خود تهیه کند. این پلان کمک می‌کند که کار به‌صورت مرحله‌به‌مرحله پیش برود، زمان ضایع نشود و پروژه به موقع تکمیل گردد. علاوه بر این، دانش آموز باید معیارهایی تعیین کند تا بتواند در پایان بررسی کند که آیا کارش موفق بوده یا نه. استفاده از روش **SMART**کمک می‌کند که اهداف دقیق، قابل اندازه‌گیری و واقعی باشند.

- **اهمیت پلان‌سازی**

تمام کارهای روزانه‌ای که موفقیت آمیز میباشد با پلان منظم از قبل برنامه ریزی شده است. مانند برگذاری صنف‌های یک کورس، مکتب و یا هم دانشگاه که اسایتد و مدیریت میداند در کدام ساعت چی مضمون تدریس میشود. دقیقا برای پیشبرد امورات شخصی در زندگی پلان های نقش اساسی دارند. که اگر بدون پلان به کارهای اقدام کنیم بی نظم و موفقیت آمیز به سرانجام نخواهد سید. لذا باید قبل از قبل پلان و برنامه ریزی داشته باشیم.

بدون پلان:

- کار بی‌نظم می‌شود

- زمان از دست می‌رود
- نتیجه ضعیف می‌شود

پلان = راهنمای انجام پروژه

🔹 **اجزای اصلی پلان**

دانش آموز باید در پلان خود شامل کند:

- زمان‌بندی **(Timescales)**
- معیار موفقیت **(Success Criteria)**
-
- اهداف **SMART**

🔹 **زمان‌بندی (Timescale)**

دانش آموز باید مشخص کند:

- هر بخش پروژه چه وقت شروع و ختم می‌شود
- چه مقدار زمان نیاز است

مثال:

طراحی → 2 روز

ساخت → 3 روز

🔹 **معیار موفقیت(Success Criteria)**

دانش آموز باید بداند:

- یک کار خوب چه ویژگی دارد؟
- چگونه می‌فهمد کارش موفق است؟

مثال:

- پروفایل کامل باشد
- طراحی واضح باشد
- بدون اشتباه باشد

🔹 **اهداف SMART**

اهداف باید:

نماد رسیدن به اهداف واقعی

- مشخص **(Specific)**
- قابل اندازه‌گیری **(Measurable)**
- قابل دستیابی **(Achievable)**
- مرتبط **(Relevant)**
- زمان‌دار **(Time-bound)**

این روش باعث دقیق بودن پلان می‌شود

🔹 **نکات کلیدی**

- پلان باید واضح باشد
- زمان‌بندی دقیق باشد
- هدف‌ها قابل اندازه‌گیری باشد
- پیشرفت کار باید قابل بررسی باشد

🔹 **مثال واقعی**

یک دانش آموز پلان می‌سازد:

❌ اشتباه:

- فقط می‌گوید "پروفایل می‌سازم "
- زمان مشخص ندارد

✅ درست:

- روز 1: تحقیق
- روز 2: طراحی
- روز 3: ساخت

نتیجه: کار منظم و موفق

همیشه در زمان پلان ریزی برنامه ساعت کنار دست خود داشته باشید!

جدول نمونه پلان

توضیح	زمان	بخش کار
جمع‌آوری معلومات	روز 1	**تحقیق**
انتخاب رنگ و ساختار	روز 2	**طراحی**
ایجاد پروفایل	روز 3	**ساخت**
اصلاح اشتباهات	روز 1	**بررسی**

جدول SMART

مثال	بخش
ساخت پروفایل دیجیتلی	**Specific**

شامل 5 بخش	**Measurable**
با ابزار موجود	**Achievable**
مرتبط به درس	**Relevant**
روز 7	**Time-bound**

باید به یاد داشته باشید پروژه ها در رشته های مختلف با نحوه ارائه و پچیده‌گی مفاهیم آن فرق میکند لذا اینجا بعنوان از طراحی، برنامه ریزی دقیق یک ساختار ارائه دادیم مورد دیگر را باید بررسی کنید که چطور میتوانیم از ساختارهای مختلف برای برنامه ریزی استفاده کنیم.

مشخص‌سازی برنامه‌ها و نوع فایل‌ها در پلان پروفایل دیجیتلی

در این بخش، دانش آموز باید در پلان خود به‌صورت واضح مشخص کند که برای ساخت پروفایل دیجیتلی از **کدام برنامه‌ها (Applications)** و **کدام نوع فایل‌ها (File Types)** استفاده خواهد کرد. این کار بسیار مهم است، زیرا انتخاب نادرست ابزار یا فایل می‌تواند باعث شود که پروژه به‌درستی کار نکند، کیفیت پایین بیاید یا برای دیگران قابل استفاده نباشد. همچنان دانش آموز باید مشکلات احتمالی را از قبل پیش‌بینی کند تا در جریان کار دچار مشکل نشود.

اهمیت انتخاب برنامه‌ها (Applications)

هر بخش پروژه نیاز به ابزار مناسب دارد. اگر ابزار درست انتخاب نشود:

- کار سخت می‌شود
- کیفیت پایین می‌آید
- وقت ضایع می‌شود

مثال:

- نوشتن **CV** → **Word**
- ارائه → **PowerPoint**
- طراحی **Canva** → یا **Photoshop**

اهمیت نوع فایل‌ها (File Types)

نوع فایل تعیین می‌کند:

- آیا دیگران می‌توانند آن را باز کنند؟
- آیا قابل ویرایش است یا نه؟
- حجم آن چقدر است؟

مثال:

- **PDF** → برای اشتراک‌گذاری
- **DOCX** → برای ویرایش
- **JPG** → برای تصویر

🔹 **بخش‌های که باید در پلان ذکر شود**

دانش آموز باید در پلان خود شامل کند:

1. برنامه‌های مورد استفاده

برای هر بخش پروژه مشخص کند:

- از کدام نرم‌افزار استفاده می‌کند
- چرا آن را انتخاب کرده

2. نوع فایل‌ها

برای هر بخش مشخص کند:

- چه نوع فایل استفاده می‌شود
- چرا آن مناسب است

3. مشکلات احتمالی(Potential Issues)

دانش آموز باید پیش‌بینی کند:

- چه مشکلاتی ممکن است پیش بیاید
- چگونه آن را حل کند

مشکلات احتمالی

برخی مشکلات ممکن:

- حجم زیاد فایل
- باز نشدن فایل در سیستم دیگر
- نبود نرم‌افزار
- کندی سیستم

باید از قبل فکر شود و راه های بدیل قبل از برنامه ریزی شود.

🔹 **نکات کلیدی**

- انتخاب برنامه مناسب برای هر کار
- انتخاب فایل مناسب برای اشتراک
- توجه به حجم و سازگاری فایل
- پیش‌بینی مشکلات

🔹 **مثال واقعی**

یک دانش آموز پروفایل می‌سازد:

❌ **اشتباه**:

- استفاده از فایل‌های سنگین و ناشناخته
- عدم در نظر گرفتن باز شدن فایل

نتیجه: کارفرما نمی‌تواند فایل را باز کند

✅ **درست**:

- استفاده از **PDF** برای **CV**
- استفاده از **JPG** برای تصاویر

نتیجه: پروفایل قابل استفاده

جدول برنامه‌ها و کاربرد

بخش پروژه	برنامه	دلیل انتخاب
CV	Word	ساده و قابل ویرایش
ارائه	PowerPoint	نمایش خوب
طراحی	Canva	آسان و سریع
دیتا	Excel	مدیریت معلومات

جدول نوع فایل‌ها

بخش	نوع فایل	دلیل
سند	PDF	قابل باز شدن
متن	DOCX	قابل ویرایش
تصویر	JPG / PNG	کیفیت مناسب
ویدیو	MP4	سازگار با اکثر سیستم‌ها

جدول مشکلات و راه‌حل

مشکل	علت	راه‌حل
حجم زیاد	فایل ویدیو	کاهش حجم
باز نشدن فایل	فرمت نامناسب	PDF تبدیل به
نبود نرم‌افزار	محدودیت سیستم	استفاده از آنلاین
کندی سیستم	فایل سنگین	ساده‌سازی

استفاده از پلان برای مدیریت امنیت پروفایل دیجیتلی

در این بخش، دانش آموز باید نشان دهد که چگونه از **پلان خود** برای محافظت از پروفایل دیجیتلی استفاده می‌کند. یعنی فقط ساختن پروفایل مهم نیست، بلکه باید **امنیت (Security)** آن نیز از ابتدا در پلان در نظر گرفته شود. دانش آموز باید فکر کند که چگونه از معلومات خود محافظت کند، چگونه از تغییر یا دسترسی غیرمجاز جلوگیری کند و در عین حال امکان **کار گروهی (Collaboration)** را نیز حفظ نماید. این کار نیاز به برنامه‌ریزی دقیق دارد تا بین **امنیت و انعطاف‌پذیری (Flexibility)** تعادل برقرار شود.

