



Jordan Youth Innovation Forum
الملتقى الأردني للإبداع الشبابي



3. الرقمنة

3.1 المبادئ العامة، والآليات، والمنطق الأساسي وراء تطور التقنيات الرقمية.

الملتقى الأردني للإبداع الشبابي.
المدة : 6.5 ساعة.



Co-funded by
the European Union

بتمويل من الاتحاد الأوروبي. مع ذلك، فإن الآراء والوجهات النظر الواردة هنا هي آراء المؤلفين فقط، ولا تعكس بالضرورة آراء الاتحاد الأوروبي أو الوكالة التنفيذية الأوروبية للتعليم والثقافة (EACEA). ولا يتحمل الاتحاد الأوروبي ولا الوكالة التنفيذية الأوروبية للتعليم والثقافة أي مسؤولية عنها..

MMC Mediterranean
Management Centre

المنظم



الشركاء



Jordan Youth Innovation Forum
الملتقى الأردني للإبداع الشبابي

تفاصيل المشروع

العنوان : " التطوير المشترك، والتجريب، و التحقق من مناهج التدريب والمواد التدريبية لتنمية العقلية الريادية والمهارات الأساسية في الدول الثالثة "

الاختصار : EMSA (العقلية الريادية والمهارات للجميع)

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

البرنامج : إيراسموس+ لبناء القدرات في مجال التعليم والتدريب المهني (VET)

دعوة لتقديم المقترحات : ERASMUS-EDU-2022-CB-VET

تاريخ البدء: 01.01.2023

تاريخ الانتهاء: 31.12.2025

المبادئ العامة والآليات والمنطق الأساسي وراء تطور التقنيات الرقمية الهدف من التدريب



يهدف هذا التدريب إلى تزويد المشاركين بفهم واضح للتقنيات الرقمية وكيفية عملها. من خلال الأنشطة العملية ودراسات الحالة، سيتعلمون تطبيق المبادئ الرقمية والبقاء على اطلاع على الاتجاهات الناشئة. بنهاية التدريب، سيكون المشاركون قادرين على استخدام الأدوات الرقمية بثقة واتخاذ قرارات مدروسة لتنفيذ الحلول الرقمية في مشاريعهم.

من حيث المعرفة:

- تعريف الرقمنة وتحديد التقنيات الرقمية المتطورة.

من حيث المهارات:

- تحليل وتطبيق تقنيات إدارة المعلومات الرقمية لاسترجاع البيانات من مصادر موثوقة.

- إظهار الفهم من خلال الالتزام بالمبادئ العامة والآليات الخاصة بالتقنيات الرقمية.

- تقييم واحترام المنطق الكامن وراء تقييم التقنيات الرقمية.

من حيث المواقف:

- احترام اللائحة العامة لحماية البيانات (GDPR) ومعايير

- حماية البيانات والأخلاقيات عند استخدام التقنيات الرقمية.

- إظهار الثقة في ممارسة آداب السلوك الرقمي أثناء

- التفاعلات الرقمية.

- تطبيق استراتيجيات لحماية النفس والآخرين من التهديدات

- والمخاطر الإلكترونية.

المبادئ العامة والآليات الخاصة بالتقنيات
الرقمية الناشئة

نتائج التعلم

ERF: The European Reference Framework (Key Competences for Lifelong Learning)

