المنهج

ICDL Arabia

# مقرر ICDL
# الأمن الرقمي

اصدار المنهاج ١,٠ (الجزء الأول)

**الهدف**

تقدم هذه الوثيقة تفاصيل المنهاج الخاص بمقرر الأمن الرقمي يصف المنهج من خلال مخرجات التعلم والمعرفة والمهارات التي يجب أن يمتلكها متدرب الأمن الرقمي يوفر المنهاج أيضاً أساسيات النظرية والاختبار القائم على الممارسة في هذا المقرر.

| الموضوع | المهارة | رقم المرجع | نقاط الموضوع |
|---|---|---|---|
| **١ مفاهيم الأمان** | ١,١ تهديدات البيانات | ١,١,١ | التفريق بين البيانات والمعلومات. |
| | | ١,١,٢ | فهم مصطلح ي جرائم الإنترنت والقرصنة. |
| | | ١,١,٣ | التعرف على البرامج الضارة والتهديدات العرضية التي تتعرض لها البيانات من قبل أفراد مقدمي الخدمة أو المنظمات الخارجية. |
| | | ١,١,٤ | التعرف على التهديدات التي تتعرض لها البيانات نتيجة ظروف استثنائية غير عادية، على سبيل المثال: الحريق والفياضات والحروب والزلازل. |
| | | ١,١,٥ | التعرف على التهديدات التي تتعرض لها البيانات نتيجة استخدام الحوسبة السحابية، علىسبيل المثال: التحكم في البيانات واحتمالية فقدان الخصوصية. |
| | ١,٢ قيمة البيانات | ١,٢,١ | إدراك الخصائص الأساسية لأمن المعلومات، على سبيل المثال: السرية والنزاهة والإتاحة. |
| | | ١,٢,٢ | إدراك أسباب حماية المعلومات الشخصية، على سبيل المثال: تجنب سرقة الهوية والاحتيال والحفاظ على الخصوصية. |
| | | ١,٢,٣ | إدراك أسباب حماية معلومات العمل المخزنة على أجهزة الكمبيوتر وغيرها من الأجهزة،على سبيل المثال: منع السرقة وعمليات الاحتيال وفقدان البيانات العرضي والأعمال التخريبية. |
| | | ١,٢,٤ | تعريف المبادئ العامة لحماية البيانات/ الخصوصية والحفظ والتحكم، على سبيل المثال: الشفافية والأغراض الشرعية والتناسب. |
| | | ١,٢,٥ | إدراك وفهم مصطلح ي أصحاب البيانات ومراقبي البيانات وكيفية تطبيق مبادئ حماية البيانات/الخصوصية والحفظ والتحكم عليهما. |
