Jordan Youth Innovation Forum
الملتقى الأردني للإبداع الشبابي

EMSA

الإطار الأوروبي المرجعي :الكفاءات الأساسية للتعلم المستمر

3.الكفاءة الرقمية

الملتقى الأردني للأبداع الشبابي

مدة التدريب: 6.5 ساعات.

Co-funded by the European Union

بتمويل من الاتحاد الأوروبي. الآراء والآراء المعبر عنها هي آراء المؤلف (المؤلفين) فقط ولا تعكس بالضرورة آراء الاتحاد الأوروبي أو الوكالة الأوروبية للتعليم والثقافة (EACEA). ولا يمكن اعتبار الاتحاد الأوروبي ولا EACEA مسؤولين عنها.

مجموعة المشروع

منسق المشروع

MMC Mediterranean Management Centre

الشركاء

Cyprus Certification Company

DIMITRA educational organization

have a dream

Arab College of Applied Sciences

Jordan Youth Innovation Forum
الملتقى الأردني للإبداع الشبابي

تفاصيل المشروع

العنوان :التطوير المشترك و التجريب والتحقق من صحة المناهج الدراسيى والمواد التدريبية لتعزيز التفكر الريادي والمهارات الأساسية في الدول النامية.

اختصار المشروع :التفكير الرادي والمهارات للجميع

رقم الاتفاقية :إيراسموس – EMSA – 101092477 -EDU-2022-CB-VET

البرنامج :ايراسموس +لبناء القدرات في مجال التعليم والتدريب المهني

دعوة تقديم المقترحات :إيراسموس-EDU-2022-CB-VET

تاريخ البدء 1 :يناير 2023

تاريخ الانتهاء 31 :ديسمبر 2025

المبادى العامة والأليات والمنطق الكامن وراء تطور التكنولوجيا الرقمية

غرض التدريب

هدف التدريب :تقديم فهم شامل للآليات الأساسية والمنطق وراء تطور التكنولوجيا الرقمية .ستعرف هذه الجلسة المشاركين بأسس الرقمنة، وحماية البيانات، واللائحة العامة لحماية البيانات (GDPR)، بالإضافة إلى مهارات إدارة البيانات الضرورية في السياقات الشخصية والمهنية.

Descriptor

مخرجات التعلم

جميع مخرجات الكفاءة

فيما يتعلق بالمعرفة:

- تعريف الرقمنة ومبادئها الأساسية.
- تحليل المصادر الرقمية الموثوقة واسترجاع البيانات ذات الصلة.
- وصف الامتثال للائحة العامة لحماية البيانات (GDPR)وقضايا حماية البيانات وسلامة الإنترنت.

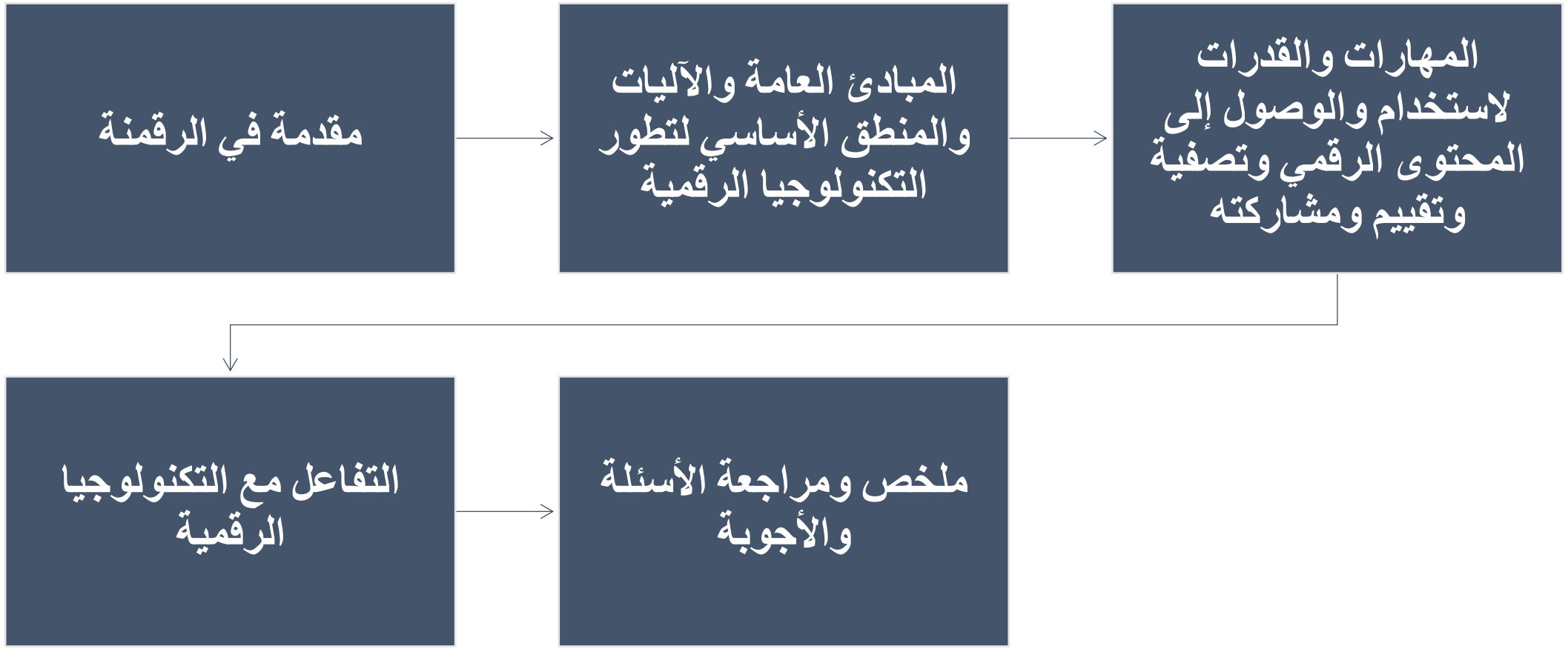
فيما يتعلق بالمهارات:

- إظهار القدرة على استخدام المنصات السحابية للتعاون وإنتاج المحتوى الرقمي.
- تطوير ومشاركة المحتوى الرقمي باستخدام المنصات الإعلامية المناسبة)نصوص، صور، صوت، فيديو.(
- تطبيق أدوات مثل Google Analyticsلتقييم تأثير المحتوى الرقمي.

فيما يتعلق بالمواقف:

- إظهار الاحترام للائحة العامة لحماية البيانات (GDPR)ومعايير حماية البيانات والأخلاقيات أثناء استخدام التكنولوجيا الرقمية.
- إظهار الثقة في تطبيق آداب التعامل عبر الإنترنت)الإتيكيت والنيتيكيت (في بيئات رقمية متنوعة.
- تنفيذ استراتيجيات لحماية النفس والآخرين من المخاطر والتهديدات على الإنترنت.