- **حفظ یکپارچگی (Integrity)**

دانش آموز باید درک کند که:

- معلومات پروفایل نباید بدون اجازه تغییر کند
- فایل‌ها باید سالم باقی بمانند
- نسخه درست همیشه حفظ شود

این را **«Integrity»** می‌گویند.

🔹 **نقش پلان در امنیت**

پلان باید مشخص کند:

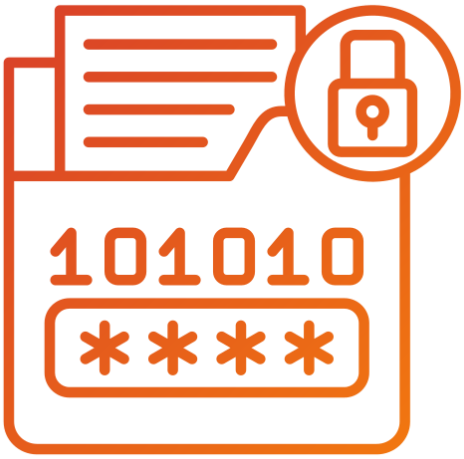
- چه کسی به کدام بخش دسترسی دارد
- چگونه فایل‌ها محافظت می‌شوند
- چه ابزارهای امنیتی استفاده می‌شود

امنیت باید از اول در پلان باشد، نه بعداً که تمام دیتا آسیب دید بعد پلان امنتی را تطبیق کنید.

🔹 **ابزارها و روش‌های محافظت**

دانش آموز باید از ابزارهای زیر استفاده کند:

- **Password** قوی
- **Permissions** سطح دسترسی
- **Encryption** در صورت نیاز
- **Backup** گرفتن



سیستم های جدید همه از میتو رمزنگاری شده برای محافظ از دیتا در مقابل حملات و هکرها استفاده میکند.

🔹 **تعادل بین امنیت و کار گروهی**

اگر امنیت خیلی زیاد باشد:

- کار گروهی سخت می‌شود

اگر امنیت کم باشد:

- خطر زیاد می‌شود

پس باید تعادل برقرار شود.

🔹 **نکات کلیدی**

- امنیت باید در پلان ذکر شود
- دسترسی‌ها باید کنترول شود
- از ابزارهای محافظتی استفاده شود
- تعادل بین امنیت و همکاری رعایت شود.

🔹 **مثال واقعی**

یک دانش آموز پروژه گروهی دارد:

❌ اشتباه:

- همه اعضا **Full Access** دارند
- هر کس می‌تواند فایل را حذف کند

نتیجه: خطر تخریب

✅ درست:

- بعضی اعضا **Read Only**
- فقط مدیر **Edit** دارد

نتیجه: امنیت + همکاری

جدول ابزارهای امنیتی

ابزار	کاربرد	هدف
Password	محافظت حساب	جلوگیری از ورود
Permissions	تعیین دسترسی	کنترول کاربران
Backup	ذخیره نسخه	جلوگیری از از دست رفتن
Encryption	رمزگذاری	امنیت بیشتر

رعایت محدودیت‌ها در پلان پروفایل دیجیتلی

در این بخش، دانش آموز باید نشان دهد که در پلان خود فقط کار و طراحی را در نظر نگرفته، بلکه **تمام محدودیت‌ها (Constraints)** را نیز در نظر گرفته است. این محدودیت‌ها می‌تواند از طرف مکتب، سیستم، زمان یا حتی توانایی خود دانش آموز باشد. هدف این است که دانش آموز یک پلان واقع‌بینانه بسازد که بتواند **مشکلات احتمالی را پیش‌بینی کرده و برای آن راه‌حل داشته باشد** .یعنی قبل از شروع کار بداند چه موانعی وجود دارد و چگونه آن‌ها را مدیریت کند.

🔹 **درک اهمیت محدودیت‌ها**

اگر محدودیت‌ها در نظر گرفته نشود:

- پروژه ناقص می‌ماند
- زمان از دست می‌رود
- مشکلات حل نشده باقی می‌ماند

پس پلان باید واقع‌بینانه باشد

🔹 **محدودیت‌های مهم**

دانش آموز باید این موارد را در پلان خود شامل کند:

1. **قوانین استفاده AUP**
   - قوانین مکتب در استفاده از سیستم
   - محدود بودن بعضی فعالیت‌ها
2. **محدودیت اینترنت**
   - بعضی سایت‌ها بسته است

- دانلود محدود است

3. دسترسی به نرم‌افزار

- ممکن است همه برنامه‌ها موجود نباشد
- باید از ابزارهای در دسترس استفاده شود

4. زمان(Time)

- پروژه باید در وقت مشخص تکمیل شود
- مدیریت زمان بسیار مهم است

5. مهارت کاربر(User Skills)

- سطح مهارت دانش آموز مهم است
- ابزار باید مطابق توانایی انتخاب شود

🔹 **پلان مؤثر (Effective Plan)**

یک پلان خوب باید:

- مشکلات را پیش‌بینی کند
- برای هر مشکل راه‌حل داشته باشد
- قابل اجرا باشد

این یعنی پلان حرفه‌ای

🔹 **نکات کلیدی**

- در نظر گرفتن تمام محدودیت‌ها
- انتخاب ابزار مطابق شرایط
- مدیریت زمان
- توجه به توانایی خود

🔹 **مثال واقعی**

یک دانش آموز می‌خواهد پروژه بسازد:

❌ اشتباه:

- انتخاب نرم‌افزار پیچیده
- در نظر نگرفتن زمان

نتیجه: پروژه نیمه‌کاره

✅ درست:

- انتخاب ابزار ساده
- تقسیم کار در زمان

نتیجه: پروژه کامل

یک پروفایل دیجیتالی امن و قابل استفاده بساز تا مهارت‌ها و درک من را به شکل ایمن و حرفه‌ای معرفی و تبلیغ کند

ساخت یک سیستم کاری برای مدیریت مهارت‌ها و معلومات دیجیتلی

در این بخش، دانش آموز باید بتواند یک **سیستم دیجیتلی (Digital System)** ایجاد کند که در آن مهارت‌ها و معلومات خود را به‌صورت منظم، واضح و حرفه‌ای نمایش دهد. این سیستم معمولاً به شکل یک **ePortfolio (پروفایل دیجیتلی)** ساخته می‌شود که هدف آن معرفی توانایی‌های دانش آموز برای **کار، کالج یا اپرنتسشیپ (Apprenticeship)** است. این پروفایل باید نشان دهد که دانش آموز در استفاده از تکنالوژی مهارت دارد و می‌تواند کارهای دیجیتلی را به‌صورت عملی انجام دهد.

ePortfolio چیست؟

ePortfolio یک مجموعه از فایل‌های دیجیتلی است که شامل:

- مهارت‌ها
- پروژه‌ها
- نمونه کارها

می‌باشد

هدف: معرفی خود به کارفرما یا مکتب

هدف ساخت سیستم

دانش آموز باید بتواند:

- خود را به‌صورت حرفه‌ای معرفی کند
- مهارت‌های دیجیتلی خود را نشان دهد
- برای فرصت‌های کاری آماده شود

برعلاوه در فصلهای قبلی شما معلومات نسبی کسب کردید.

محتویات ePortfolio

پروفایل دیجیتلی می‌تواند شامل باشد:

- **CV** رزومه
- پروژه‌ها
- تصاویر یا ویدیو
- اسناد **(Documents)**
- ارائه‌ها **(Presentations)**

بستگی به علاقه یا هدف دانش آموز دارد

ویژگی‌های یک سیستم خوب

یک **ePortfolio** خوب باید:

- منظم و واضح باشد
- حرفه‌ای به نظر برسد
- آسان قابل استفاده باشد

یعنی**"Semi-professional"**

استفاده برای کار و تحصیل

این پروفایل می‌تواند برای:

- درخواست کار
- اپرنتسشیپ
- ثبت‌نام در کالج استفاده شود.