| | | ١,٢,٦ | إدراك أهمية الالتزام باتباع إرشادات استخدام الاتصالات وتكنولوجيا المعلومات(ICT) وسياساته وكيفية الوصول إليهما. |
| | ١.٣ الأمان الشخصي | ١.٣.١ | إدراك أن المعلومات الشخصية الموجودة على جهاز الحاسوب الخاص بك يجب أن يتم حمايتها. |
| | | ١.٣.٢ | فهم مصطلح سرقة الهوية والآثار المترتبة عليها وإدراكهما: الشخصية والمالية والقانونية والمتعلقة بالعمل. |
| | | ١.٣.٣ | تعرف على طرق سرقة الهوية، على سبيل المثال: الحصول على المعلومات من المواد التقنية المهملة والتزوير المالي والتحجج الاحتيالي. |
| | | ١.٣.٤ | إدراك مصطلح الهندسة الاجتماعية والآثار المترتبة عليه، على سبيل المثال: الوصول غير المصرح به لأجهزة الكمبيوتر وغيرها من الأجهزة وجمع المعلومات غير المصرح به والاحتيال. |
| | | ١.٣.٥ | التعرف على طرق الهندسة الاجتماعية، على سبيل المثال: المكالمات الهاتفية والتصيد الإلكتروني (Phishing) والتسلل من فوق الكتف (shoulder surfing) |
| | ١,٤ أمان الملفات | ١.٤.١ | إدراك تأثيرات تمكين/عدم تمكن الإعدادات الأمنية لملف الماكرو. |
| | | ١.٤.٢ | إدراك مزايا التشفير وحدود تقييده، وكن على دراية بأهمية وضرورة عدم الإفصاح عن كلمة مرور التشفير أو مفتاحه أو شهادته أو فقدانها. |
| | | ١.٤.٣ | تشفير ملف أو مجلد أو محرك أقراص. |
| | | ١.٤.٤ | تعين كلمة مرور للملفات، على سبيل المثال: المستندات وجداول البيانات والملفات المضغوطة. |
| **٢ – البرمجيات الخبيثة** | ٢,١ الأنواع والطرق | ٢.١.١ | إدراك مصطلح البرامج الخبيثة وفهمه، إلى جانب التعرف على مختلف الطرق التي يمكن استخدامها كوسيلة لإخفاء البرامج الضارة على أجهزة الكمبيوتر وغيرها من الأجهزة،على سبيل المثال: أحصنة طروادة والجذور الخفية( rootkits)والأبواب الخلفية ( backdoors). |
| | | ٢.١.٢ | التعرف على أنواع البرامج الخبيث المعدية وإدراك طريقة عملها: الفيروسات والديدان. |