مخطط مسار التدريب

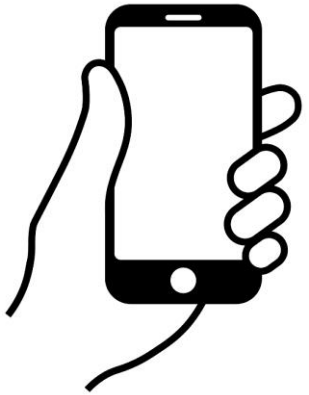


تشير الكفاءة الرقمية إلى القدرة على استخدام التقنيات الرقمية بثقة ومسؤولية في السياقات الشخصية والمهنية. ستركز هذه الدورة على الآليات والمبادئ الكامنة وراء التحول الرقمي، بما في ذلك حماية البيانات والامتثال لائحة حماية البيانات العامة (GDPR). سيتناول المشاركون المشهد المتطور للتقنيات الرقمية وسيتعلمون كيفية تطبيق مهارات الإدارة الرقمية لضمان سلامة البيانات، ودقتها، واستخدامها الأخلاقي في عالم اليوم المترابط.

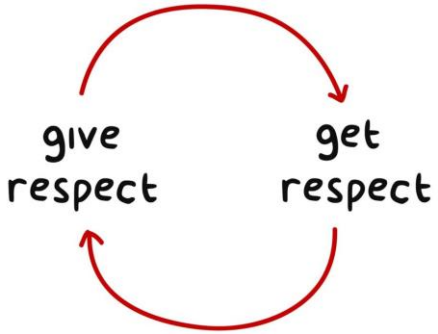
ما هي الكفاءة التي يتعلق بها تدريبنا في إطار الإطار الأوروبي المرجعي(ERF) ؟

EMSA

قواعد التدريب



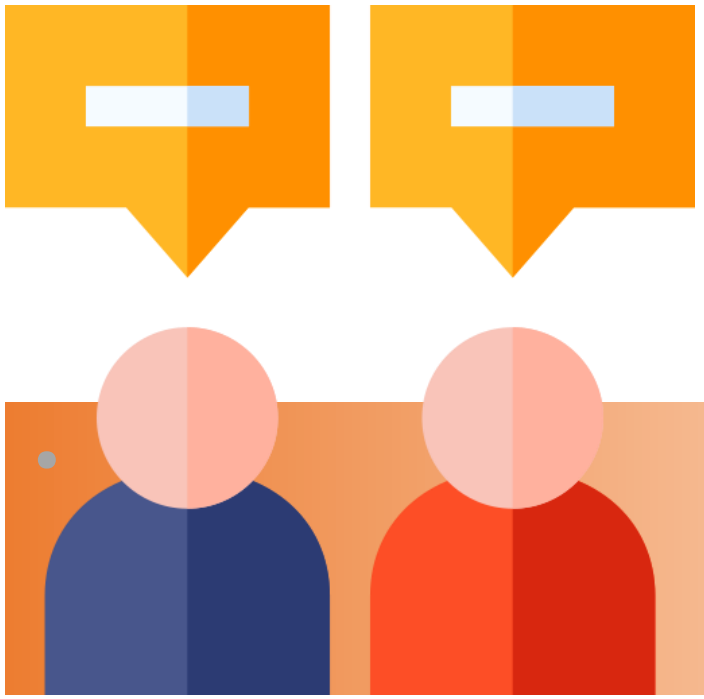
Participation



لعبة "بنجو الأثر الرقمي "هي نشاط مدته 15دقيقة، حيث يتفاعل المشاركون للعثور على أشخاص آخرين يشاركونهم تجارب رقمية مشابهة .يقومون بتعبئة بطاقات البنغو بمهمات مثل حضور اجتماع افتراضي أو استخدام التخزين السحابي .الفائز هو أول من يكمل صفًا أو عمودًا، وبعدها يُعقد نقاش حول التجارب الرقمية الفريدة لكل مشارك.

نشاط البنجو الرقمي

EMSA



مقدمة

لنتعرف على بعضنا البعض

"التكنولوجيا تكون في أفضل حالاتها عندما تجمع الناس معاً"

مات مولنويغ، مؤسس ووردبريس

مقدمة في الرقمنة

مقدمة عن الرقمنة

- **تعريف الرقمنة:**تشير الرقمنة إلى دمج التكنولوجيا الرقمية في العمليات والأنشطة اليومية، مما يُحول طريقة عمل الشركات والحكومات والأفراد .وهي تشمل تحويل المعلومات إلى صيغة رقمية، وتحسين سير العمل، وتمكين طرق جديدة للتواصل وتقديم الخدمات .تمتد الرقمنة إلى ما هو أبعد من مجرد تحويل البيانات الموجودة إلى صيغة رقمية؛ إذ تعيد تشكيل نماذج الأعمال بالكامل، والقطاعات الاقتصادية، ووظائف المجتمع من خلال استغلال قوة التكنولوجيا الرقمية لخلق قيمة، وزيادة الكفاءة، وتعزيز التجارب.