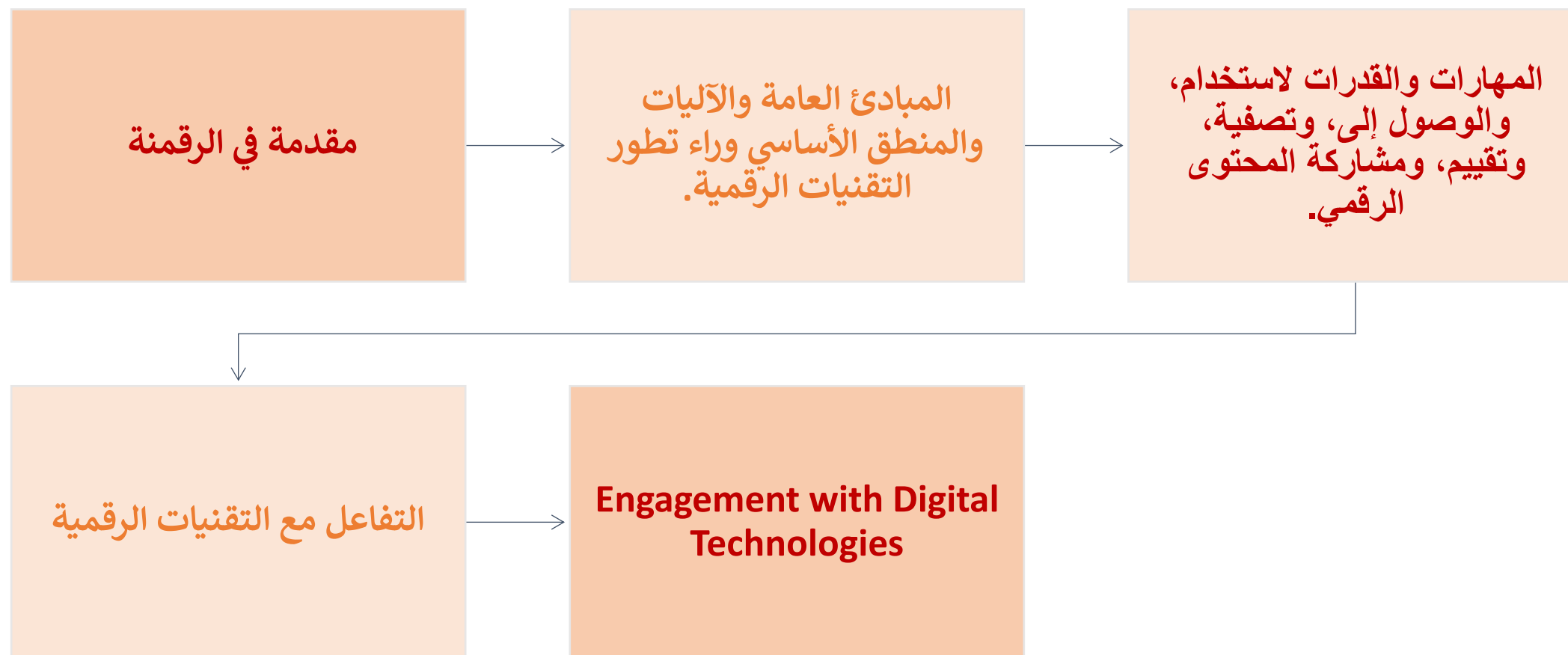


الكفاءة الرقمية هي القدرة على استخدام التقنيات الرقمية بثقة ومسؤولية في السياقات الشخصية والمهنية. سيغطي هذا البرنامج التدريبي هذا المبدأ وآليات الرقمنة، مع التركيز على حماية البيانات والامتثال للائحة العامة لحماية البيانات GDPR.

سيستكشف المشاركون المشهد الرقمي المتطور ويتعلمون تطبيق مهارات إدارة البيانات لضمان السلامة والدقة والاستخدام الأخلاقي.

**ما هي الكفاءة في الإطار الأوروبي
المرجعي التي يتناولها تدريبنا؟**

خريطة مسار التدريب

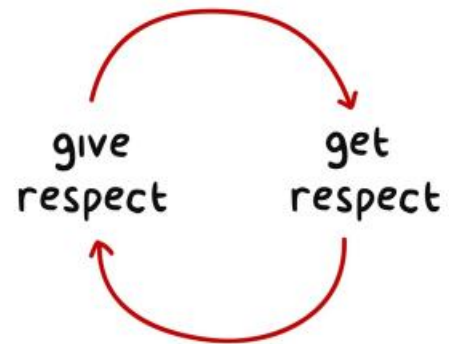
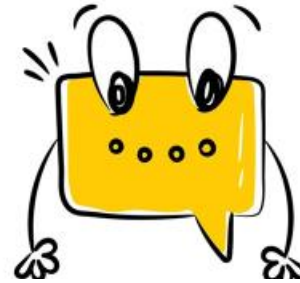


الكفاءة الرقمية

تشير الكفاءة الرقمية إلى القدرة على استخدام التقنيات الرقمية بثقة ومسؤولية في السياقات الشخصية والمهنية. يركز هذا البرنامج على آليات ومبادئ الرقمنة، بما في ذلك حماية البيانات والامتثال لـ **GDPR**. سيستكشف المشاركون التطور المستمر للتقنيات الرقمية وسيتعلمون كيفية تطبيق مهارات إدارة البيانات لضمان الأمان، الدقة، والاستخدام الأخلاقي في عالم اليوم المتصل رقميًا.

ما هي الكفاءة في الإطار الأوروبي
المرجعي ERF التي يغطيها تدريبنا؟

Training Rules

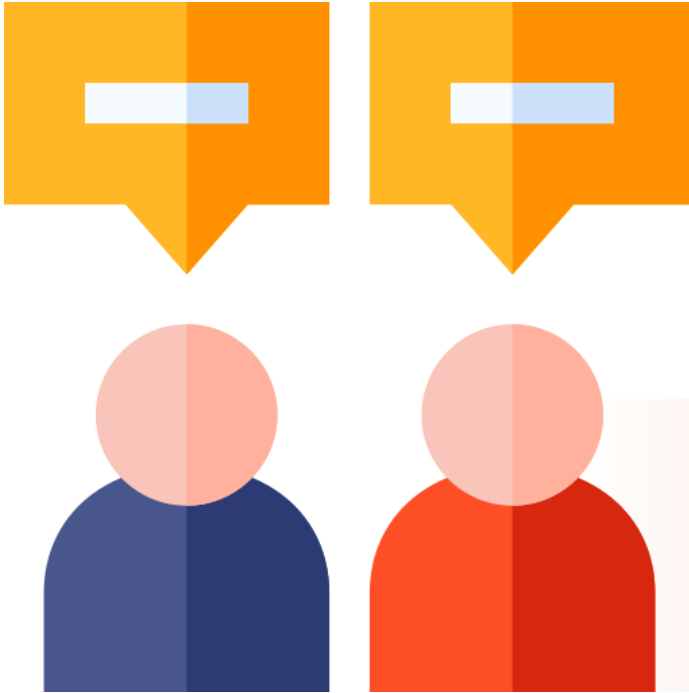


BREAK TIME



MT3.1_6

البحث عن الكنز



المقدمة

لنتعرف على بعضنا البعض!