دریافت بازخورد(Feedback)

پروفایل باید:

- تست شود
- نظر دیگران گرفته شود.

مثل:

- کارفرما
- استاد
- کالج

نکات کلیدی

- ساخت یک سیستم منظم
- نمایش مهارت‌ها
- استفاده از فایل‌های مناسب
- طراحی نیمه‌حرفه‌ای
- گرفتن بازخورد

🔹 **مثال واقعی**

یک دانش آموز **ePortfolio** می‌سازد:

❌ اشتباه:

- فایل‌ها پراکنده
- طراحی نامنظم

نتیجه: تأثیر ضعیف

✅ درست:

- دسته‌بندی فایل‌ها
- طراحی ساده و واضح

نتیجه: تأثیر مثبت

جدول محتویات ePortfolio

هدف	توضیح	بخش
معرفی	معلومات شخصی و مهارت‌ها	**CV**
نشان دادن توانایی	کارهای انجام شده	**پروژه**
جذابیت	نمونه کار	**تصویر/ویدیو**
اعتبار	گزارش‌ها	**اسناد**

استفاده از برنامه‌ها و نوع فایل مناسب برای ارائه پروفایل آنلاین

در این بخش، دانش آموز باید نشان دهد که می‌تواند از برنامه‌های دیجیتلی **(Applications)** و نوع فایل‌ها **(File Types)** به‌صورت درست و مناسب استفاده کند تا پروفایل آنلاین خود را به بهترین شکل ارائه دهد. انتخاب درست ابزار و فایل بسیار مهم است، زیرا هر نوع محتوا (متن، تصویر، ویدیو) نیاز به فرمت و نرم‌افزار خاص خود دارد. اگر این انتخاب درست باشد، پروفایل واضح، حرفه‌ای و قابل استفاده برای دیگران خواهد بود.

اهمیت انتخاب برنامه مناسب

هر نوع محتوا ابزار خاص خود را دارد:

- متن → **Word**
- ارائه → **PowerPoint**
- طراحی → **Canva** درصورتیکه انترنت داشته باشید اما در غیر آنصورت فتوشاپ
- دیتا → **Excel**

انتخاب درست = کیفیت بهتر.

اهمیت انتخاب نوع فایل

نوع فایل تعیین می‌کند:

- آیا باز می‌شود یا نه
- قابل ویرایش است یا نه
- حجم آن چقدر است

مثال:

- **PDF** → برای نمایش
- **DOCX** → برای ویرایش
- **MP4** → برای ویدیو

🔹 **ارتباط با رشته و مهارت دانش آموز**

بسته به رشته دانش آموز:

- دانش آموز **IT** → اسناد و پروژه‌های ساده
- دانش آموز هنر → ویدیو و طراحی پیشرفته

نوع فایل‌ها متفاوت می‌شود.

🔹 **نمایش مهارت‌ها از طریق فایل‌ها**

فایل‌هایی که دانش آموز استفاده می‌کند:

- سطح مهارت او را نشان می‌دهد
- توانایی واقعی او را ثابت می‌کند

پروفایل فقط متن نیست، بلکه "نمایش مهارت" است.

گرفتن بازخورد(Feedback)

پروفایل باید:

- توسط دیگران دیده شود
- نظر داده شود

مثل:

- کارفرما
- استاد
- مشاور تحصیلی

نکات کلیدی

- استفاده از برنامه مناسب
- انتخاب فایل قابل استفاده
- توجه به رشته و هدف
- نمایش مهارت‌ها
- گرفتن بازخورد

مثال واقعی

یک دانش آموز هنر:

❌ **اشتباه**:

- فقط فایل **Word** استفاده می‌کند

مهارت واقعی دیده نمی‌شود

✅ **درست**:

- استفاده از **JPG** برای طراحی
- استفاده از **MP4** برای ویدیو

مهارت واضح نمایش داده می‌شود.

محافظت از سیستم در برابر حملات رایج

در این بخش، دانش آموز باید بتواند با استفاده از دانش و مهارت‌های خود، یک سیستم امن دیجیتلی ایجاد کند که در برابر تهدیدهای رایج محافظت شود. این کار تنها با نصب یک نرم‌افزار خلاصه نمی‌شود؛ بلکه ترکیبی از تنظیمات درست، ابزارهای امنیتی، و رفتار صحیح کاربر است. دانش آموز باید بداند چه نوع حملاتی (مثل ویروس، فیشینگ، هک) ممکن است رخ دهد و برای هرکدام چه راه‌حل مناسب وجود دارد. همچنان باید بتواند توضیح دهد که چرا یک ابزار خاص (مثلاً فایروال یا آنتی‌ویروس) را انتخاب کرده و چه مزایایی دارد.

مهم‌ترین تهدیدها

سیستم‌های دیجیتلی معمولاً با تهدیدهای زیر روبه‌رو هستند:

- ویروس‌ها و بدافزارها
- فیشینگ (ایمیل‌های جعلی)
- هک و دسترسی غیرمجاز
- سرقت معلومات شخصی
- استفاده از **Wi-Fi** ناامن

اگر سیستم محافظت نشود، ممکن است اطلاعات از بین برود یا سوءاستفاده شود.

ابزارها و روش‌های محافظت

برای محافظت از سیستم، دانش آموز باید از ترکیب این موارد استفاده کند:

- آنتی‌ویروس
- فایروال
- رمز عبور قوی
- رمزگذاری **(Encryption)**
- بروزرسانی سیستم

هیچ ابزار به‌تنهایی کافی نیست؛ امنیت یعنی ترکیب چند روش.

بزارهای امنیتی

ابزار	وظیفه	مزیت
Antivirus	حذف ویروس	جلوگیری از آلودگی
Firewall	کنترل ترافیک	جلوگیری از هک
Encryption	رمزگذاری داده	حفظ محرمانگی
Password	امنیت حساب	جلوگیری از دسترسی

Update	بروزرسانی	رفع آسیب‌پذیری

تهدید و راه‌حل

تهدید	توضیح	روش جلوگیری
Phishing	ایمیل جعلی	کلیک نکردن لینک
Malware	برنامه مخرب	استفاده از آنتی‌ویروس
Hacking	نفوذ غیرمجاز	فایروال + رمز قوی
Data Theft	سرقت دیتا	رمزگذاری
Unsafe Wi-Fi	اینترنت ناامن	استفاده از VPN

سیستم من مطابق قوانین و محدودیت‌های قانونی و محلی است

در این بخش، دانش آموز باید نشان دهد که **پروفایل دیجیتلی و سیستم آنلاین** او مطابق قوانین، مقررات و محدودیت‌های محلی و عمومی ساخته شده است. یعنی هنگام ساخت **ePortfolio** یا پروفایل آنلاین، فقط ظاهر و محتوا مهم نیست؛ بلکه رعایت قانون نیز ضروری است. هر نوع استفاده نادرست از محتوا، اطلاعات شخصی یا سیستم‌های آنلاین می‌تواند مشکلات قانونی یا اخلاقی ایجاد کند.

دانش آموز باید ثابت کند که محتوای استفاده‌شده قانونی است، از قوانین مکتب یا اداره پیروی می‌کند و حقوق دیگران را نقض نمی‌کند.

قوانین و محدودیت‌های مهم

AUP (Acceptable Use Policy)

AUP یعنی قوانین استفاده قابل قبول از سیستم ها و محتوایی دیگران:

این قوانین مشخص می‌کند کاربر در شبکه مکتب، اداره یا سازمان:

- چه کار می‌تواند انجام دهد
- چه کار ممنوع است

مثال:

- دانلود غیرمجاز ممنوع
- ورود به سایت‌های نامناسب ممنوع
- اشتراک رمز عبور ممنوع

هدف: استفاده مسئولانه از سیستم

Copyright حق نشر

Copyright یعنی مالکیت قانونی محتوا.

اگر کسی:

- عکس
- ویدیو
- مقاله
- موسیقی
- کتاب
- نقاشی
- طرح یا ایده

ساخته باشد، دیگران بدون اجازه حق استفاده آزاد ندارند. در صورت موافقت یعنی اجازه صاحب اثر میتواند از آن استفاده نماید.

مثال:

❌ اشتباه:

کپی تصویر از اینترنت بدون ذکر منبع

✅ درست:

ذکر منبع یا استفاده از محتوای مجاز اما باید یاد داشت باشید بعضی وقت ها با ذکر منبع هم کپی رایت گفته میشود بدلیل منافع مالی و منحصر بفرد بودن محصول یا اثر.