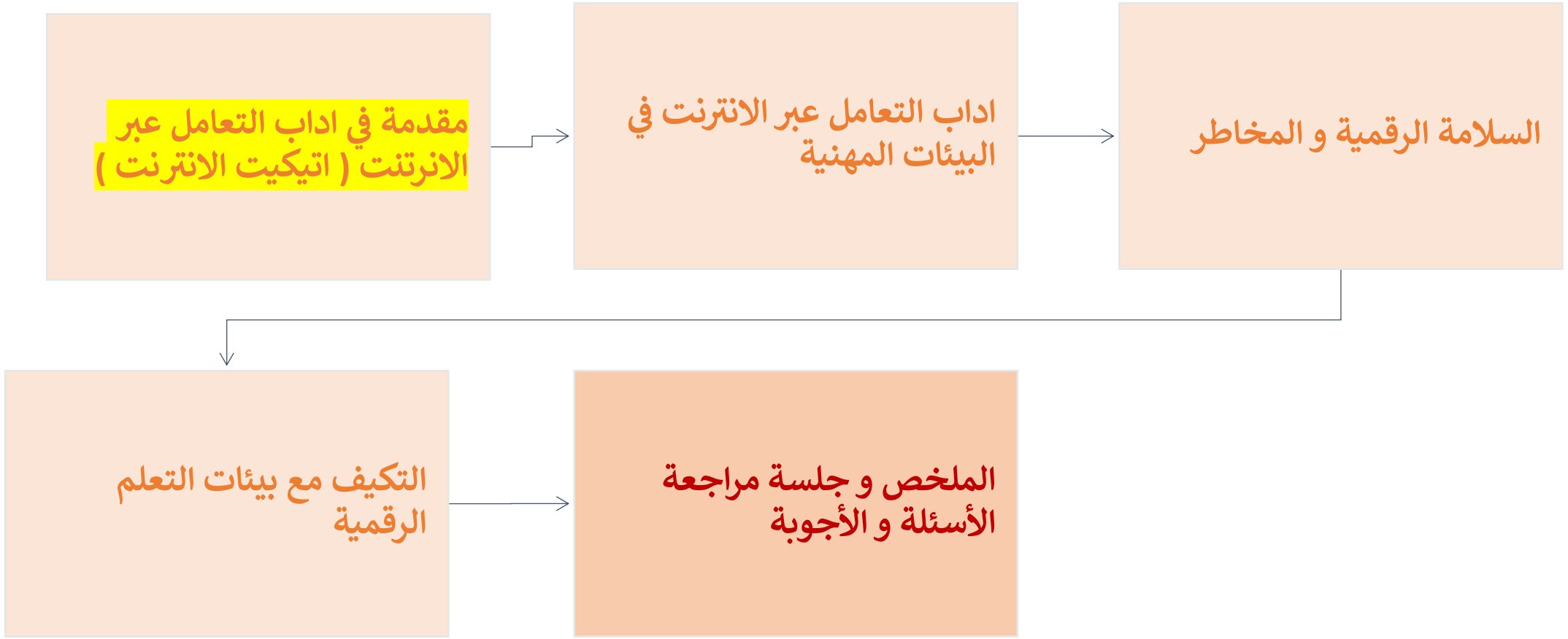
الجوانب والأمثلة

- **الجوانب الرئيسية:**
- **الأتمتة :**استبدال المهام اليدوية بعمليات رقمية آلية، مما يحسن السرعة ويقلل من الأخطاء البشرية.
- **التحليل المعتمد على البيانات :**الاستفادة من البيانات الرقمية لاتخاذ قرارات مستنيرة، وتحليل الاتجاهات، والتنبؤ بالنتائج المستقبلية.
- **الاتصال :**تعزيز التواصل من خلال الشبكات والإنترنت، مما يتيح التعاون الفوري عبر الحدود الجغرافية.
- **الابتكار :**تمكن الرقمنة من إنشاء منتجات وخدمات وحتى صناعات جديدة من خلال استغلال التقدم التكنولوجي.

- **أمثلة:**
- **الرعاية الصحية :**استخدام سجلات المرضى الرقمية، والطب عن بُعد، والتشخيصات المدعومة بالذكاء الاصطناعي.
- **التجزئة :**منصات التجارة الإلكترونية التي تحول طريقة تسوق العملاء وتفاعلهم مع العلامات التجارية.
- **التعليم :**منصات التعلم عبر الإنترنت التي توفر إمكانية الوصول إلى التعليم للطلاب حول العالم.

الموضوع 3 . المشاركة مع التقنيات الرقمية

الموضوع 3 خريطة الطريق



"الإنترنت هو أول شيء بنته البشرية دون أن تفهمه، وهو أكبر تجربة في الفوضى شهدناها على الإطلاق."

— إريك شميدت، المدير التنفيذي السابق لشركة جوجل

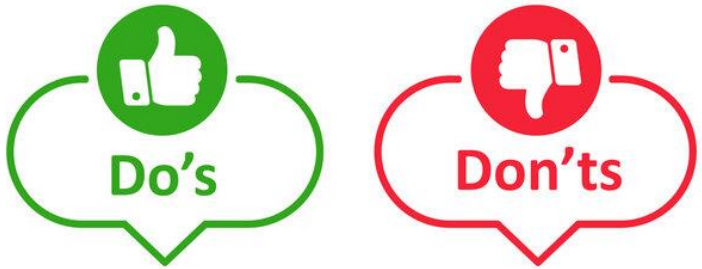
مقدمة إلى آداب السلوك عبر الانترنت (إتيكيت الانترنت)

تعريف إتيكيت الإنترنت:
إتيكيت الإنترنت هو مجموعة القواعد والسلوكيات المتوقعة للتواصل باحترام في البيئة الرقمية.

- **لماذا يعتبر ذلك مهمًا:**
- مع ازدياد التواصل الرقمي، يصبح من الضروري الحفاظ على تفاعلات مهنية ومحترمة لبناء علاقات إيجابية ومجتمعات على الإنترنت.
- **اللغة والنبرة الاحترامية:**
- تأكد دائمًا من التواصل بطريقة تحترم الآخرين، وتجنب اللغة المسيئة أو غير اللائقة.
تذكر أن النص يفتقر إلى النبرة الصوتية—ما قد يبدو محايدًا بالنسبة لك قد يُفهم كوقاحة من قِبل شخص آخر.
- **تجنب الكتابة بالأحرف الكبيرة (الصراخ):**
- تُعتبر الكتابة بالأحرف الكبيرة بمثابة صراخ أو عدوانية. استخدم الكتابة بحالة الأحرف القياسية للتعبير عن وجهة نظرك بطريقة مهنية.
- **الاعتراف الصحيح بعمل الآخرين:**
- قم دائمًا بإعطاء الفضل للجهة الأصلية التي أنشأت المحتوى (الأفكار، الاقتباسات، الموارد) لتجنب الانتحال وإظهار الاحترام للملكية الفكرية.
- **الامتناع عن الهجمات الشخصية أو "الفلمنغ":**
- تجنب التعليقات العدائية أو العدوانية، المعروفة باسم "الفلمنغ". المشاركة في الهجمات الشخصية تضر بالبيئة الإلكترونية وتُعطل التواصل المثمر.

آداب السلوك الرقمي: ما يجب فعله وما لا يجب فعله

- **ما يجب فعله :** كن مهذبًا، تحقق من معلوماتك، وابقَ على الموضوع.
- **ما لا يجب فعله:** تجنب نشر محتوى استفزازي، أو الرسائل غير المرغوب فيها، أو احتكار المناقشات.
- استخدام الرموز التعبيرية والفكاهة بشكل مناسب، تذكر أن النبرة يمكن أن تُساء فهمها.



أمثلة على الإتيكيت الجيد والسيئ عبر الإنترنت

أمثلة سلبية (الإتيكيت السيئ عبر الإنترنت)

1. **استخدام لغة عدائية**

1. المثال: "أنت مخطئ! هذا لا يُعقل، ومن الواضح أنك لم تفكر في ذلك جيدًا."

2. الشرح: هذا النوع من الردود يبدو عدائيًا ومتعاليًا، مما يمكن أن يؤدي إلى تصعيد النزاعات وإلحاق الضرر بالعلاقات

2. **عدم الإشارة إلى عمل الآخرين**

1. المثال: "أعتقد أنه ينبغي علينا التركيز على... (فكرة مأخوذة من شخص آخر دون اعتراف)."