اقتباس عن الكفاءة
"التكنولوجيا تكون في أفضل حالاتها عندما تجمع الناس معًا." — مات مولينوغيغ،
مؤسس ووردبريس

مقدمة في الرقمنة:

مقدمة في الرقمنة

• تعريف الرقمنة:

تشير الرقمنة إلى دمج التقنيات الرقمية في العمليات والأنشطة اليومية، مما يُحدث تحولاً في طريقة عمل الشركات، الحكومات، والأفراد. وتتضمن تحويل المعلومات إلى صيغة رقمية، وتحسين سير العمل، وتسهيل طرق جديدة للتواصل وتقديم الخدمات. تتجاوز الرقمنة مجرد تحويل البيانات إلى شكل رقمي، إذ تعيد تشكيل نماذج الأعمال بالكامل، والقطاعات الاقتصادية، والوظائف المجتمعية، من خلال تسخير التقنيات الرقمية لخلق القيمة، وزيادة الكفاءة، وتحسين التجارب.



- **الجوانب الرئيسية:**
- **الأتمتة:** استبدال المهام اليدوية بالعمليات الرقمية المؤتمتة، مما يُحسن السرعة ويقلل من الأخطاء البشرية.
- **الاعتماد على البيانات:** الاستفادة من البيانات الرقمية لاتخاذ قرارات مستنيرة، وتحليل الاتجاهات، والتنبؤ بالنتائج المستقبلية.
- **الاتصال:** تعزيز التواصل عبر الشبكات والإنترنت، مما يتيح التعاون الفوري عبر الحدود الجغرافية.
- **الابتكار:** تمكّن الرقمنة من تطوير منتجات وخدمات وصناعات جديدة من خلال الاستفادة من التقدم التكنولوجي.
- **أمثلة:**
- **الرعاية الصحية:** استخدام السجلات الرقمية للمرضى، الطب عن بُعد، والتشخيص القائم على الذكاء الاصطناعي.
- **التجزئة:** منصات التجارة الإلكترونية التي تغير طريقة تسوق العملاء وتفاعلهم مع العلامات التجارية.
- **التعليم:** منصات التعلم عبر الإنترنت التي توفر الوصول إلى التعليم للطلاب في جميع أنحاء العالم.

الموضوع 3: التفاعل مع التقنيات الرقمية

Topic 3 Route Map



"الإنترنت هو أول شيء تبنيه البشرية ولا تفهمه، وهو أكبر تجربة في الفوضوية شهدناها على الإطلاق."
— إريك شميدت، الرئيس التنفيذي السابق لشركة جوجل

مقدمة في آداب السلوك الرقمي (Netiquette)

• **تعريف آداب السلوك الرقمي Netiquette** : هو مجموعة من القواعد والسلوكيات المتوقعة لضمان تواصل محترم في البيئة الرقمية.

• **أهمية :**

مع تزايد التواصل الرقمي، يصبح الالتزام بالتفاعل المهني والمحترم أمرًا أساسيًا لبناء علاقات إيجابية ومجتمعات رقمية سليمة.

• **لغة محترمة ونبرة مناسبة:**

1. تواصل دائمًا بأسلوب يحترم الآخرين، وتجنب استخدام لغة مسيئة أو غير لائقة.

2. تذكر أن النص المكتوب يفقر إلى نبرة الصوت، لذا قد يبدو محايدًا لك لكنه قد يُفسر على أنه غير لائق للآخرين.

• **تجنب الكتابة بالأحرف الكبيرة بالكامل حيث انها تعني (الصراخ)**

• **الإشارة إلى عمل الآخرين بالشكل الصحيح:**

قم دائمًا بنسبة المحتوى إلى صاحبه الأصلي (الأفكار، الاقتباسات، الموارد) لتجنب السرقة الأدبية واحترام حقوق الملكية الفكرية.

• **الامتناع عن الهجمات الشخصية أو "Flaming"**

تجنب التعليقات العدوانية أو المسيئة المعروفة باسم **Flaming**، حيث تؤدي الهجمات الشخصية إلى بيئة سلبية وتعيق التواصل الفعال.



آداب السلوك الرقمي: ما يجب فعله وما يجب تجنبه

-  ما يجب فعله: كن مهذبًا، تحقق من صحة المعلومات، وابقَ في صلب الموضوع.
-  ما يجب تجنبه: لا تنشر محتوى تحريضيًا، لا ترسل رسائل غير مرغوبة (Spam)، ولا تحتكر النقاشات.
-  استخدم الرموز التعبيرية والفكاهة بشكل مناسب، مع تذكر أن النبرة قد يساء فهمها.