Plagiarism سرقت علمی/کپی‌برداری

Plagiaris یعنی استفاده از کار دیگران و معرفی آن به‌نام خود.

مثال:

❌ کپی متن مقاله و ثبت به نام خود

✅ نوشتن منبع یا بازنویسی درست.

Data Protection محافظت از داده

Data Protection یعنی حفاظت از اطلاعات شخصی.

باید از این موارد محافظت شود:

- نام
- ایمیل
- شماره تماس
- اسناد شخصی

مثال:

❌ نشر شماره تماس عمومی

✅ محدود کردن دسترسی

ساخت یک برنامه برای بررسی امنیت و درست کار کردن پروفایل

آزمایش سیستم بر اساس معیارهای موفقیت

در این بخش، دانش آموز باید سیستم یا پروفایل دیجیتلی (**ePortfolio**) خود را بررسی کند تا ببیند آیا مطابق اهدافی که در مرحله پلان تعیین کرده بود، کار می‌کند یا نه. یعنی هر چیزی که قبلاً به‌عنوان معیار موفقیت (**Success Criteria**) مشخص شده، حالا باید تست شود. اگر نتیجه مطابق هدف نبود، باید اصلاح شود.

معیارهای مهم برای تست

دانش آموز باید پروفایل خود را بر اساس این معیارها آزمایش کند:

- ظاهر نیمه‌حرفه‌ای داشته باشد
- منظم و قابل فهم باشد
- آسان قابل استفاده **(Navigation)** باشد
- فقط معلومات مناسب برای مخاطب نمایش دهد
- برای افراد دارای معلولیت قابل استفاده باشد
- در سیستم‌ها و مرورگرهای مختلف درست کار کند

جدول معیارهای موفقیت

معیار	توضیح
ظاهر حرفه‌ای	طراحی مناسب و تمیز
نظم	دسته‌بندی واضح
استفاده آسان	حرکت ساده بین بخش‌ها
کنترل محتوا	نمایش هدفمند معلومات
دسترسی	قابل استفاده برای همه
سازگاری	کار در همه دستگاه‌ها

مثال واقعی

یک دانش آموز پروفایل خود را تست می‌کند:

مشکل:
- در موبایل درست نمایش نمی‌شود
- متن‌ها به‌هم ریخته است

اصلاح:
- طراحی را Responsive می‌کند

نتیجه: در همه دستگاه‌ها درست کار می‌کند

نکات مهم
- تست باید بر اساس هدف باشد
- مشکلات باید اصلاح شود
- سیستم باید برای همه قابل استفاده باشد

پاسخ به بازخورد و اصلاح پروفایل دیجیتلی

در این بخش، دانش آموز باید نشان دهد که می‌تواند **بازخورد (Feedback)** دیگران را به‌صورت حرفه‌ای قبول کند و بر اساس آن سیستم یا پروفایل دیجیتلی خود را بهتر بسازد. در پروژه‌های واقعی، هیچ سیستم از بار اول کامل نیست؛ به همین دلیل نظر دیگران بسیار مهم است. بازخورد کمک می‌کند اشتباهات، ضعف‌ها و مشکلاتی که شاید خود دانش آموز متوجه نشده باشد، شناسایی و اصلاح شود.
دانش آموز باید نشان دهد که:
- به نظر دیگران احترام می‌گذارد
- انتقاد را با برخورد خوب قبول می‌کند
- تغییرات لازم را عملی می‌سازد

این یک مهارت مهم حرفه‌ای و کاری است.

Feedback چیست؟
فیدبک یعنی نظرخواهی دیگران در مورد نتیجه کار شما میباشد. حالا میتواند فیدبک بسیار بد و مأثیر کننده باشد اما شما باید جنبه های مثبت آنرا گل چین کنید. در مقابل نظرات بد پرخاشگری نکنید بلکه بسیار با خونسرد از آنها تشکری کنید. اما هدف خود را دنبال کرده و کیفیت اثر خود را ارتقاء دهید. چون اگر شما پرخاشگری کنید این ضعف شما را نشان میدهد.
Feedback یعنی:
- نظر
- پیشنهاد
- ارزیابی دیگران

درباره سیستم یا پروفایل.
این بازخورد می‌تواند از:

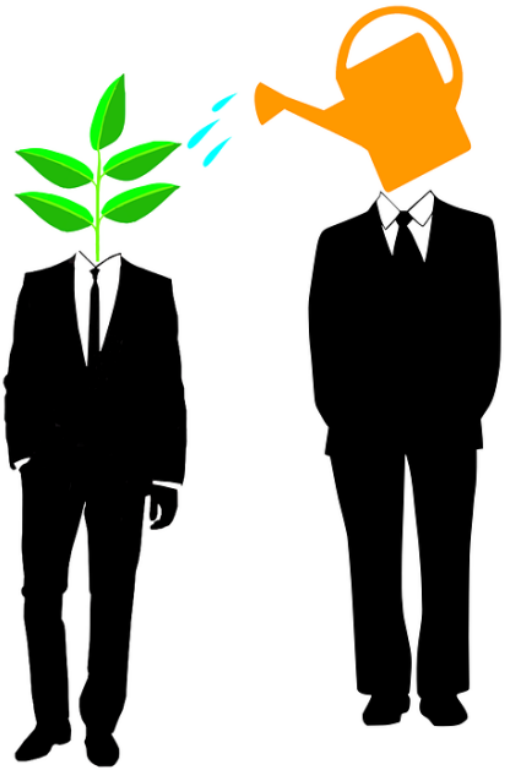
- استاد
- هم‌صنفی
- کارفرما
- دوستان دریافت شود.

اهمیت بازخورد (Feedback)

گاهی دانش آموز فکر می‌کند سیستمش کامل است، اما دیگران ممکن است مشکلاتی ببینند مثل:

- طراحی ضعیف
- رنگ نامناسب
- نوشته‌های نامنظم
- لینک خراب

بازخورد باعث بهتر شدن کیفیت کار می‌شود.



تأثیر فیدبک بر ذهنیت طرح اثر

🔹 **برخورد حرفه‌ای با بازخورد**

دانش آموز باید:

✅ مؤدب باشد
✅ انتقاد را شخصی نگیرد
✅ پیشنهاد مفید را قبول کند
✅ تغییرات لازم را انجام دهد

نباید:

- عصبی شود
- مخالفت غیرمنطقی کند
- همه نظرها را رد کند

اصلاح سیستم بر اساس بازخورد

بعد از دریافت **Feedback** :

1️⃣ مشکل شناسایی می‌شود
2️⃣ راه‌حل پیدا می‌شود
3️⃣ سیستم اصلاح می‌شود
4️⃣ دوباره تست می‌شود

این روند باعث پیشرفت سیستم می‌شود.

خلاصه فیدبک یا بازخورد در مورد طرح و پروفایل شما

نوع بازخورد	مثال	نتیجه
طراحی	رنگ مناسب نیست	تغییر رنگ
محتوا	متن زیاد است	خلاصه‌سازی
ساختار	پیدا کردن بخش‌ها سخت است	تنظیم منو
امنیت	اطلاعات زیاد نمایش داده شده	محدود کردن دسترسی

خلاصه فیدبک های نادرست

برخورد درست	برخورد نادرست
گوش دادن	بحث کردن
تشکر کردن	ناراحت شدن
اصلاح سیستم	نادیده گرفتن
قبول نظر منطقی	رد همه نظرها

آزمایش سیستم در برابر حملات رایج

در این بخش، دانش آموز باید سیستم یا **ePortfolio** خود را در برابر حملات معمول امنیتی آزمایش کند تا مطمئن شود معلومات و فایل‌هایش محفوظ است. هدف این است که سیستم فقط زیبا و منظم نباشد، بلکه از نگاه امنیتی نیز قوی باشد. دانش آموز باید از روش‌ها و پروتوکول‌هایی که قبلاً در بخش 3.4 ساخته بود استفاده کند تا نقاط ضعف سیستم را پیدا کرده و امنیت آن را بهتر سازد.

چرا تست امنیت مهم است؟

اگر سیستم تست نشود:

- رمز عبور ممکن است ضعیف باشد
- دیگران شاید به فایل‌ها دسترسی پیدا کنند
- حساب ممکن است هک شود

بنابراین تست امنیتی کمک می‌کند قبل از وقوع مشکل، ضعف‌ها شناسایی شود.