2. الشرح: عدم الاعتراف بعمل أو أفكار شخص آخر يمكن أن يُعتبر انتحالًا أو عدم احترام، خاصة في البيئات المهنية أو الأكاديمية.

3. **الصراخ (استخدام الأحرف الكبيرة)**

1. المثال: "يرجى إرسال التقرير بحلول الساعة 5 مساءً اليوم!"
2. الشرح: استخدام الأحرف الكبيرة في التواصل المكتوب يُعتبر بمثابة صراخ ويمكن أن يُفهم كعدوانية، مما يؤدي إلى سوء الفهم أو نبرة سلبية.

أمثلة إيجابية (الإتيكيت الجيد عبر الإنترنت)

1. **استخدام لغة محترمة**

1. المثال: "شكرًا لك على ملاحظاتك. سأأخذ اقتراحاتك بعين الاعتبار للمشروع المقبل!"
2. الشرح: هذا الرد يُظهر اللباقة والانفتاح، ويشجع على تقديم ملاحظات بناءة، مما يعزز التواصل الإيجابي.

2. **الاعتراف بعمل الآخرين المثال:**

1. المثال: "كما ذكر [اسم] في تقريره، يجب أن نركز على..."
2. الشرح: إعطاء الفضل حيث يستحق يُظهر الاحترام لمساهمات الآخرين ويضمن الاعتراف بالملكية الفكرية

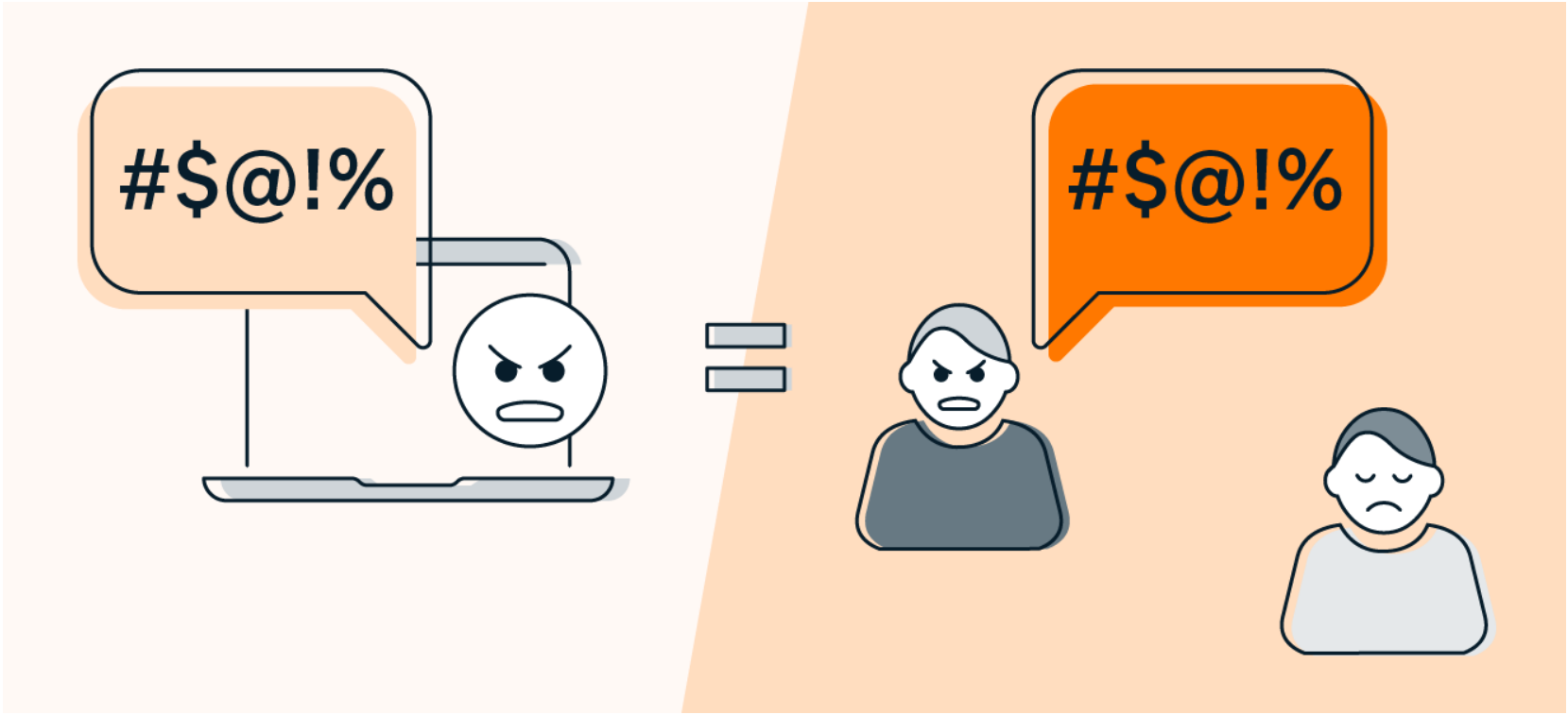
3. **استخدام تنسيق مناسب (تجنب الكتابة بالأحرف الكبيرة)**

1. المثال: "يرجى مراجعة الوثيقة المرفقة وإخباري برأيك."

2. الشرح: الاستخدام الصحيح للقواعد النحوية وعلامات الترقيم والتنسيق (دون استخدام قفل الأحرف) يضمن أن الرسالة مهنية وواضحة.

التفكير في سيناريوهات سوء الاتيكيت على الإنترنت

MT3.3_1



الموضوع 3.1: الاتيكيت على الإنترنت في البيئات المهنية

ما هو الاحتراف في البيئات عبر الإنترنت؟

- الاحتراف: مجموعة من السلوكيات وتقنيات التواصل المتوقعة في بيئة مهنية.
يتضمن الاحتراف عبر الإنترنت:
- استخدام لغة رسمية.
- الالتزام بسياسات الشركة.
- الحفاظ على التواصل الاحترامي والواضح.

المبادئ الأساسية للتواصل المهني عبر الإنترنت

- استخدام التحيات والإغلاق المناسبين:
- ابدأ بتحيات رسمية وأنهِ برسالة وداع مهذبة.
- مثال: "عزيزي/عزيزتي السيدة سميث" أو "مع أطيب التحيات، [اسمك]."

كن موجزًا وواضحًا:

- تواصل بفعالية وتجنب الغموض.
- مثال: "يرجى إكمال المهمة المرفقة بحلول يوم الجمعة."

احترام الوقت والحدود:

- أرسل الرسائل أو البريد الإلكتروني خلال ساعات العمل المناسبة.

التعامل مع سوء الفهم بشكل احترافي:

- احل النزاعات بأسلوب هادئ وبنّاء.

مثال على التواصل المهني السيء

- "مرحبًا فريق! الأمر عاجل! أحتاج هذا الآن!