| الموضوع | المهارة | رقم المرجع | نقاط الموضوع |
|---|---|---|---|
| | | ٢.١.٣ | التعرف على أنواع البرامج الخبيثة لسرقة البيانات مثل توليد الأرباح/الابتزاز، إلى جانب إدراك طريقة عملها: البرامج الإعلانية وبرامج الفدية وبرامج التجسس وشبكات البوتات وتسجيل ضربات المفاتيح والمسجلات والأجهزة القائمة بعملية الاتصال للربط على شبكة الإنترنت. |
| | ٢,٢ الحماية | ٢.٢.١ | إدراك طريقة عمل البرامج المضادة للفيروسات وحدود تقييدها. |
| | | ٢.٢.٢ | إدراك ضرورة تثبيت برنامج لمكافحة الفيروسات على أجهزة الكمبيوتر وغيرها من الأجهزة. |
| | | ٢.٢.٣ | إدراك أهمية تحديث البرامج بصورة منتظمة، على سبيل المثال: برامج مكافحة الفيروسات ومتصفح الويب والمكونات الإضافية والتطبيقات ونظام التشغيل. |
| | | ٢.٢.٤ | فحص محركات أقراص أو مجلدات أو ملفات معينة باستخدام برنامج مضاد للفيروسات، مع الحرص على جدولة عمليات الفحص باستخدام برنامج مضاد للفيروسات. |
| | | ٢.٢.٥ | إدراك المخاطر الناتجة عن استخدام البرامج القديمة وغير المدعومة، على سبيل المثال: المخاطر المتزايدة للبرامج الضارة وعدم التوافق. |
| | ٢,٣ حل المشكلة والتغلب عليها | ٢.٣.١ | فهم مصطلح فرض العزل والآثار المترتبة على الملفات الملوثة/المشبوهة |
| | | ٢.٣.٢ | عزل الملفات الملوثة / المشبوهة وحذفها |
| | | ٢.٣.٣ | إدراك إمكانية تشخيص هجمات البرامج الضارة واكتشافها والقضاء عليها باستخدام مصادر إلكترونية، على سبيل المثال: مواقع أنظمة التشغيل وبرامج مكافحة الفيروسات والشركات الموردة لبرامج متصفح الويب والمواقع الإلكترونية للأطراف المعنية. |
| **٣ - أمان الشبكة** | ٣,١ الشبكة والاتصال | ٣.١.١ | فهم مصطلح شبكة وإدراك أنواع الشبكات الشائعة مثل: الشبكة المحلية ( LAN )، الشبكة المحلية الواسعة ( WLAN )، الشبكات الواسعة ( WAN )، الشبكة الخاصة الافتراضية ( VPN). |
| | | ٣.١.٢ | فهم كيفية الاتصال بشبكة آمنة ضد: البرامج الضارة، الدخول غير المصرح به، الحفاظ على الخصوصية. |
| | | ٣.١.٣ | فهم دور مسؤول الشبكة في إدارة توثيق دفعات الحماية ذات الصلة وترخيصها وتقديرها ومراقبتها وتثبيتها بجانب تحديث مراقبة شبكة المرور والتعامل مع البرامج الضارة التي توجد داخل الشبكة. |
| | | ٣.١.٤ | فهم وظيفة جدار الحماية وحدود تقييده في بيئة العمل الشخصية. |
| | | ٣.١.٥ | تشغيل جدار حماية شخصي وإيقافه، تخصيص جهاز أو خادم/وظيفة ومنع الوصول إليهم من خال جدار الحماية الشخصي. |
| | ٣,٢ أمان الشبكة اللاسلكية | ٣.٢.١ | إدراك الخيارات المتعددة للأمن اللاسلكي وحدود تقيدها مثل: تكافئ السرية للشبكة السلكية ( WEP )، الوصول المحمي اللاسلكي ( WPA)، الوصول المحمي اللاسلكي (WPA2 ) رقم بطاقة الشبكة ( MAC ) اختفاء معرف ضبط الخادم SSID |
| | | ٣.٢.٢ | إدراك خطورة استخدام شبكة لاسلكية غير مؤمنة حيث يمكن أن تؤدي إلى: المتطفلين على الشبكة، مخترقي الشبكات. |
| | | ٣.٢.٣ | فهم مصطلح نقاط الاتصال الشخصية. |
| | | ٣.٢.٤ | تمكن وتعطيل نقاط اتصال شخصية مؤمنة وتوصيل الأجهزة وفصلها بشكل آمن. |
| **٤- التحكم في الوصول** | ٤,١ الوسائل | ٤.١.١ | تعريف إجراءات منع الوصول غير المصرح به إلى البيانات مثل: اسم المستخدم، كلمة المرور، رمز التعريف الشخصي، برامج التشفير، المصادقة المتعددة. |
| | | ٤.١.٢ | فهم مصطلح كلمة المرور لمرة واحدة واستخدامها بشكل نموذجي. |
| | | ٤.١.٣ | إدراك الغرض من إنشاء حساب على الشبكة. |