بخش‌های مهم تست امنیت

1. Password Strength قدرت رمز عبور

همانطوریکه در سطح قبلی شما در مورد نحوه‌ای انتخاب رمزعبور برای حساب های آنلاین و افلاین خود آموختید یک یادآوری دباره لازم است. چرا که اولین محافظ از دیتاها شما و امنیت سیستم به همین

قوت و یا قویی بودن پسود شما میباشد. یک پسورد قویی؛ پسورد از که ساختار از: اعداد، سمبولها، کارکترهای خاص مانند %,$,#,@ و غیره همچنان حروفی خرد و بزرگ انگلیسی ترکیب شده باشد و طول آن احداقل 8 تا 12 کارکتر باشد.

رمز عبور باید:

- طولانی باشد
- ترکیبی از حروف، اعداد و نشانه‌ها داشته باشد
- حدس زدن آن سخت باشد

مثال:

ضعیف:

123456

قوی:

R3zv@n2026!

2. Read Only Versions

بعضی فایل‌ها باید فقط قابل دیدن باشند، نه ویرایش.

یعنی:

- دیگران بتوانند فایل را بخوانند
- اما نتوانند تغییر دهند

مزیت:

- جلوگیری از خراب شدن فایل‌ها
- محافظت از محتوا

3. **Brute Force Attack**

در این حمله، هکر بارها رمزهای مختلف را امتحان می‌کند تا رمز درست پیدا شود.

جلوگیری:

- رمز قوی
- محدود کردن تعداد تلاش
- قفل شدن حساب بعد از چند اشتباه

استفاده از reCAPTCHA

reCAPTCHA سیستمی است که تشخیص می‌دهد کاربر انسان است یا ربات. چون بعضی افراد مخرب ربات های را طراحی میکند که وب هایت و سیستم ها را هر دوم لاگین کند و سیستم همان سازمان کند شود و در پی این کار اهداف مختلف دارد. که در اینجا لازم نیست در این رابطه بحث کنیم.

مثال:

“I’m not a robot”

مزیت:

- جلوگیری از حملات خودکار
- افزایش امنیت ورود

آیکن کپچه شرکت گوگل

جدول حملات و محافظت

نوع تهدید	توضیح	روش محافظت
رمز ضعیف	حدس آسان رمز	رمز قوی
ویرایش فایل	تغییر محتوا	Read Only
Brute Force	امتحان مکرر رمز	محدودیت تلاش
Bot Attack	حمله ربات	reCAPTCHA

مثال واقعی

یک دانش آموز برای پروفایل خود:

❌ رمز ساده انتخاب می‌کند

❌ فایل‌ها را **Editable** می‌گذارد

نتیجه:

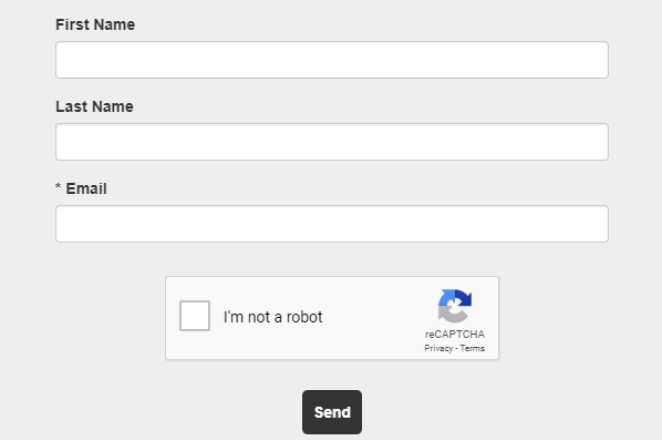
- حساب هک می‌شود
- فایل‌ها تغییر می‌کند

روش درست:

- استفاده از رمز قوی
- فعال کردن **Read Only**
- استفاده از **reCAPTCHA**

نتیجه:

سیستم امن‌تر می‌شود.



لایه امنیتی کپچه در فورم واقعی

استفاده از روش‌های دیجیتلی و غیردیجیتلی برای جمع‌آوری فیدبک

در این بخش، دانش آموز باید بتواند از روش‌های مختلف برای جمع‌آوری بازخورد (**Feedback**) درباره پروفایل دیجیتلی خود استفاده کند. هدف این است که بداند دیگران درباره طراحی، امنیت، محتوا و مؤثریت سیستم او چه نظری دارند. هرچه بازخورد بیشتر و دقیق‌تر باشد، دانش آموز بهتر می‌تواند نقاط ضعف و قوت سیستم خود را تشخیص دهد و آن را بهبود ببخشد.

اهمیت جمع‌آوری بازخورد

گاهی سازنده سیستم مشکلات کار خود را متوجه نمی‌شود، اما کاربران یا بینندگان ممکن است:

- اشتباهات را ببینند
- مشکلات امنیتی را تشخیص دهند
- پیشنهادهای بهتر ارائه کنند

به همین دلیل بازخورد بخش مهم ارزیابی سیستم است.

روش‌های جمع‌آوری فیدبک (Feedback)

دانش آموز باید بتواند از روش‌های مختلف استفاده کند، مانند:

- پرسش‌نامه **(Questionnaire)**
- نظر هم‌صنفی‌ها **(Peer Comment)**
- فورم آنلاین
- بلاگ و فورم گفتگو
- ایمیل
- **Survey** آنلاین

Questionnaire پرسش‌نامه

پرسش‌نامه یکی از بهترین روش‌ها برای دریافت نظر کاربران است.

مثال سوال‌ها:

- آیا طراحی واضح است؟
- آیا پیدا کردن بخش‌ها آسان است؟
- آیا پروفایل حرفه‌ای به نظر می‌رسد؟

مزیت:

دریافت نظر منظم و قابل تحلیل

Peer Comment نظر هم‌صنفی

دانش آموزان دیگر می‌توانند:

- مشکلات را پیدا کنند
- پیشنهاد بدهند
- کیفیت کار را ارزیابی کنند

این روش در پروژه‌های آموزشی بسیار مفید است.

روش‌های آنلاین

بعضی سیستم‌های آنلاین امکانات بازخورد دارند:

- **Forum**
- **Blog**
- **Forms**
- **Surveys**

مزیت:

- دریافت نظر سریع
- جمع‌آوری معلومات زیاد

Email Contact

ایمیل نیز می‌تواند برای دریافت بازخورد استفاده شود.

مثال:

- ارسال لینک پروفایل
- درخواست نظر از استاد یا کارفرما

جدول روش‌های فیدبک

روش	توضیح	مزیت
Questionnaire	پرسش‌نامه	منظم و دقیق
Peer Comment	نظر هم‌صنفی	کشف اشتباهات
Survey Online	فورم آنلاین	سرعت بالا
Email	درخواست رسمی نظر	ارتباط حرفه‌ای
Forum/Blog	بحث آنلاین	دریافت نظر گسترده

مثال واقعی

یک دانش آموز لینک **ePortfolio** خود را برای ۱۰ نفر می‌فرستد.

نتیجه بازخورد:

- رنگ متن ضعیف است
- نسخه موبایل مشکل دارد
- تصاویر زیاد بزرگ است

دانش آموز مشکلات را اصلاح می‌کند و سیستم بهتر می‌شود.

نکات مهم

- بازخورد باید از چند منبع جمع شود
- نظرها باید تحلیل شود
- پیشنهادهای مفید باید عملی شود
- برخورد حرفه‌ای مهم است

ارزیابی انتقادی پروفایل دیجیتلی و امنیت آن

در این بخش، دانش آموز باید بتواند به‌صورت انتقادی و دقیق پروفایل دیجیتلی خود را بررسی کند و ببیند آیا به اهداف و معیارهایی که قبلاً تعیین کرده بود رسیده یا نه. این ارزیابی فقط ظاهر سیستم را شامل نمی‌شود، بلکه امنیت، عملکرد، سهولت استفاده و کیفیت کلی سیستم را نیز در بر می‌گیرد.

دانش آموز باید درباره این موارد فکر کند:

- چه بخش‌هایی موفق بوده؟
- چه مشکلاتی وجود داشته؟
- چه چیزهایی نیاز به اصلاح دارد؟
- آیا امنیت سیستم کافی بوده؟

این مرحله کمک می‌کند دانش آموز فقط "استفاده‌کننده" نباشد، بلکه مانند یک تحلیل‌گر حرفه‌ای سیستم خود را بررسی کند.