- "هل يمكنك إنجاز ذلك في أسرع وقت ممكن؟ لا يهم كيف، فقط قم بإتمام المهمة "

مثال على التواصل المهني الصحيح

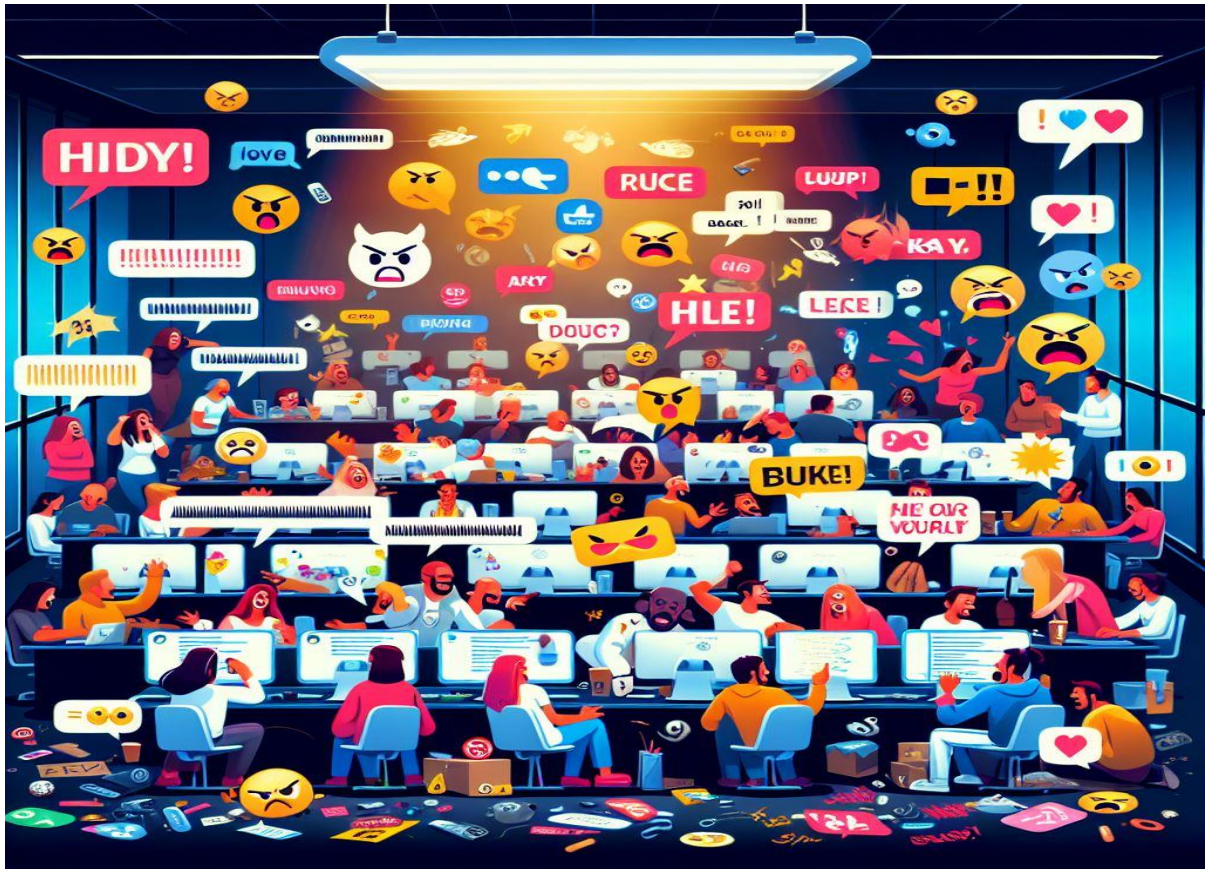
- "فريق العمل العزيز،

آمل أن تكونوا بخير. هل يمكنكم من فضلكم إتمام المهمة المرفقة بنهاية اليوم؟ إذا كنتم بحاجة إلى أي مساعدة، فلا تترددوا في إخباري.

مع أطيب التحيات،
[اسمك]."

تحسين رسائل البريد الإلكتروني المهنية

MT3.3_2



تحديات التواصل الرقمي المهني

سوء تفسير النغمة:

- **التحدي:** يفتقر التواصل القائم على النص إلى المؤشرات الصوتية، مما يجعل من الصعب نقل النغمة. فقد يُفسَّر ما يبدو كرسالة محايدة على أنه قاسٍ أو غير ودود.
- **الحل:** استخدم لغة واضحة وموجزة. تجنب السخرية أو التعبيرات غير الرسمية بشكل مفرط. اعتبر إضافة عبارات توضيحية، أو، عند الاقتضاء، رموز تعبيرية للتعبير عن النية.

حدود العمل والحياة:

- **التحدي:** مع وجود أدوات رقمية مثل البريد الإلكتروني وتطبيقات المراسلة، توجد توقعات دائمة للتوفر، مما ي blurالحدود بين الوقت الشخصي والعمل.
- **الحل:** حدد حدودًا واضحة لمتى تكون متاحًا. قم بالتواصل مع فريقك حول ساعات العمل الخاصة بك، واستخدم أدوات مثل ميزات "عدم الإزعاج" لحماية وقتك الشخصي.

نقص الإشارات البصرية أو الصوتية:

- **التحدي:** في التواصل الرقمي، تكون لغة الجسد والتعبيرات الوجهية ونبرة الصوت غائبة، مما قد يؤدي إلى سوء الفهم أو نقص الوضوح.
- **الحل:** استخدم مؤتمرات الفيديو للمناقشات الأكثر تعقيدًا، أو استخدم الرسائل الصوتية عند الاقتضاء. بالنسبة للتواصل الكتابي، كن محددًا قدر الإمكان لتجنب سوء التفسير.

الإفراط في استخدام اللغة غير الرسمية:

- **التحدي:** يمكن أن يؤدي التواصل الرقمي، وخاصة عبر الرسائل الفورية، إلى تواصل غير رسمي بشكل مفرط قد لا يكون مناسبًا للإعدادات المهنية.
- **الحل:** قم دائمًا بتقييم السياق والجمهور. استخدم لغة مهنية مع العملاء أو في المناقشات الرسمية. عدِّل مستوى الرسمية بناءً على الإعداد.

التغلب على التحديات في التواصل الرقمي المهني

MT3.3_3

الموضوع 3.2: السلامة الرقمية والمخاطر

ما هي السلامة الرقمية؟
تشير السلامة الرقمية إلى الممارسات التي تحمي المستخدمين من المخاطر والأذى عند التفاعل في البيئات الرقمية.