| الموضوع | المهارة | رقم المرجع | نقاط الموضوع |
|---|---|---|---|
| | | ٤.١.٤ | إدراك أهمية الوصول إلى الحساب على الشبكة من خال إدخال اسم المستخدم وكلمة المرور وضرورة قفل الحساب أو الخروج منه عندما لا يكون قيد الاستخدام. |
| | | ٤.١.٥ | تعريف تقنيات مقاييس الحماية الحيوية المستخدمة في التحكم بالوصول مثل: بصمة الإصبع، المسح الضوئي ببصمة العن، التعرف على الوجه، الهندسة اليدوية. |
| | ٤,٢ إدارة كلمات المـــــرور | ٤.٢.١ | إدراك سياسات كلمة المرور الجيدة، مثل: ملائمة طول كلمة المرور، ملائمة الحروف،المزيج الملائم من الحروف الخاصة والأرقام والأحرف الأبجدية، عدم مشاركة كلماتالمرور، تغيير كلمة المرور بشكل منتظم، استخدام كلمات مرور مختلفة للخدمات المختلفة. |
| | | ٤.٢.٢ | إدراك وظيفة وحدود تقييد برامج إدارة كلمة المرور. |
| ٥ - **الاستخدام الآمن لشبكة الإنترنت** | ٥,١ إعدادات المتصفح | ٥.١.١ | اختر إعدادات مناسبة لتمكن وعدم تمكن خاصية الإكمال التلقائي وعدم الحفظ عند إكمال نموذج. |
| | | ٥.١.٢ | حذف البيانات الشخصية من المتصفح مثل: سجل المتصفح، السجلات المحملة، ملفات الإنترنت المخزنة، كلمات المرور، ملفات التعريف، البيانات التي تم إكمالها بشكل تلقائي. |
| | ٥,٢ تأميـــن المتصفح | ٥.٢.١ | الانتباه إلى أهمية إجراء أي نشاط محدد عبر الإنترنت )الشراء، المعاملات المالية( منخال صفحات إنترنت آمنة باستخدام اتصال آمن بالإنترنت. |
| | | ٥.٢.٢ | تعريف طرق متعددة لتأكيد صحة موقع الإنترنت مثل: المحتويات عالية الجودة، العملات الأجنبية، عنوان URL حقيقي، المعلومات الخاصة بالشركة أو المالك، معلومات الاتصال،شهادة الأمان، التحقق من مالك المجال. |
| | | ٥.٢.٣ | فهم مصطلح الاحتيال الإلكتروني. |
| | | ٥.٢.٤ | إدراك وظيفة برامج التحكم في المحتوى وأنواعها مثل: برامج تصفية مواقع الإنترنت. |
| ٦ - **التواصل** | ٦,١ البريـــد الإلكتروني | ٦.١.١ | إدراك الهدف من تشفير رسائل البريد الإلكتروني أو فك تشفيرها. |
| | | ٦.١.٢ | فهم مصطلح التوقيع الرقمي. |
| | | ٦.١.٣ | التعرف على رسائل البريد الإلكتروني الاحتيالية وغير المرغوب فيها. |
| | | ٦.١.٤ | لتعرف على الخصائص الشائعة للتصيد الإلكتروني (phishing) مثل: استخدام أسماء المنظمات القانونية والأشخاص وروابط الويب المزيفة والشعارات والعلامات التجارية وتشجيع الكشف عن المعلومات الشخصية |
| | | ٦.١.٥ | الانتباه إلى إمكانية إبلاغ المؤسسات القانونية والجهات المعنية عن محاولات التصيد الإلكتروني. |
| | | ٦.١.٦ | إدراك خطر إصابة الكمبيوتر أو الجهاز بالبرامج الضارة عن طريق فتح مرفق البريد الالكتروني الذي يحتوي على ملف ماكرو أو ملف تنفيذي. |
| | ٦,٢ الشبكات الإجتماعية | ٦.٢.١ | إدراك أهمية تجنب الكشف عن المعلومات السرية أو الشخصية على الشبكات الاجتماعية. |
| | | ٦.٢.٢ | إدراك لضرورة ضبط إعدادات حساب موقع التواصل الاجتماعي ومراجعته بانتظام مثل:إعدادات الخصوصية الخاصة بالحساب والموقع الجغرافي. |
| | | ٦.٢.٣ | ضبط إعدادات حساب موقع التواصل الاجتماعي: إعدادات الخصوصية والموقع الجغرافي. |