Reflection چیست؟

Reflection یعنی فکر و تحلیل درباره کار انجام‌شده.

در این بخش، دانش آموز:

- نتیجه تست‌ها را بررسی می‌کند
- موفقیت‌ها و مشکلات را تحلیل می‌کند
- برای نسخه بعدی تصمیم بهتر می‌گیرد

ارزیابی بر اساس Success Criteria

دانش آموز باید سیستم را با معیارهایی که قبلاً تعیین کرده بود مقایسه کند.

مثال:

معیار	نتیجه
ظاهر حرفه‌ای	**موفق**
امنیت رمز عبور	**متوسط**
نسخه موبایل	**نیاز به اصلاح**

این کار نشان می‌دهد پروژه تا چه اندازه موفق بوده است.

بررسی امنیت سیستم

دانش آموز باید ببیند:

- آیا رمزها قوی هستند؟
- آیا دسترسی‌ها درست تنظیم شده؟
- آیا فایل‌ها محفوظ مانده‌اند؟
- آیا احتمال هک یا نشت معلومات وجود دارد؟

مشکلات نرم‌افزاری و Bug

گاهی مشکل سیستم از دانش آموز نیست، بلکه از خود نرم‌افزار است.

مثال:

- **Bug**
- خطای برنامه
- ناسازگاری سیستم

در این حالت دانش آموز باید:

- فورم‌های پشتیبانی را بررسی کند
- راه‌حل‌های کاربران دیگر را بخواند
- وضعیت بروزرسانی نرم‌افزار را بررسی کند

استفاده از Community وForum

در سیستم‌های **Open Source** معمولاً انجمن‌های پشتیبانی وجود دارد.

مثل:

- **Forum**
- **GitHub**
- **Community Support**

مزیت:

- پیدا کردن راه‌حل سریع
- فهمیدن مشکلات عمومی نرم‌افزار

مشکلات و راه‌حل

مشکل	علت احتمالی	راه‌حل
سیستم کند	فایل‌های زیاد	کاهش حجم
Login مشکل	نرم‌افزار Bug	بررسی Forum
امنیت ضعیف	رمز ساده	رمز قوی
نمایش خراب	ناسازگاری مرورگر	تست چند Browser

مثال واقعی

یک دانش آموز متوجه می‌شود:

پروفایل در **Firefox** درست کار نمی‌کند.

او:

- **Forum** نرم‌افزار را بررسی می‌کند
- می‌بیند دیگران هم همین مشکل را دارند
- **Update** جدید نصب می‌کند

مشکل حل می‌شود.

توجیه ابزارهای استفاده‌شده برای ساخت پروفایل دیجیتلی

در این بخش، دانش آموز باید توضیح دهد که چرا برای ساخت پروفایل دیجیتلی خود از ابزارها و برنامه‌های خاص استفاده کرده است. هدف فقط استفاده از نرم‌افزار نیست، بلکه دانش آموز باید بتواند انتخاب خود را با دلیل، تحقیق و تحلیل توجیه کند. یعنی نشان دهد که ابزار انتخاب‌شده برای هدف پروژه مناسب بوده و چه مزایا و محدودیت‌هایی داشته است.

چرا انتخاب ابزار مهم است؟

هر نرم‌افزار یا سیستم ویژگی‌های متفاوت دارد.

بعضی ابزارها:

- آسان‌تر هستند
- امنیت بهتر دارند
- طراحی حرفه‌ای‌تر ارائه می‌کنند
- فضای ذخیره بیشتر دارند

بنابراین انتخاب درست ابزار، کیفیت پروفایل را بهتر می‌سازد.

ePortfolio Platform چیست؟

Platform یعنی سیستمی که پروفایل آنلاین در آن ساخته می‌شود.

مثال‌ها:

- **Mahara**
- **Google Sites**
- **WordPress**
- **Wix**

این سیستم‌ها کمک می‌کنند:

- فایل‌ها مدیریت شود
- محتوا آنلاین نمایش داده شود
- کاربران به پروفایل دسترسی پیدا کنند

چرا Mahara استفاده می‌شود؟

Mahara یک سیستم **Open Source** برای ساخت **ePortfolio** است.

مزیت‌های آن:

- رایگان
- مناسب آموزش
- قابلیت اشتراک‌گذاری
- مدیریت آسان فایل‌ها
- مناسب برای مکاتب و پوهنتون‌ها

تحلیل نقاط قوت و ضعف

دانش آموز باید فقط مزایا را نگوید؛ بلکه ضعف‌ها را نیز تحلیل کند.

مثال:

ابزار	قوت	ضعف
Mahara	رایگان و آموزشی	طراحی محدود
Google Sites	ساده و سریع	امکانات کم
WordPress	حرفه‌ای	نیاز به مهارت بیشتر

این نشان می‌دهد دانش آموز تحلیل واقعی انجام داده است.

نقش تحقیق در انتخاب ابزار

قبل از انتخاب**Platform** ، دانش آموز باید:

- امکانات سیستم را بررسی کند
- امنیت آن را بسنجد
- نظر کاربران را بخواند
- هزینه و سهولت استفاده را مقایسه کند

سپس بهترین گزینه را انتخاب کند.

جدول مقایسه ابزارها

سیستم	نوع	مزیت	محدودیت
Mahara	**Open Source**	مناسب آموزش	ظاهر ساده
Google Sites	**Cloud**	آسان	امکانات محدود
WordPress	**Web Platform**	حرفه‌ای	پیچیده‌تر
Wix	**Website Builder**	طراحی زیبا	بعضی امکانات پولی

مثال واقعی

یک دانش آموز بین **Mahara** و **WordPress** انتخاب می‌کند.

او تحقیق می‌کند:

- **Mahara** برای آموزش مناسب‌تر است
- **WordPress** حرفه‌ای‌تر اما پیچیده‌تر است

در نتیجه **Mahara** را انتخاب می‌کند چون:

- رایگان است
- برای **ePortfolio** طراحی شده
- استفاده آسان دارد

توضیح روش‌های بهبود آینده پورتفلیوی دیجیتلی

در این بخش، دانش آموز باید توضیح دهد که چگونه می‌تواند پورتفلیوی دیجیتلی خود را در آینده بهتر و پیشرفته‌تر بسازد. هدف این است که دانش آموز درک کند هیچ پروژه یا سیستم دیجیتلی کاملاً پایان

نمی‌یابد و همیشه امکان پیشرفت، بروزرسانی و اصلاح وجود دارد. **ePortfolio** فقط برای امروز نیست؛ بلکه بخشی از یادگیری دوامدار (**Lifelong Learning**) و آینده تحصیلی و کاری فرد می‌باشد.

چرا پورتفلیو باید همیشه بروزرسانی شود؟

مهارت‌ها و تکنالوژی همیشه تغییر می‌کنند.

اگر پورتفلیو بروزرسانی نشود:

- معلومات قدیمی می‌شود
- مهارت‌های جدید نمایش داده نمی‌شود
- برای کار یا پوهنتون کمتر مفید می‌شود

بنابراین باید به‌طور دوامدار بهبود پیدا کند.

راه‌های بهبود پورتفلیو در آینده

دانش آموز می‌تواند:

- مهارت‌های جدید اضافه کند
- طراحی حرفه‌ای‌تر بسازد
- پروژه‌های جدید شامل کند
- امنیت سیستم را بهتر کند
- نسخه موبایل را قوی‌تر سازد
- محتوای قدیمی را اصلاح کند

نقش ePortfolio در آینده

پورتفلیو می‌تواند برای:

- درخواست کار
- ادامه تحصیل
- اپرنتیس‌شیپ **(Apprenticeship)**
- معرفی مهارت‌ها

استفاده شود.

یعنی پورتفلیو یک معرفی دیجیتلی حرفه‌ای از فرد است.

Lifelong Learning چیست؟

Lifelong Learning یعنی یادگیری همیشگی در تمام زندگی.

در دنیای دیجیتلی:

- مهارت‌ها سریع تغییر می‌کند
- نرم‌افزارها بروزرسانی می‌شود
- نیاز بازار کار تغییر می‌کند

پس دانش آموز باید همیشه:

- یاد بگیرد

- تمرین کند
- پورتفلیوی خود را بهتر سازد.