مجالات التركيز الرئيسية:

- **خصوصية البيانات:** حماية المعلومات الشخصية من الوصول غير المصرح به.
- **الأمن السيبراني:** حماية الأنظمة والشبكات من الهجمات.
- **حماية الهوية الرقمية:** ضمان عدم سرقة أو إساءة استخدام الهويات الشخصية على الإنترنت.

المخاطر الشائعة على الإنترنت:

- **الاحتيال Phishing** : محاولات احتيالية للحصول على معلومات حساسة من خلال التظاهر بكونها كيانًا موثوقًا.
- **البرمجيات الضارة Malware** : برامج ضارة مصممة لإيذاء أو استغلال أو تهديد الأجهزة الرقمية.
- **سرقة الهوية:** الاستحواذ الاحتيالي واستخدام المعلومات الشخصية الخاصة بشخص ما لتحقيق مكاسب مالية.
- **خرق البيانات:** الوصول غير المصرح به إلى المعلومات الشخصية أو الحساسة مما قد يؤدي إلى سوء استخدامها

حماية الهوية الرقمية

- **كلمات مرور قوية :** استخدام كلمات مرور معقدة وفريدة لكل منصة.
- **المصادقة الثنائية :** إضافة طبقة أمان إضافية من خلال مطالبة المستخدم بشكل ثانٍ من التعريف.
- **التصفح الآمن :** التأكد من أن المواقع آمنة قبل إدخال المعلومات الشخصية.(HTTPS)
- **تجنب مشاركة المعلومات الشخصية :** الحد من مشاركة التفاصيل الشخصية على وسائل التواصل الاجتماعي أو المواقع غير الآمنة .

التهديدات الرقمية وكيفية التعامل معها

1. **هجمات الصيد الاحتيالي:**
   - **التعريف**: محاولات احتيالية للحصول على معلومات حساسة (مثل كلمات المرور، وأرقام بطاقات الائتمان) من خلال التظاهر بكونها كيانًا موثوقًا عبر البريد الإلكتروني أو الهاتف أو الرسائل النصية.
   - **كيفية التعامل مع الصيد الاحتيالي:**
     - لا تنقر على الروابط في رسائل البريد الإلكتروني غير المرغوب فيها.
     - تحقق من هوية المرسل من خلال الاتصال بالشركة مباشرة عبر قنوات الاتصال الرسمية.
     - قم بالإبلاغ عن محاولات الصيد الاحتيالي لمزود البريد الإلكتروني الخاص بك أو قسم تكنولوجيا المعلومات.
2. **البرمجيات الخبيثة (الفيروسات، أحصنة طروادة، برامج الفدية)**
   - **التعريف:** البرمجيات الضارة المصممة لإلحاق الضرر أو استغلال الأجهزة أو الشبكات أو البيانات.
   - **كيفية التعامل مع البرمجيات الخبيثة:**
     - تثبيت وتحديث برامج مكافحة الفيروسات والبرمجيات الخبيثة بانتظام.
     - تجنب تحميل المرفقات من مصادر غير معروفة.
     - النسخ الاحتياطي للبيانات المهمة بانتظام تحسبًا لهجمات برامج الفدية أو أي هجمات قد تضر بالبيانات
3. **سرقة الهوية**
   - **التعريف:** الاستخدام الاحتيالي لهوية شخص آخر، عادةً لتحقيق مكاسب مالية.
   - **كيفية التعامل مع سرقة الهوية:**
     - استخدم كلمات مرور قوية وفريدة، وفعل خاصية التحقق الثنائي.
     - كن حذرًا عند مشاركة المعلومات الشخصية عبر الإنترنت.
     - راقب حساباتك المالية بانتظام لرصد أي نشاط مشبوه

التهديدات الرقمية وكيفية التعامل معها

4. اختراق البيانات

- **التعريف:** الوصول غير المصرح به إلى المعلومات الشخصية أو الحساسة، غالبًا من خلال القرصنة
- **كيفية التعامل مع اختراق البيانات:**
- تغيير كلمات المرور فور اكتشاف الاختراق.
- مراقبة الحسابات بحثًا عن أي علامات على سوء الاستخدام أو الاحتيال.
- تفعيل تنبيهات للنشاط غير المعتاد في الحساب واستخدام التشفير للبيانات الحساسة

5. هجمات الهندسة الاجتماعية

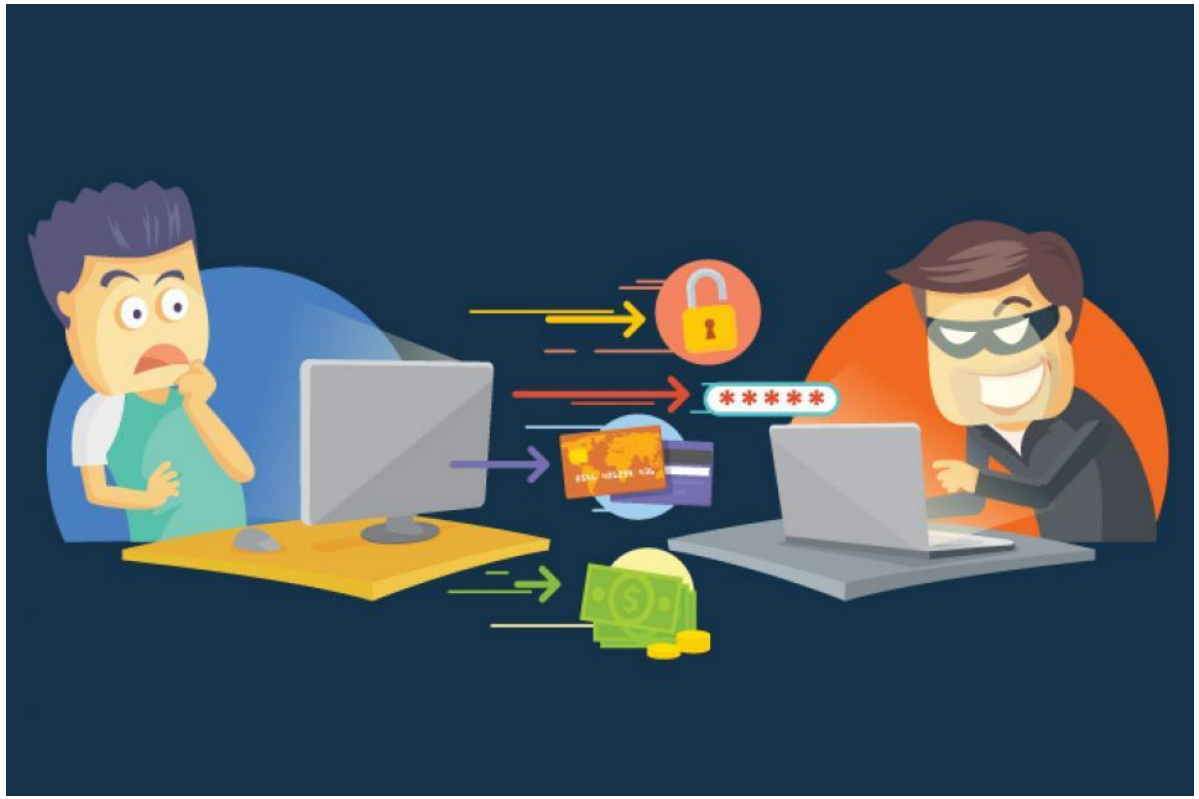
- **التعريف:** التلاعب بالأشخاص للكشف عن معلومات سرية من خلال الخداع (مثل: التظاهر بكون الشخص زميلًا).
- **كيفية التعامل مع الهندسة الاجتماعية:**
- كن حذرًا من الطلبات غير المطلوبة للمعلومات الحساسة، حتى لو كانت من أشخاص مألوفين.
- تحقق من الهويات من خلال قنوات الاتصال الثانوية (مثل: الاتصال بالشخص مباشرة).
- تعليم الموظفين كيفية التعرف على تقنيات الهندسة الاجتماعية