أمثلة على السلوك الرقمي الجيد والسيئ

- أمثلة إيجابية (السلوك الرقمي الجيد)

- استخدام لغة محترمة

مثال:

"شكرًا على ملاحظتك، سأضع اقتراحاتك في الاعتبار للمشروع القادم!"

التفسير: يُظهر هذا الرد الاحترام والانفتاح على الآراء، ويشجع على تقديم ملاحظات بناءة لتعزيز التواصل الإيجابي.

- الإشارة إلى عمل الآخرين

مثال:

"كما ذكر [الاسم] في تقريره، يجب أن نركز على..."

التفسير: إعطاء الفضل لأصحاب العمل يعبر عن احترام مساهماتهم ويضمن الاعتراف بحقوق الملكية الفكرية.

- استخدام التنسيق المناسب (تجنب الأحرف الكبيرة بالكامل)

مثال:

"يرجى مراجعة المستند المرفق وإعلامي بآرائك."

التفسير: استخدام القواعد النحوية الصحيحة وعلامات الترقيم وتنسيق النص بشكل مناسب (دون الحروف الكبيرة بالكامل) يجعل الرسالة أكثر احترافية ووضوحًا.

أمثلة على السلوك الرقمي الجيد والسيئ

- أمثلة سلبية (السلوك الرقمي السيئ)

- استخدام لغة عدوانية

مثال:

"أنت مخطئ! هذا لا معنى له، ومن الواضح أنك لم تفكر في الأمر جيدًا."

التفسير: هذا النوع من الردود يبدو عدائيًا ومتجاهلاً لآراء الآخرين، مما قد يؤدي إلى تصعيد النزاعات وإفساد العلاقات.

- عدم إعطاء الفضل للآخرين

مثال:

"أعتقد أننا يجب أن نركز على..." (فكرة مأخوذة من شخص آخر دون الإشارة إليه).

التفسير: عدم الاعتراف بعمل الآخرين أو أفكارهم قد يُعتبر سرقة فكرية أو عدم احترام، خاصة في البيئات المهنية أو الأكاديمية.

- الصراخ (استخدام الأحرف الكبيرة بالكامل)

مثال:

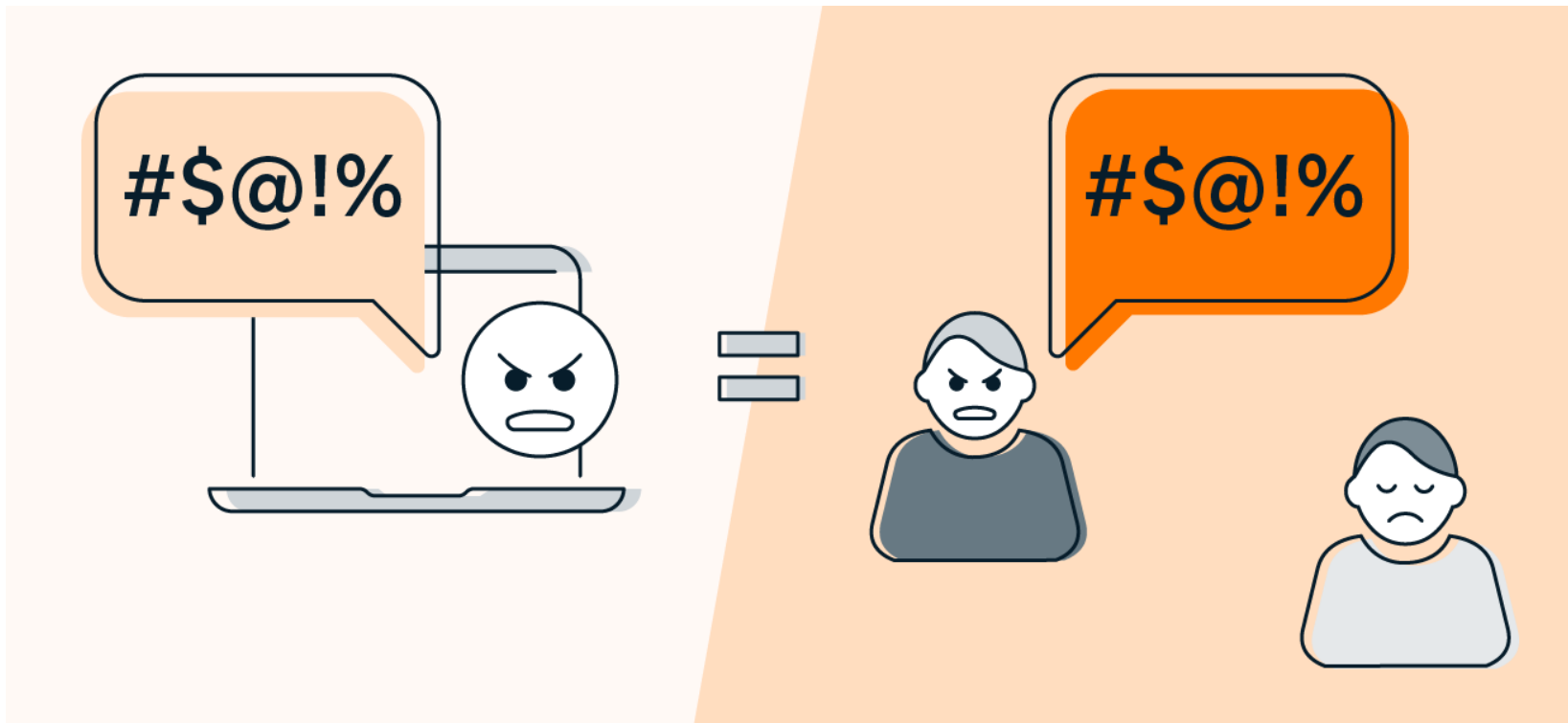
"يرجى إرسال التقرير بحلول الساعة 5 مساءً اليوم!"