روش‌های بهبود

روش بهبود	فایده
اضافه کردن پروژه جدید	نمایش تجربه بیشتر
طراحی بهتر	ظاهر حرفه‌ای
افزایش امنیت	محافظت از معلومات
بروزرسانی محتوا	جدید و مفید ماندن
سازگاری موبایل	دسترسی آسان

مهارت‌های آینده

مهارت	اهمیت
طراحی دیجیتلی	**ارائه حرفه‌ای**
امنیت سایبری	**محافظت از داده**
مدیریت فایل	**نظم بهتر**
ارتباط آنلاین	**همکاری بهتر**
تولید محتوا	**نمایش توانایی‌ها**

مثال واقعی

یک دانش آموز در صنف ۱۰ فقط مهارت **Word** و **PowerPoint** دارد.

بعداً:

- **Photoshop** یاد می‌گیرد
- طراحی ویب یاد می‌گیرد
- پروژه‌های جدید اضافه می‌کند

پورتفلیوی او حرفه‌ای‌تر و قوی‌تر می‌شود.

نکات مهم

- پورتفلیو باید همیشه بروزرسانی شود
- مهارت‌های جدید باید اضافه گردد
- طراحی و امنیت باید بهتر شود
- یادگیری هیچ‌وقت متوقف نمی‌شود

ارزیابی ابزارهای استفاده‌شده و پیشنهاد آن‌ها به دیگران

در این بخش، دانش آموز باید ابزارها و نرم‌افزارهایی را که برای ساخت پورتفلیوی دیجیتلی خود استفاده کرده است، ارزیابی کند و توضیح دهد که این ابزارها چگونه باعث افزایش سرعت، آسانی کار، نظم و صرفه‌جویی در وقت شده‌اند. همچنان باید بتواند بر اساس تجربه واقعی خود، این ابزارها را به دیگران پیشنهاد کند.

هدف این است که دانش آموز فقط "استفاده‌کننده" نرم‌افزار نباشد، بلکه بتواند تشخیص دهد:

- کدام ابزار مؤثرتر است
- کدام نرم‌افزار کار را سریع‌تر می‌سازد
- کدام سیستم برای کاربران دیگر مناسب‌تر است

Productivity چیست؟

Productivity یعنی افزایش سرعت و کیفیت انجام کار.

مثال:

اگر یک نرم‌افزار باعث شود:

- کار سریع‌تر انجام شود
- فایل‌ها منظم‌تر شود
- اشتباهات کمتر شود

آن ابزار **Productivity** را افزایش داده است.

Efficiency چیست؟

Efficiency یعنی انجام کار با:

- وقت کمتر
- انرژی کمتر
- نتیجه بهتر

مثال:
استفاده از قالب‌های آماده **Canva** باعث صرفه‌جویی در زمان طراحی می‌شود.

اهمیت ارزیابی ابزارها

دانش آموز باید بعد از استفاده از ابزارها بررسی کند:

- آیا نرم‌افزار مفید بود؟
- آیا استفاده آن آسان بود؟
- آیا برای پروژه مناسب بود؟
- آیا دوباره از آن استفاده می‌کند؟

این تحلیل نشان‌دهنده درک حرفه‌ای دانش آموز است.

ابزارهایی که دانش آموز می‌تواند ارزیابی کند

ممکن است دانش آموز از این ابزارها استفاده کرده باشد:

- **Word**
- **PowerPoint**
- **Canva**
- **Mahara**
- **Google Sites**
- **Photoshop**
- **Video Editors**

ارزیابی ابزارها

ابزار	استفاده	مزیت	ضعف
Word	اسناد	ساده و سریع	طراحی محدود
Canva	طراحی	قالب آماده	بعضی امکانات پولی
PowerPoint	ارائه	مناسب پریزنتیشن	حجم زیاد فایل
Mahara	ePortfolio	مناسب آموزش	ظاهر ساده
Photoshop	ویرایش تصویر	حرفه‌ای	پیچیده

نمونه مهارت‌ها و پروژه‌ها

مهارت	نمونه پروژه
Website Production	ساخت وب‌سایت
Digital Animation	انیمیشن
Digital Image Production	طراحی تصویر
Digital Video	ویرایش ویدیو
Digital Games Production	ساخت بازی
Digital Publishing	نشر دیجیتلی

نظم‌دهی محتوا

دانش آموز ممکن است فایل‌های زیادی داشته باشد.

پس باید:

- فایل‌ها را دسته‌بندی کند
- بهترین پروژه‌ها را انتخاب کند
- محتوا را منظم نمایش دهد

تا پورتفلیو حرفه‌ای‌تر دیده شود.

مثال واقعی

یک دانش آموز:

- برای طراحی از Canva استفاده می‌کند
- برای اسناد از Word
- برای پروفایل از Mahara

بعد از ارزیابی می‌گوید:

Canva:

- سریع

- آسان
- مناسب طراحی صنفی

اما:

- بعضی ابزارها پولی است

سپس آن را به دیگران پیشنهاد می‌کند.

نکات مهم

- هر ابزار باید تحلیل شود
- سرعت و کیفیت مهم است
- قوت و ضعف باید ذکر شود
- ابزار مناسب باید به دیگران پیشنهاد شود

جدول لغات

لغت (Term)	مخفف / Full Form	معنی دری	کاربرد
ICT	Information & Communication Technology	تکنالوژی معلومات و ارتباطات	استفاده در آموزش و سیستم‌های دیجیتلی
Cybersecurity	—	امنیت سایبری	محافظت سیستم و دیتا
Data	—	دیتا / معلومات	ذخیره و انتقال معلومات
Digital Material	—	مواد دیجیتلی	فایل‌ها، تصاویر، اسناد
Information Security	InfoSec	امنیت معلومات	حفاظت معلومات حساس
Data Protection	—	محافظت دیتا	جلوگیری از نشت معلومات
Personal Security	—	امنیت شخصی	محافظت معلومات فردی
Malware	Malicious Software	بدافزار	تخریب یا سرقت دیتا
Virus	—	ویروس	آلوده ساختن سیستم
Worm	—	کرم نرم‌افزاری	انتشار خودکار در شبکه
Trojan	Trojan Horse	تروجان	بدافزار مخفی
Spyware	—	نرم‌افزار جاسوسی	نظارت مخفی
Ransomware	—	باج‌افزار	قفل کردن فایل‌ها
Antivirus	Anti-Virus	ضد ویروس	حذف ویروس‌ها
Firewall	—	دیوار آتش	جلوگیری از نفوذ
IDS	Intrusion Detection System	سیستم تشخیص نفوذ	شناسایی حملات
IPS	Intrusion Prevention System	سیستم جلوگیری نفوذ	توقف حملات
Encryption	—	رمزگذاری	مخفی‌سازی دیتا
Decryption	—	رمزگشایی	باز کردن رمز
Encryption Key	—	کلید رمز	باز کردن دیتای رمزگذاری‌شده
Password	—	رمز عبور	محافظت حساب
Strong Password	—	رمز قوی	جلوگیری از هک
2FA	Two-Factor Authentication	تأیید دو مرحله‌ای	امنیت بیشتر ورود
Authentication	—	تصدیق هویت	تشخیص کاربر واقعی
Authentication Token	—	کود تأیید	ورود امن

Authorization	—	اجازه دسترسی	تعیین سطح دسترسی
Access Rights	—	سطح دسترسی	کنترول کاربران
Access Control	—	کنترول دسترسی	مدیریت اجازه‌ها
Permissions	—	مجوزها	تعیین نوع دسترسی
User Account	—	حساب کاربری	ورود کاربر
Login	Log In	ورود به سیستم	دسترسی به حساب
Logout	Log Out	خروج از سیستم	ختم نشست کاربر
Read Only	—	فقط خواندن	جلوگیری از تغییر فایل
Full Control	—	کنترول کامل	دسترسی کامل
Write	—	نوشتن	امکان تغییر فایل
Privacy	—	حریم خصوصی	محافظت معلومات شخصی
Privacy Settings	—	تنظیمات حریم خصوصی	محدود کردن نمایش معلومات
VPN	Virtual Private Network	شبکه خصوصی مجازی	اتصال امن اینترنت
Proxy	Proxy Server	واسطه اینترنت	تغییر مسیر اتصال
HTTP	HyperText Transfer Protocol	پروتوکول عادی ویب	انتقال غیرامن دیتا
HTTPS	HyperText Transfer Protocol Secure	پروتوکول امن ویب	انتقال امن دیتا
SSL	Secure Sockets Layer	گواهی امنیتی	امنیت ویب‌سایت
TLS	Transport Layer Security	امنیت انتقال دیتا	محافظت ارتباط
Secure Protocol	—	پروتوکول امن	انتقال امن معلومات
Secure Connection	—	ارتباط امن	جلوگیری از شنود
Network Security	—	امنیت شبکه	محافظت شبکه
Server	—	سرور	ذخیره و مدیریت دیتا
Secure Server	—	سرور امن	محافظت پیشرفته
Router	—	روتر	مدیریت شبکه
Port	—	دروازه ارتباط	مسیر انتقال دیتا
DMZ	Demilitarized Zone	منطقه جدا امنیتی	محافظت شبکه
IoT	Internet of Things	اینترنت اشیا	دستگاه‌های هوشمند
Cloud Storage	—	ذخیره ابری	نگهداری آنلاین فایل
Local Storage	—	ذخیره محلی	ذخیره در دستگاه
Cloud Security	—	امنیت کلود	محافظت دیتای آنلاین