الاستجابة لتهديد رقمي

MT3.3_4

سرقة الهوية الرقمية

MT3.3_5



الموضوع 3.3: التكيف مع بيئات التعلم الرقمي

- **ما هو التعلم الرقمي؟**

التعلم الرقمي هو عملية اكتساب المهارات أو المعرفة باستخدام الأدوات والمنصات الرقمية

أمثلة:

- **تعلم في مكان العمل:** استخدام منصات مثل LinkedIn Learningأو Courseraلتعلم المهارات المتعلقة بالوظيفة.
- **التطوير الشخصي:** تطبيقات مثل Duolingo لتعلم اللغات أو Headspaceللرفاهية النفسية.
- **حل المشكلات اليومية:** دروس على YouTubeأو المنتديات الإلكترونية لتعلم مهارات جديدة أو حل المشكلات.
- **لماذا يعتبر التعلم الرقمي مهمًا ؟**

1. **المرونة:** التعلم بالوتيرة التي تناسبك، في أي وقت ومن أي مكان.
2. **سهولة الوصول:** تجعل الأدوات الرقمية التعلم متاحًا للجميع على مستوى العالم.
3. **تكلفة فعالة:** تقدم العديد من المنصات خيارات تعلم مجانية أو بأسعار معقولة.
4. **موجه ذاتيًا:** يمكنك تخصيص تعلمك وفقًا لاحتياجاتك وأهدافك.
5. **التعلم أثناء التنقل:** الوصول إلى المحتوى على مختلف الأجهزة، مما يسهل دمجه في الروتين اليومي.
6. **البقاء في المنافسة:** التكيف مع التقدم التكنولوجي والبقاء ذي صلة في مجالك

النقطة الأساسية:

- التعلم الرقمي متجذر في الحياة اليومية، سواءً كان ذلك لتطوير المهنة، أو النمو الشخصي، أو اكتساب المهارات العملية. التكيف مع هذا النمط من التعلم يضمن استمرار النمو في عالم غني بالمعلومات

التحديات الشائعة في التعلم الرقمي للحياة والعمل

- **الازدحام المعلوماتي:**
توجد كمية هائلة من الموارد عبر الإنترنت، مما يجعل من الصعب تحديد وجهة التركيز.

- **الإرهاق الرقمي:**
يمكن أن تؤدي الاعتماد المفرط على الشاشات إلى الإرهاق وفقدان الدافع.

- **الانضباط الذاتي:**
يتطلب التعلم الرقمي مستويات عالية من التحفيز الذاتي وإدارة الوقت، خاصةً في البيئات غير الرسمية (مثل مشاريع العمل أو الأهداف الشخصية).

- **الفجوات التكنولوجية:**
الصعوبة في استخدام بعض المنصات أو نقص المهارات الرقمية.

استراتيجيات التعلم الرقمي الفعال في العمل والحياة

- **حدد أهدافًا واضحة:**
حدد ما تريد تعلمه وضع أهدافًا قابلة للقياس (مثل اكتساب مهارة جديدة لمشروع عمل أو تحسين عادات الإنتاجية).
- **استخدم الأدوات المناسبة:**
اختر الأدوات أو المنصات الأكثر صلة بأهدافك التعليمية.
- **أمثلة:**
- لإدارة المشاريع، استخدم Trelloأو Monday.com.
- للتطوير الشخصي، استخدم تطبيقات مثل Headspaceأو Coursera.
- **إدارة الوقت:**
خصص وقتًا في جدولك للتعلم الذاتي والممارسة.
- **ابحث عن مجتمع:**
انضم إلى المنتديات عبر الإنترنت، أو الندوات، أو مجموعات الأقران لمشاركة تجربتك التعليمية والحصول على الدعم.

تطوير خطة تعليم رقمي شخصية

MT3.3_6

الأدوات الرقمية للتعلم المهني والحياتي

للعمل:

- أدوات إدارة المشاريع: Trello، Monday.com، Asana .
- مؤتمرات الفيديو: Zoom، Microsoft Teams .
- التدريب والتطوير: LinkedIn Learning، Coursera .

للنمو الشخصي:

- المالية الشخصية: Mint، You Need A Budget (YNAB) .
- الصحة والرفاهية: Headspace، MyFitnessPal .
- تطوير المهارات: Duolingo (تعلم اللغات)، Skillshare (المهارات الإبداعية).

لإدارة الحياة:

- إدارة الوقت: Google Calendar، Todoist .
- أدوات التنظيم: Evernote، Notion .

تكييف الاستراتيجيات الرقمية لسيناريوهات العمل

MT3.3_7

دراسة حالة – تعزيز المهارات الرقمية من أجل ترقية وظيفية

- **السيناريو:**

تم عرض ترقية على أحد المحترفين، لكنه يحتاج إلى اكتساب مهارات متقدمة في إدارة المشاريع خلال 3 أشهر. قرر استخدام المنصات الرقمية، مثل LinkedIn Learningللتدريب و Monday.com للتطبيق العملي في إدارة المشاريع.

- **نقاط التعلم الرئيسية:**

موازنة التعلم مع الوظيفة بدوام كامل:

- تعلم كيفية إدارة الوقت بفعالية من خلال تخصيص ساعات محددة للتطوير المهني كل أسبوع.
- استخدم أدوات الإنتاجية (مثل Google Calendarو Todoist)لتحديد أولويات التعلم دون التأثير على أداء العمل.

استخدام منصات التعلم المهيكلة:

- استفد من الدورات التدريبية المنظمة جيدًا عبر الإنترنت التي تقسم المواضيع المعقدة إلى دروس قابلة للإدارة.
- تقدم منصات مثل LinkedIn Learning شهادات وتتبع التقدم، مما يجعل التعلم أكثر تنظيمًا وقابلية للقياس .