| الموضوع | المهارة | رقم المرجع | نقاط الموضوع |
|---|---|---|---|
| | | ٦.٢.٤ | إدراك المخاطر المحتملة لاستخدام مواقع التواصل الاجتماعي مثل: التسلط عبر الإنترنت والاستمالة والكشف عن البيانات الشخصية والهويات الزائفة و الروابط الاحتيالية أو الضارة والمحتوى والرسائل والمحتوى الإباحي ومشكلات التحقق من الفئة العمرية والوصول إلى الملف الشخصي والمتحرشين عبر الإنترنت والاستمالة عبر الإنترنت. |
| | ٦,٣ بـــروتـوكـول نقل الصـوت عبر الإنترنت والتراسل الفوري | ٦.٢.٥ | إدراك إمكانية إبلاغ مزود الخدمة والجهات المعنية عن الاستخدام أو السلوك غير الصحيح لمواقع التواصل الاجتماعي. |
| | | ٦.٣.١ | إدراك نقاط الضعف الكامنة في أمان التراسل الفوري وبروتوكول نقل الصوت عبر الإنترنت مثل: البرامج الخبيثة والوصول المستتر والوصول إلى الملفات والتنصت. |
| | | ٦.٣.٢ | التعرف على طرق ضمان السرية عند استخدام بروتوكول نقل الصوت عبر الإنترنت والتراسل الفوري مثل: التشفير وعدم الكشف عن المعلومات الهامة وحظر مشاركة الملفات. |
| | ٦,٤ الهاتف المتحرك | ٦.٤.١ | إدراك الآثار المحتملة لاستخدام تطبيقات من متاجر التطبيقات غير الرسمية مثل: البرامج الضارة للهواتف المحمولة والاستخدام غير الضروري للمصادر والوصول إلى البيانات الشخصية ورداءة الجودة والرسوم الخفية. |
| | | ٦.٤.٢ | فهم مصطلح صلاحيات التطبيقات |
| | | ٦.٤.٣ | إدراك إمكانية استخلاص المعلومات الخاصة من تطبيقات الهواتف المحمولة مثل: تفاصيل الاتصال وسجل الموقع والصور. |
| | | ٦.٤.٤ | إدراك الإجراءات الاحتياطية وإجراءات الطوارئ التي يجب اتخاذها في حالة فقدان الهاتف مثل: التعطيل عن بعد والمسح عن بعد وتحديد موقع الهاتف. |
| **٧ - تأمين إدارة البيانات** | ٧,١ تأمين عمليـــات النسخ الاحتياطي والبيانات | ٧.١.١ | التعرف على أهمية نسخ البيانات احتياطي ا في حالة فقدانها من أجهزة الكمبيوتر أو الأجهزة الأخرى. |
| | | ٧.١.٢ | التعرف على مميزات النسخ الاحتياطي مثل: الانتظام/التكرار والجدولة وموقع التخزين وضغط البيانات. |
| | | ٧.١.٣ | نسخ البيانات احتياطي ا إلى موقع ما مثل: محرك الأقراص المحلية أو قرص تخزين/وسيط خارجي أو الخدمة السحابية. |
| | | ٧.١.٤ | استعادة البيانات من موقع النسخ الاحتياطي مثل: محرك الأقراص المحلية أو قرص تخزين/وسيط خارجي أو الخدمة السحابية. |
| | ٧,٢ الحذف والمحو الآمن للبيانات | ٧.٢.١ | التفرقة بن حذف البيانات وبين محوها نهائيا بشكل دائم. |
| | | ٧.٢.٢ | إدراك أسباب المحو النهائي الدائم للبيانات من محركات الأقراص أو الأجهزة. |
| | | ٧.٢.٣ | إدراك تعذر محو البيانات نهائيا لبعض الخدمات مثل: مواقع التواصل الاجتماعي والمدونات ومنتديات الإنترنت والخدمات السحابية. |
| | | ٧.٢.٤ | التعرف على الطرق الشائعة لمحو البيانات نهائيا وبشكل دائم مثل : التمزيق أو تدمير محرك الأقراص/الوسائط أو إزالة المغنطة أو استعمال أدوات تدمير البيانات. |