Backup	—	نسخه پشتیبان	جلوگیری از ضایع شدن
Data Loss	—	از دست رفتن دیتا	نابودی معلومات
Data Breach	—	نشت دیتا	افشای معلومات
Vulnerability	—	آسیب‌پذیری	نقطه ضعف امنیتی
Threat	—	تهدید	خطر برای سیستم
Risk	—	ریسک	احتمال خطر
Protection Mechanism	—	روش محافظتی	جلوگیری از تهدید
Monitoring	—	نظارت	بررسی فعالیت‌ها
Log File	—	فایل ثبت فعالیت	تحلیل حملات
Patch	—	اصلاح امنیتی	رفع ضعف نرم‌افزار
Update	—	بروزرسانی	بهبود امنیت
Exploit	—	سوءاستفاده از ضعف	حمله به سیستم
Hacking	—	هک	دسترسی غیرمجاز
Brute Force Attack	—	حمله حدس رمز	امتحان رمزهای مختلف
Bot Attack	—	حمله ربات	حمله خودکار
Phishing	—	فیشینگ	فریب برای گرفتن معلومات
Pharming	—	فارمینگ	هدایت به سایت جعلی
Social Engineering	—	مهندسی اجتماعی	فریب انسان
Identity Theft	—	سرقت هویت	سوءاستفاده شخصی
Online Fraud	—	تقلب آنلاین	سرقت پول
Fraud	—	تقلب	استفاده نادرست از دیتا
Cybercrime	—	جرایم سایبری	جرم دیجیتلی
Cyberbullying	—	آزار آنلاین	اذیت اینترنتی
Spam	—	پیام ناخواسته	ایمیل اضافی
Public Wi-Fi	—	وای‌فای عمومی	اتصال پرخطر
Private Network	—	شبکه خصوصی	امنیت بیشتر
Digital Footprint	—	ردپای دیجیتلی	آثار فعالیت آنلاین
Security Protocols	—	پروتوکول‌های امنیتی	قوانین امنیت سیستم
AUP	Acceptable Use Policy	پالیسی استفاده قابل قبول	قوانین استفاده سیستم

CAPTCHA	Completely Automated Public Turing test	کپچا	تشخیص انسان از ربات
reCAPTCHA	Google reCAPTCHA	کپچای گوگل	جلوگیری از حمله ربات
Operating System	OS	سیستم‌عامل	مدیریت کمپیوتر
Browser	Web Browser	مرورگر	باز کردن ویب‌سایت
Open Source	—	متن‌باز	نرم‌افزار قابل توسعه
GitHub	—	گیت‌هاب	اشتراک کد و پروژه
ePortfolio	Electronic Portfolio	پورتفولیوی دیجیتلی	نمایش مهارت‌ها
Digital Profile	—	پروفایل دیجیتلی	معرفی آنلاین
Digital Literacy	—	سواد دیجیتلی	مهارت استفاده تکنالوژی
CV	Curriculum Vitae	رزومه	معرفی تحصیلی و کاری
Presentation	—	ارائه	نمایش معلومات
Documents	—	اسناد	ذخیره معلومات
Word	Microsoft Word	ورد	نوشتن اسناد
Excel	Microsoft Excel	اکسل	محاسبه و تحلیل دیتا
PowerPoint	Microsoft PowerPoint	پاورپوینت	ارائه معلومات
PDF	Portable Document Format	پی‌دی‌اف	نمایش ثابت فایل
.docx	Word File Format	فایل ورد	سند قابل ویرایش
Website Production	—	تولید ویب‌سایت	ساخت سایت
Digital Animation	—	انیمیشن دیجیتلی	ساخت حرکت گرافیکی
Digital Video	—	ویدیوی دیجیتلی	تولید ویدیو
Digital Publishing	—	نشر دیجیتلی	نشر آنلاین محتوا
Digital Communication	—	ارتباط دیجیتلی	ارتباط آنلاین
Digital Games Production	—	تولید بازی دیجیتلی	ساخت بازی
Mahara	Mahara ePortfolio System	سیستم مهارا	ساخت ePortfolio
ISP	Internet Service Provider	شرکت خدمات اینترنت	فراهم‌سازی اینترنت
Wi-Fi	Wireless Fidelity	وای‌فای	اتصال بی‌سیم
Bluetooth	—	بلوتوث	انتقال بی‌سیم
NFC	Near Field Communication	ارتباط نزدیک	انتقال کوتاه‌برد
SMS	Short Message Service	پیامک	ارسال پیام

بحث و کمک	انجمن آنلاین	–	**Forum**
نشر محتوا	بلاگ	Weblog	**Blog**
جمع‌آوری بازخورد	نظرسنجی	–	**Survey**
ارزیابی سیستم	بازخورد	–	**Feedback**
ظاهر مناسب کاری	نیمه‌حرفه‌ای	–	**Semi-professional**

منابع

1. Cybersecurity Essentials. (n.d.). *Cybersecurity essentials*. Cisco Networking Academy.
2. Introduction to Cyber Security. (n.d.). *Introduction to cyber security*. OpenLearn.
3. National Institute of Standards and Technology. (n.d.). *NIST cybersecurity framework*. NIST.
4. Computer Security: Principles and Practice. Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
5. Cybersecurity and Cyberwar: What Everyone Needs to Know. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
6. OWASP Foundation. (n.d.). *OWASP top 10 web application security risks*. OWASP Foundation.
7. The Web Application Hacker’s Handbook. Stuttard, D., & Pinto, M. (2011). *The web application hacker’s handbook: Finding and exploiting security flaws* (2nd ed.). Wiley.
8. Google Safety Center. (n.d.). *Google Safety Center*. Google.
9. Kaspersky Cybersecurity Resource Center. (n.d.). *Kaspersky cybersecurity resource center*. Kaspersky.
10. National Cyber Security Centre. (n.d.). *National Cyber Security Centre guidance*. NCSC.
11. Basic Concepts of Information and Communication Technology. Celebic, G., & Rendulic, D. I. (n.d.). *Basic concepts of information and communication technology*.
12. Cambridge IGCSE Information and Communication Technology. Brown, G., & Watson, D. (2012). *Cambridge IGCSE information and communication technology*. Cambridge University Press.
13. Introduction to Computer Security. Goodrich, M., & Tamassia, R. (2011). *Introduction to computer security*. Pearson.

درخواست ارسال نظریات اساتید

از آنجایی‌که این نخستین نسخهٔ کتاب **TLM Level 2** برای سطح دوم می‌باشد، احتمال موجودیت برخی خلاهای معلوماتی، اشتباهات تایپی و یا گنگ بودن بعضی موضوعات وجود دارد. بناءً از تمام اساتید و اهل مسلک محترم تقاضا می‌گردد، در صورتی‌که به مواردی نیازمند اصلاح، توضیح بیشتر یا تکمیل موضوعات برخورد نمودند، لطفاً از طریق آدرس‌های ذیل در کوتاه‌ترین فرصت با ما در میان بگذارند تا در نسخه‌های بعدی مورد بازنگری و تکمیل قرار گیرد.

راه‌های ارتباطی:

ایمیل آدرس: partner.affaire@eba.ac
شماره تماس: +447951869279
ایمیل نویسنده: rezvanpanah2@gmail.com

پیشاپیش از همکاری، نظریات سازنده و حمایت تمام استادان و همکاران محترم در راستای بهبود این اثر علمی صمیمانه سپاسگزاری می‌نماییم.