تجاوز التحديات:

- **إدارة الوقت:** طور جدولاً يوازن بين مسؤوليات العمل والتعلم. حدد أهدافًا يومية أو أسبوعية واقعية لتتبع التقدم.
- **نقص التحفيز:** ابقَ متحفزًا من خلال مكافأة التقدم، والانضمام إلى مجموعات تعلم الأقران، أو العثور على شريك للمساءلة للبقاء على المسار الصحيح.

النتيجة:

- بنهاية الثلاثة أشهر، يكتسب المحترف المهارات اللازمة بنجاح، ويكمل الشهادات، ويشعر بالثقة في التعامل مع مسؤوليات إدارة المشاريع الجديدة. يظهر كيف يمكن لتعزيز المهارات الرقمية تسريع نمو المهنة مع الحفاظ على الالتزامات الوظيفية بدوام كامل.

ملخص المراجعة

عادة تلخيص النقاط الرئيسية

مقدمة في آداب الإنترنت (النتيكت):

- تعريف آداب الإنترنت: يتطلب التواصل الرقمي استخدام لغة محترمة، والاعتراف بالآخرين، وتجنب سلوكيات مثل استخدام الأحرف الكبيرة (الصراخ) أو الهجمات الشخصية.
- المبادئ الأساسية: الحفاظ على الاحترافية ، ومنح الفضل المناسب، واستخدام النغمة المناسبة.

آداب الإنترنت في البيئات المهنية:

- **الحفاظ على الاحترافية:** تأكد من وضوح الرسائل والبريد الإلكتروني، واستخدم تحيات وتوقيعات رسمية، وتجنب اللغة العاطفية أو غير المناسبة.
- **تمرين جماعي:** تعلم المشاركون كيفية تحسين التواصل من خلال تحديد وتصحيح رسائل البريد الإلكتروني المهنية المكتوبة بشكل سيئ.

السلامة الرقمية والمخاطر:

- **تحديد التهديدات عبر الإنترنت:** تشمل التهديدات الرقمية الرئيسية التصيد الاحتيالي، والبرامج الضارة، وسرقة الهوية. الوعي بهذه المخاطر أمر حاسم لحماية البيانات الشخصية وبيانات المؤسسات.
- **حماية الهوية الرقمية:** تشمل أفضل الممارسات استخدام كلمات مرور قوية، وتمكين المصادقة الثنائية، والتوخي الحذر عند استخدام شبكة الواي فاي العامة.

التكيف مع بيئات التعلم الرقمية:

- **استراتيجيات التعلم الشخصية:** قام المشاركون بإنشاء استراتيجيات التعلم الرقمية الخاصة بهم، مختارين أدوات مثل LinkedIn Learningأو Courseraلتطوير المهارات.
- **التطبيق العملي:** عملت المجموعات على سيناريوهات حقيقية، محددة التحديات والحلول للتكيف مع الأدوات الرقمية الجديدة في بيئات العمل.

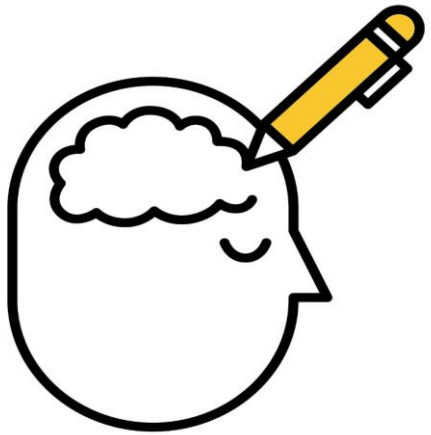
EMSA

ملخص المراجعة والأسئلة والأجوبة

✓**السلامة الرقمية وآداب الإنترنت:**

- ✓ **آداب الإنترنت:** التصرف بشكل محترم ومهني في الاتصالات الرقمية.
- ✓ **المخاطر الرقمية:** حماية الهوية عبر الإنترنت، التعرف على التهديدات، وإدارة السلامة الرقمية.
- ✓ **التكيف مع بيئات التعلم الرقمية:** استراتيجيات للتعلم بكفاءة وتطبيق الأدوات الرقمية الجديدة في مكان العمل.

هل لديك اسئلة ؟



ماذا ستحتفظ به من تدريب اليوم؟

EMSA

التدريب

التقييم

المراجع والمصادر:

Engagement with Digital Technologies

11. **Turkle, S.** (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books.
    Available at: Amazon Link

12. **Baym, N. K.** (2015). *Personal Connections in the Digital Age*. Polity Press.
    Available at: Amazon Link

13. **Cialdini, R. B.** (2006). *Influence: The Psychology of Persuasion*. Harper Business.
    Available at: Amazon Link

14. **Howard, P. N., & Hussain, M. M.** (2013). *Democracy's Fourth Wave? Digital Media and the Arab Spring*. Oxford University Press.
    Available at: Oxford University Press

15. **Rheingold, H.** (2012). *Net Smart: How to Thrive Online*. MIT Press.
    Available at: MIT Press

Digital Safety and GDPR Compliance

16. **Schneier, B.** (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.
    Available at: Amazon Link

17. **GDPR.eu** (2020). *General Data Protection Regulation: A Detailed Overview*.
    Available at: GDPR.eu

18. **Cavoukian, A.** (2009). *Privacy by Design: The 7 Foundational Principles*.
    Available at: Information and Privacy Commissioner of Ontario

19. **Singer, P. W., & Friedman, A.** (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
    Available at: Oxford University Press

20. **Westby, J.** (2017). *Cybersecurity & Privacy Best Practices for Small to Medium Enterprises*. American Bar Association.
    Available at: Amazon Link

قائمة الموارد المقترحة للتعلم الذاتي

3. Engagement with Digital Technologies

- **"Digital Minimalism: Choosing a Focused Life in a Noisy World"** – Cal Newport
  Available at: Amazon Link
- **"Netiquette"** – Virginia Shea
  Available at: Amazon Link
- **Dropbox**: *Collaborating with Dropbox for Teams*
  Available at: Dropbox
- **TED Talks**: *The Dark Side of Technology*
  Available at: TED.com
- **LinkedIn Learning**: *Developing Digital Competence*
  Available at: LinkedIn Learning

4. Digital Safety and GDPR

- **"Cybersecurity and Cyberwar: What Everyone Needs to Know"** – P.W. Singer
  Available at: Amazon Link
- **"The GDPR Handbook"** – E. Corynne McSherry
  Available at: Amazon Link
- **GDPR.eu**: *GDPR Training Materials*
  Available at: GDPR.eu
- **"Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World"** – Bruce Schneier
  Available at: Amazon Link
- **Cyber Awareness Learning Hub**
  Available at: Cyber Awareness

Entrepreneurial Mindset and Key Skills for All

شكراً.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.