التفسير: استخدام الأحرف الكبيرة بالكامل في التواصل المكتوب يُفسّر على أنه صراخ أو عدوانية، مما قد يؤدي إلى سوء فهم أو نبرة سلبية في المحادثة.

التفكير في سيناريوهات السلوك الرقمي السيئ



MT3.3_1



الموضوع 3.1: آداب السلوك الرقمي في البيئات المهنية

ما هي الاحترافية في البيئات الرقمية؟

الاحترافية هي مجموعة من السلوكيات وتقنيات التواصل المتوقعة في بيئة عمل. تشمل الاحترافية عبر الإنترنت:

1. استخدام لغة رسمية
2. الالتزام بسياسات الشركة
3. الحفاظ على تواصل واضح ومحترم



الموضوع 3.1: آداب السلوك الرقمي في البيئات المهنية



- المبادئ الأساسية للتواصل المهني عبر الإنترنت
- ☒ استخدام تحية وختام مناسبين:
ابدأ بتحية رسمية واختتم برسالة ودية.
مثال: "السيدة سميث العزيزة" أو "مع أطيب التحيات، [اسمك]."
- ☒ الوضوح والاختصار:
تواصل بكفاءة وتجنب الغموض.
مثال: "يرجى إتمام المهمة المرفقة بحلول يوم الجمعة."
- ☒ احترام الوقت والحدود:
أرسل الرسائل خلال ساعات العمل المناسبة.
- ☒ معالجة سوء الفهم باحترافية:
تعامل مع النزاعات بهدوء وبأسلوب بناء.

مثال على سوء التواصل المهني

"مرحبًا أيها الفريق! عاجل! أحتاج هذا الآن!"

"هل يمكنك القيام بهذا بأسرع وقت ممكن؟ لا يهمني كيف، فقط أنجزه."

مثال على التواصل المهني السليم

"فريق العمل العزيز،

آمل أن تكونوا بخير. هل يمكنكم إتمام المهمة المرفقة بحلول نهاية اليوم؟ أخبروني إذا كنتم بحاجة إلى أي مساعدة.

أطيب التحيات،
[اسمك].

تحسين رسائل البريد الإلكتروني المهنية



MT3.3_2



التحديات في التواصل الرقمي المهني

سوء تفسير النبذة

- **التحدي:** يفتقر التواصل النصي إلى الإشارات الصوتية، مما يجعل من الصعب إيصال النبذة بدقة. قد يُفسر النص المحايد على أنه قاسٍ أو غير ودي.
- ✓ **الحل:** استخدم لغة واضحة وموجزة. تجنب السخرية أو العبارات غير الرسمية بشكل مفرط. أضف عبارات توضيحية أو، عند الحاجة، رموزًا تعبيرية لإظهار النية.

● حدود العمل والحياة الشخصية

- **التحدي:** مع الأدوات الرقمية مثل البريد الإلكتروني وتطبيقات المراسلة، يُتوقع دائمًا أن يكون الموظفون متاحين، مما يطمس الفاصل بين العمل والحياة الشخصية.
- ✓ **الحل:** ضع حدودًا واضحة لمواعيد العمل. أخبر فريقك بساعات عملك، واستخدم ميزات مثل "عدم الإزعاج" لحماية وقتك الشخصي.

التحديات في التواصل الرقمي المهني

• غياب الإشارات البصرية أو الصوتية

التحدي: في التواصل الرقمي، لا توجد لغة جسد أو تعابير وجه أو نبرة صوت، مما قد يؤدي إلى سوء الفهم أو عدم الوضوح.

الحل: استخدم مؤتمرات الفيديو للنقاشات المعقدة، أو الرسائل الصوتية عند الحاجة. في التواصل الكتابي، كن محددًا قدر الإمكان لتجنب سوء التفسير.

• الإفراط في استخدام اللغة غير الرسمية

التحدي: يؤدي التواصل الرقمي، خاصة عبر الرسائل الفورية، إلى استخدام لغة غير رسمية قد لا تكون مناسبة في البيئات المهنية.