المنهج

ICDL Arabia

# مقرر ICDL
# الأمن الرقمي

اصدار المنهاج ١,٠ (الجزء الثاني)

| الموضوع | المهارة | رقم المرجع | نقاط الموضوع |
|---|---|---|---|
| **١- الحماية** | ١,١ الأمـــان الشخصي | ١.١.١ | إدراك أن المعلومات الشخصية الموجودة على جهاز الحاسوب الخاص بك يجب أن يتم حمايتها. |
| | | ١.١.٢ | فهم مفهوم مصادقة المستخدم. |
| | | ١.١.٣ | فهم المصادقة باستخدام "التوثيق الثنائي": الرموز، البطاقات الذكية، القياسات الحيوية. |
| **٢ - الأمان** | ٢,١ النســـخ الاحتياطي | ٢,١,١ | التعرف على أجهزة نسخ البيانات المعروفة: الأقراص المدمجة، أقراص الفيديو المدمجة،محركات الأقراص USB ، محركات الأقراص الصلبة الخارجية، التخزين السحابي و الانتباه من السعة التخزينية لكل منهم. |
| | ٢,٢ البريـــــد الإلكتروني | ٢.٢.١ | فهم مفهوم رسائل البريد الإلكتروني المزعجة / غير المرغوب فيها والحاجة لتصفية البريد الإلكتروني. معرفة كيفية فحص مرفقات رسائل البريد الإلكتروني قبل فتحها. |
| | | ٢.٢.٢ | تشغيل خاصية تصفية رسائل البريد الإلكتروني غير المرغوب فيها. |
| | | ٢.٢.٣ | وضع قواعد تصفية الرسائل غير المرغوب فيها. |
| | ٢,٣ الأجهزة الذكيـــة | ٢.٣,١ | إدراك ما هي المعلومات التي يحتوي عليها جهازك ونشرها على الإنترنت وكيف يمكن أن يساء استخدامها. |
| | | ٢.٣,٢ | الانتباه إلى خصائص الأمان الأساسية: حماية كلمات مرور الجهاز، ضبط خاصية القفل التلقائي، تثبيت برنامج حماية، تثبيت تحديثات نظام التشغيل، تعقب الهاتف المتحرك. |
| | | ٢.٣.٣ | التعرف على كيف يمكن أن تساعد عملية التشفير في الهواتف الذكية على منع سرقة البيانات. |
| | | ٢.٣,٤ | الانتباه إلى المشاكل الأمنية المتعلقة بالتطبيقات. يجب تحميل التطبيقات من المصادر المعتمدة فقط، التحقق من أذونات التطبيقات. |
| | | ٢.٣,٥ | الانتباه إلى التهديدات الأمنية التي الناتجة عن رسائل البريد الإلكتروني غير المرغوب فيها أو الرسائل النصية. فهم علامات الإصابة بالبرامج الخبيثة: وجود زيادة في رسوم استخدام البيانات بشكل غير معتاد، تغييرات غير مبررة في واجهة المستخدم. |
| | | ٢.٣,٦ | التعرف على كيفية إيقاف التشغيل التلقائي لخاصية الشبكة اللاسلكية والبلوتوث لمنع الوصول غير المصرح به إلى الجهاز والبيانات الخاصة بك. |
| | | ٢.٣,٧ | التعرف على كيفية حذف جميع المعلومات الشخصية عند التخلص من الجهاز. |
| | | ٢.٣,٨ | التعرف على كيفية تمكين وتعطيل إعدادات الموقع الجغرافي. فهم مزايا ومخاطر تمكين إعدادات الموقع الجغرافي. |
| | | ٢.٣,٩ | مشاركة رقم الهاتف المتحرك الخاص بك مع الأشخاص المعروفين والموثوقين فقط.الاحتفاظ بالرقم التعريفي IMEL في حالة فقدان الهاتف أو سرقته. |
| | | ٢.٣,١٠ | التعرف على كيفية تشغيل خاصية تصفية مواقع الإنترنت لمنع ظهور محتوى الإنترنت غير المناسب. |
| | ٢,٤ الشبكة اللاسلكية | ٢.٤.١ | إدراك المزايا والمخاطر المرتبطة باستخدام نقاط الاتصال اللاسلكية الموجودة في الأماكن العامة. |
| | ٢,٥ الأمـــان المادي | ٢.٥.١ | إدراك اعتبارات الأمان المادي عند استخدام جهاز الحاسوب الدفتري أو الحاسوب اللوحي. |