الحل: قيّم السياق والجمهور دائمًا. استخدم لغة مهنية عند التواصل مع العملاء أو في المناقشات الرسمية، واضبط مستوى الرسمية حسب الموقف.

نصائح لآداب البريد الإلكتروني



الموضوع 3.2: الأمان الرقمي والمخاطر

ما هو الأمان الرقمي؟

يشير الأمان الرقمي إلى الممارسات التي تحمي المستخدمين من المخاطر والأضرار عند التفاعل في البيئات الرقمية.

المجالات الرئيسية:

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



الموضوع 3.2: الأمان الرقمي والمخاطر

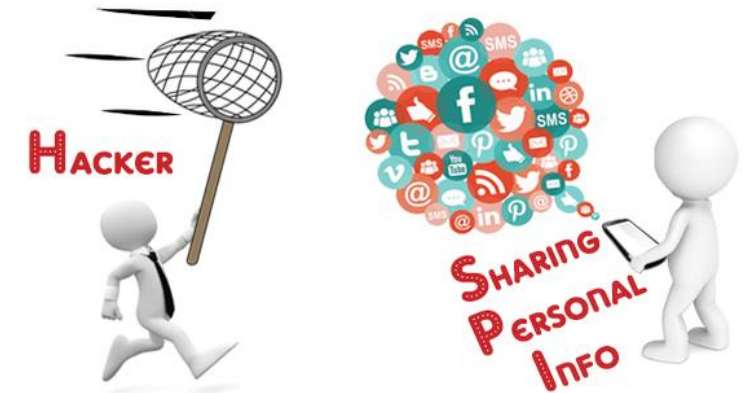
المخاطر الشائعة عبر الإنترنت:

- **التصيد الاحتيالي (Phishing)**: محاولات احتيالية للحصول على معلومات حساسة عبر التظاهر بكيان موثوق.
- **البرمجيات الضارة (Malware)**: برامج خبيثة مصممة لإلحاق الضرر بالأجهزة الرقمية أو استغلالها.
- **سرقة الهوية (Identity Theft)**: الاستحواذ الاحتيالي على المعلومات الشخصية واستخدامها لتحقيق مكاسب مالهية.
- **اختراق البيانات (Data Breaches)**: الوصول غير المصرح به إلى معلومات شخصية أو حساسة 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 عبر طلب شكل ثانٍ من التحقق.
- التصفح الآمن: التأكد من أن المواقع آمنة (HTTPS) قبل إدخال المعلومات الشخصية.
- تجنب مشاركة المعلومات الشخصية: الحد من مشاركة التفاصيل الخاصة على وسائل التواصل الاجتماعي أو المواقع غير المؤمنة.



التحديات الرقمية وكيفية التعامل معها

- هجمات التصيد الاحتيالي Phishing

- التعريف:

محاولات احتيالية للحصول على معلومات حساسة (مثل كلمات المرور، أرقام بطاقات الائتمان) عن طريق التظاهر بكيان موثوق عبر البريد الإلكتروني أو الهاتف أو الرسائل النصية.

- كيفية التعامل مع التصيد الاحتيالي:

- لا تنقر على الروابط في الرسائل الإلكترونية غير المرغوب فيها.
- تحقق من هوية المرسل عن طريق التواصل المباشر مع الشركة عبر القنوات الرسمية.
- قم بالإبلاغ عن محاولات التصيد الاحتيالي لمزود البريد الإلكتروني أو قسم تكنولوجيا المعلومات.

التحديات الرقمية وكيفية التعامل معها

- البرمجيات الضارة - **Malware** الفيروسات، أحصنة طروادة، الفدية **Ransomware**
- **التعريف:**
برامج خبيثة مصممة لإلحاق الضرر أو استغلال الأجهزة أو الشبكات أو البيانات.
- **كيفية التعامل مع البرمجيات الضارة:**
- قم بتنشيط وتحديث برامج مكافحة الفيروسات والبرمجيات الخبيثة بانتظام.
- تجنب تنزيل المرفقات من مصادر غير معروفة.
- احتفظ بنسخ احتياطية للبيانات الهامة بانتظام في حالة حدوث هجمات فدية أو هجمات أخرى قد تعرض البيانات للخطر.

التحديات الرقمية وكيفية التعامل معها

- تعريف سرقة الهوية:
استخدام هوية شخص آخر بشكل احتيالي، عادةً من أجل الحصول على مكاسب مالية.
- كيفية التعامل مع سرقة الهوية:
 1. استخدم كلمات مرور قوية وفريدة، وفعل المصادقة الثنائية.
 2. كن حذرًا عند مشاركة معلوماتك الشخصية عبر الإنترنت.
 3. راقب حساباتك المالية بانتظام للتحقق من أي نشاط مشبوه.

التحديات الرقمية وكيفية التعامل معها

• 4. اختراق البيانات (Data Breaches)

• التعريف:

الوصول غير المصرح به إلى معلومات شخصية أو حساسة، وغالبًا ما يحدث من خلال الاختراقات.

• كيفية التعامل مع اختراق البيانات:

• غير كلمات المرور فورًا بعد اكتشاف الاختراق.

• راقب الحسابات لأي إشارات على سوء الاستخدام أو الاحتيال.

• فعل التنبيهات لأي نشاط غير معتاد على الحساب واستخدم التشفير للبيانات الحساسة.

التحديات الرقمية وكيفية التعامل معها

• 5. هجمات الهندسة الاجتماعية (Social Engineering Attacks)

• التعريف:

التلاعب بالأشخاص لجعلهم يكشفون معلومات سرية عبر الخداع (مثل التظاهر بكونك زميلًا).

• كيفية التعامل مع هجمات الهندسة الاجتماعية:

• كن حذرًا من الطلبات غير المرغوب فيها للحصول على معلومات حساسة، حتى من الأشخاص المألوفين.

• تحقق من هوية الشخص عبر قنوات تواصل ثانوية (مثل الاتصال بالشخص مباشرة).

• تدريب الموظفين على التعرف على تقنيات الهندسة الاجتماعية.

الاستجابة للتهديدات الرقمية



MT3.3_4



سرقة الهوية الرقمية



الموضوع 3.3: التكيف مع بيئات التعلم الرقمية



- ما هو التعلم الرقمي؟
- التعلم الرقمي هو عملية اكتساب المهارات أو المعرفة باستخدام الأدوات والمنصات الرقمية.
- أمثلة:
- **التعلم في مكان العمل:** استخدام منصات مثل **LinkedIn Learning** أو **Coursera** لتطوير مهارات مرتبطة بالوظيفة.
- **التطوير الشخصي:** تطبيقات مثل **Duolingo** لتعلم اللغات أو **Headspace** لتحسين الرفاهية.
- **حل المشكلات اليومية:** دروس على **YouTube** أو المنتديات عبر الإنترنت لتعلم مهارات جديدة أو حل المشكلات.

الموضوع 3.3: التكيف مع بيئات التعلم الرقمية

لماذا يعتبر التعلم الرقمي مهمًا؟

- المرونة: يمكنك التعلم وفقًا لسرعتك الخاصة، في أي وقت وأي مكان.
- الوصولية: تتيح الأدوات الرقمية التعلم للجميع حول العالم.
- التكلفة الفعالة: توفر العديد من المنصات خيارات تعلم مجانية أو بأسعار معقولة.
- التعلم الذاتي: يمكنك تخصيص تعلمك وفقًا لاحتياجاتك وأهدافك.
- التعلم أثناء التنقل: الوصول إلى المحتوى عبر أجهزة متعددة، مما يسهل دمجه في روتينك اليومي.
- البقاء تنافسيًا: التكيف مع التقدم التكنولوجي والبقاء ذا صلة في مجالك.



التحديات الشائعة في التعلم الرقمي للحياة والعمل



1. التحميل الزائد للمعلومات :

- هنالك كمية هائلة من الموارد عبر الإنترنت، مما يجعل من الصعب تحديد مكان التركيز.

2. الإرهاق الرقمي :

- الاعتماد المفرط على الشاشات يمكن أن يؤدي إلى الإرهاق وفقدان الدافع.

3. الانضباط الذاتي:

- يتطلب التعلم الرقمي مستويات عالية من التحفيز الذاتي وإدارة الوقت، خاصة في البيئات غير الرسمية (مثل المشاريع العملية أو الأهداف الشخصية).

4. الفجوات التكنولوجية :

- صعوبة في استخدام بعض المنصات أو نقص في معرفة المعارف الرقمية.

استراتيجيات للتعلم الرقمي الفعال في العمل والحياة

1. تحديد أهداف واضحة:

- حدد ما ترغب في تعلمه وأنشئ أهدافاً قابلة للقياس (مثل تعلم مهارة جديدة لمشروع عمل أو تحسين عادات الإنتاجية).

2. استخدام الأدوات المناسبة:

- اختر الأدوات أو المنصات الأنسب لأهدافك التعليمية

الأمثلة:

- لإدارة المشاريع، استخدم **Trello** أو **Monday.com**.
- للتطوير الشخصي، استخدم تطبيقات مثل **Headspace** أو **Coursera**.

3. إدارة الوقت: خصص وقتاً في جدولك للتعلم لذاتي والممارسة.

- ## 4. الانخراط في المجتمع :
- انضم إلى المنتديات الإلكترونية، الندوات عبر الإنترنت، أو مجموعات الأقران لمشاركة رحلتك التعليمية والحصول على الدعم



تطوير خطة تعلم رقمية شخصية



MT3.3_6



لأدوات الرقمية للتعلم المهني والحياة

في العمل:

- إدارة المشاريع : Asana. 'Monday.com 'Trello
- اجتماعات الفيديو: 'Zoom Microsoft Teams.
- التدريب والتطوير: 'LinkedIn Learning Coursera



للنمو الشخصي:

- إدارة 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 Todois
- أدوات التنظيم: 'Evernote Notion.