| الموضوع | المهارة | رقم المرجع | نقاط الموضوع |
|---|---|---|---|
| | | ٢.٥.٢ | التعرف على كيفية تقليل المخاطر المرتبطة بالسرقة أو الفقدان: وضع الجهاز في مجال الرؤية، استخدام قفل الحماية )إذا كان مناسبا (، حماية كلمات المرور، تسجيل الرقم التسلسلي، استخدام قلم التحديد الأمني. |
| | | ٢.٥.٣ | إدراك المخاطر الأمنية فيما يتعلق بالتخلص من أجهزة الحاسوب القديمة وأهمية إزالة البيانات قبل التخلص من الأجهزة. |
| | ٢,٦ عالم الجريمة الرقميـــة | ٢.٦.١ | الانتباه إلى المحتوى الذي يمكن أن يصل إليه الأشخاص خارج نطاق الشبكة العالمية العنكبوتية (.com, .org, etc.) |
| | | ٢.٦.٢ | الانتباه إلى المصطلحات "الإنترنت الخفي" ( Deep Web ) و "الشبكة السوداء" ( Dark Net )وكيفية استخدام الأشخاص لهم خارج نطاق الشبكة العالمية العنكبوتية( .com, .org, etc. ) |
| | | ٢.٦.٣ | فهم ما هو برنامج TOR وكيف يقوم الأشخاص بإرسال الرسائل عن طريقه. |
| **٣ - الوقاية من المخاطر** | ٣,١ المخاطـــر العامة للإنترنت | ٣.١.١ | إدراك كيف ينتشر المحتوى غير اللائق على الإنترنت. |
| | | ٣.١.٢ | الانتباه للتهديدات الأمنية العامة: التعرف على طلبات البريد الإلكتروني المشبوهة، المواقع الإلكترونية التي يوجد بها برمجيات خبيثة. |
| | ٣,٢ الشبكات الإجتماعية | ٣.٢.١ | إدراك المخاطر المحتملة لاستخدام مواقع التواصل الاجتماعي مثل: التسلط عبر الإنترنت والاستمالة والكشف عن البيانات الشخصية والهويات الزائفة و الروابط الاحتيالية أو الضارة والمحتوى والرسائل والمحتوى الإباحي ومشكلات التحقق من الفئة العمرية والوصول إلى الملف الشخصي والمتحرشين عبر الإنترنت والاستمالة عبر الإنترنت. |
| **٤ - الهوية** | ٤,١ الهويـــة الشخصية | ٤.١.١ | تحديد من يمكنه الوصول إلى معلوماتك الشخصية: الأصدقاء، زملاء العمل، أصحاب العمل، مرتكبي الجرائم، المتحرشين. |
| | ٤,٢ مشاركة الأجهـزة | ٤.١.٢ | الانتباه إلى نطاق الأجهزة التي يمكن استخدامها لمشاركة المعلومات: الهواتف المتحركة،الهواتف الذكية، مشغلات MP3 ، iPods ، الحواسيب اللوحية، إلى آخره. |
| | ٥,١ مقاطع الفيديو / المدونات | ٥.١.١ | فهم آلية عمل مواقع مشاركة الملفات على الإنترنت، و احتمالية الإصابة بالفيروسات والبرمجيات الخبيثة عند استخدام مواقع مشاركة الملفات. |
| **٥ - حماية المواطن** | ٥,٢ التسلط الإلكتروني | ٥.٢.١ | فهم وإدراك ما هو التسلط الإلكتروني. |
| | | ٥.٢.٢ | فهم الأساليب التي تساعد على حدوث التسلط الإلكتروني. |
| | | ٥.٢.٣ | فهم مدى السرعة التي يمكن أن تنتشر بها المعلومات / الصور وتأثيرها على التسلط الإلكتروني. |
| | | ٥.٢.٤ | إدراك العواقب المترتبة على التسلط الإلكتروني. فهم دوافع التعدي على الإنترنت، مثل إخفاء الهوية، شعور مرتكب الجريمة أنه لن يفلت من العقاب. فهم أن جريمة التعدي على الإنترنت يمكن أن تكون عملية ذات اتجاهين أيضا. |
| | | ٥.٢.٥ | معرفة كيفية مواجهة التسلط الإلكتروني، وكيفية تسجيل حدوثه وإبلاغ السلطات المختصة عن مخالفات التسلط الإلكتروني. |
| | | ٥.٢.٦ | إدراك أن البالغين يمكن أن يعانون أيضا من التسلط الإلكتروني: تعليقات غير لائقة في الرسائل، رسائل البريد الإلكتروني، في المنتديات العامة ومواقع التواصل الاجتماعي،رسائل نصية غير لائقة، الملاحقة على الإنترنت. فهم الفرق بين الملاحقة على الإنترنت والهندسة الاجتماعية. |