تكييف الاستراتيجيات الرقمية مع سيناريوهات مكان العمل



MT3.3_7



دراسة حالة – تحسين المهارات الرقمية للترقية الوظيفية

• السيناريو:

تم عرض ترقية علي محترف، ولكنه يحتاج إلى اكتساب مهارات متقدمة في إدارة المشاريع خلال 3 أشهر. قرر أن يستخدم منصات رقمية مثل LinkedIn Learning للتدريب و Monday.com للتطبيق العملي في إدارة المشاريع.

• النقاط الرئيسية للتعلم:

1. موازنة التعلم مع العمل بدوام كامل:

2. تعلم كيفية إدارة الوقت بفعالية عن طريق تخصيص ساعات محددة أسبوعياً للتطوير المهني.

3. استخدام أدوات الإنتاجية مثل Google Calendar و Todo List لترتيب الأولويات في التعلم دون التأثير على أداء العمل.

• استخدام منصات التعلم المنظمة:

1. الاستفادة من الدورات التدريبية المنظمة عبر الإنترنت التي تقسم المواضيع المعقدة إلى دروس قابلة للإدارة.

2. منصات مثل LinkedIn Learning تقدم شهادات تتبع التقدم، مما يجعل التعلم أكثر تنظيماً وقابلية للقياس.

• تجاوز التحديات:

• إدارة الوقت: تطوير جدول زمني يوازن بين المسؤوليات الوظيفية والتعلم. تحديد أهداف يومية أو أسبوعية واقعية لتتبع التقدم.

• نقص الدافع: البقاء متحمساً عن طريق مكافأة التقدم، الانضمام إلى مجموعات تعلم جماعية، أو العثور على شريك مسؤول للبقاء على المسار الصحيح.

• النتيجة:

• بنهاية الثلاثة أشهر، اكتسب المحترف المهارات المطلوبة، أكمل الشهادات، وأصبح واثقاً من التعامل مع مسؤوليات إدارة المشاريع الجديدة. أظهر كيف يمكن أن يسرع تحسين المهارات الرقمية من نمو الوظيفة بينما يحافظ على التزامه بالعمل بدوام كامل

المراجعة - الملخص

مراجعة للنقاط الرئيسية:

مقدمة في اداب السلوك الرقمي :

- تعريف اداب السلوك الرقمي: يتطلب التواصل الرقمي استخدام لغة محترمة، والاعتراف بالآخرين، وتجنب التصرفات مثل استخدام الأحرف الكبيرة بالكامل (الصراخ) أو الهجمات الشخصية.
- المبادئ الأساسية: الحفاظ على الاحترافية، إعطاء الفضل الصحي، واستخدام النبرة المناسبة.

اداب السلوك الرقمي في البيئات المهنية:

- الحفاظ على الاحترافية:

1. ضمان وضوح الرسائل والبريد الإلكتروني.
2. استخدام التحيات الرسمية والتوقيعات المناسبة.
3. تجنب اللغة العاطفية أو غيراللائقة.

المراجعة – الملخص:

الأمان الرقمي والمخاطر:

- التعرف على التهديدات عبر الإنترنت:

- تشمل التهديدات الرقمية الرئيسية التصيد الاحتيالي، البرمجيات الضارة، وسرقة الهوية.

حماية الهوية الرقمية: تشمل أفضل الممارسات استخدام كلمات مرور قوية، تفعيل المصادقة الثنائية، والحذر عند استخدام الواي فاي العام.

التكيف مع بيئات التعلم الرقمية:

- استراتيجيات التعلم الشخصي

- التطبيق العملي



المراجعة - الملخص والأسئلة والأجوبة

✓الأمان الرقمي واداب السلوك الرقمي:

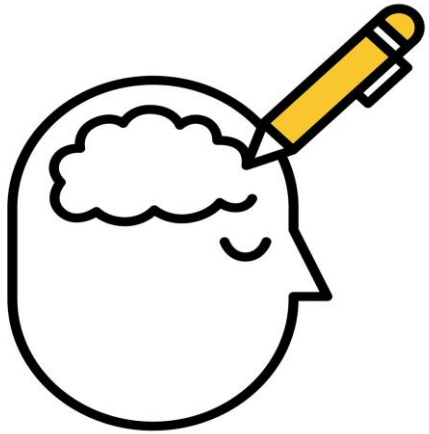
✓السلوك المحترم والمهنية في التواصل الرقمي

✓المخاطر الرقمية: حماية الهوية الرقمية، التعرف على التهديدات، وإدارة الأمان الرقمي.

✓التكيف مع بيئات التعلم الرقمية: استراتيجيات لتعلم وتطبيق الأدوات الرقمية الجديدة بكفاءة في بيئة العمل.



هل لديك أي أسئلة؟



ما الذي ستحتفظ به من تدريب اليوم؟

تقديم التدريب



لائحة المراجع

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 بالموارد 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

شكرا لكم!



**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.