| الموضوع | المهارة | رقم المرجع | نقاط الموضوع |
|---|---|---|---|
| | ٥,٣ السلوك والمسؤولية الافتراضيـــة | ٥.٣.١ | لا تنشر الرسائل أو الصور أو غيرها من المواد التي يمكن أن تتسبب في حدوث أذى.شارك الصور مع الأشخاص التي تعرفهم وتثق بهم فقط. |
| | | ٥.٣.٢ | التعرف على كيفية رفض أو حظر الغرباء وجهات الاتصال غير المرغوب فيها. الانتباه عند التخطيط للقاء الأشخاص الذين لا تعرفهم حقا ، حتى لو أصبحوا أصدقاؤك على الإنترنت. |
| | | ٥.٣.٣ | استخدم كاميرا الويب مع الأشخاص الذين تعرفهم فقط – قطع أو إيقاف تشغيل الكاميرا عندما لا تكون قيد الاستخدام. |
| | | ٥.٣.٤ | الانتباه أن تنزيل الصور أو برامج الحاسوب من الإنترنت قد يكون مخالفا للقانون، إلا إذا كان مصرحا به على الموقع الذي تستخدمه. |
| | | ٥.٣.٥ | فهم المقصود بآداب التعامل على الإنترنت. |
| | | ٥.٣.٦ | معرفة لماذا يتم استخدام أسماء المستخدمين الذكية التي تقتصر على معلومات شخصية محدودة فقط على الإنترنت. |
| | | ٥.٣.٧ | إدراك لماذا تعد حماية المعلومات الشخصية والحفاظ على الخصوصية أمرا ضروريا وهاما . |
| | | ٥.٣.٨ | فهم أن المنشورات الشخصية والمتعلقة بالعمل والتعليقات والرسائل الموجودة على المنصات الاجتماعية مثل (WhatsApp ، Snapchat ، Instagram ، Facebook )إلى آخره. يمكن أن يؤثر على سمعة صاحب العمل الخاص بك وعلى مستقبلك المهني. |
| | | ٥.٣.٩ | فهم أن المنظمات يجب أن تكون قد أعلنت عن إخلاء المسؤولية والتي توضح أن آراء الموظفين على وسائل التواصل الإجتماعي هي شخصية ولا تمثل المنظمة بأي شكل |
| | | ٥.٣.١٠ | فهم لماذا يجب تقييد الموظفين من الإفراج علنا عن أي تعليقات أو معلومات قد تؤثر على أي قرار قانوني أو تجاري أو سياسي |
| | | ٥.٣.١١ | فهم لماذا قد يكون من المناسب إنشاء حسابات مستخدمين مختلفة في أذونات وصلاحيات الدخول وفقا لكل حساب. |
| | ٥,٤ إدمـان الإنترنت | ٥.٤.١ | فهم كيف أن استخدام الإنترنت يمكن أن يؤثر على الحياة اليومية والعمل والعلاقات. |
| | ٥.٥ التطـــرف على الإنترنت | ٥.٥.١ | فهم المصطلحات التطرف على الإنترنت والإرهاب على الإنترنت. |
| | | ٥.٥.٢ | الانتباه إلى كيفية استخدام المتطرفين لوسائل التواصل الاجتماعي لاستمالة الشباب وارتكاب أعمال غير قانونية. |
| **٦ - السياسة العامة** | ٦,١ الاستخدام | ٦.١.١ | فهم المقصود بسياسة الاستخدام المقبول(AUP ) وما هي أهميته بالنسبة للمؤسسات. |
| | | ٦.١.٢ | التعرف على القواعد التي يجب اتباعها في سياسة الاستخدام المقبولة: تقليل المخاطر، تشجيع آداب التعامل على الإنترنت والسلوك الاجتماعي والأخلاقي والهوية الشخصية وحماية كلمات المرور. |
| | | ٦.٢.١ | الانتباه إلى قوانين حقوق النشر والتأليف ومدى تأثيرها على تحميل المحتوى بشكل غير مشروع باستخدام خدمات مشاركة الملفات. |