الديوان العام للمحاسبة
General Court of Audit

المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة
ARABOSAI

اللقاء التدريبي حول مخاطر التشغيل الإلكتروني للبيانات وكيفية اكتشاف وسائل الغش ومواطن الفساد

الرياض، ٢٢-٢٦ أكتوبر ٢٠٢٣م

تنمية معارف ومهارات المشاركين في اكتشاف مخاطر التشغيل الإلكتروني للبيانات وأساليب ووسائل اكتشاف مواطن الغش والفساد وفقا لإطار المعايير الدولية للإنتوساي، وسيساعد ذلك على:

- التعرف على المخاطر (تعريفها، أنواعها، أسبابها) التي ينبغي التنبه لها في بيئة تقنية المعلومات.
- إتقان المهارات الضرورية للتعرف على مخاطر التشغيل الإلكتروني للبيانات، وطرق التعامل معها.
- فهم أساليب ووسائل الغش والفساد في بيئة تقنية المعلومات، وطرق مواجهتها.
- التعرف على تجارب وخبرات المشاركين حول الرقابة على التشغيل الإلكتروني للبيانات.
- إتقان بعض المهارات التي تساعد في تخطيط وتنفيذ ومتابعة الخطط حول البيانات وبيئة العمل الإلكتروني.
- التمكن من المساهمة في إعداد خطوات استراتيجية لتعزيز الرقابة على البيانات في بيئة التشغيل الإلكتروني للبيانات (الحكومة الإلكترونية).

الأهــداف

- التعريف بأساليب وأنواع الرقابات في ظل التشغيل الالكتروني للبيانات وأهم المخاطر المتوقعة وطرق اكتشافها وتلافيها
- مواكبة موضوع الرقابة على تكنولوجيا المعلومات والتطورات الحديثة في هذا المضمار

محاور
الاهتمام

عناصر
اللقـاء

- التشغيل الإلكتروني للبيانات الحكومية ومخاطرها.
- أساليب ووسائل الغش في بيئة تقنية المعلومات.
- تخطيط وتنفيذ ومتابعة عمليات الرقابة في بيئة العمل الإلكتروني.
- خطوات إعداد استراتيجية لتعزيز الرقابة على البيانات.
- استعراض تجارب وخطوات المشاركين حول موضوع اللقاء.

تعارف المشاركين:

الاسم، الجهاز الرقابي

المؤهل الأكاديمي وطبيعة العمل الفعلي

الخبرات السابقة

الخبرة في تدقيق البيانات الإلكترونية

الخبرة في التدقيق في ظل مخاطر الغش الفساد المالي والإداري

ماهي توقعاتك وأهدافك من المشاركة في هذا اللقاء؟

شكراً لكم

المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة
ARABOSAI

الديوان العام للمحاسبة
General Court of Audit

التشغيل الإلكتروني للبيانات الحكومية ومخاطره

(الوحدة الأولى)

الوحدة الأولى: التشغيل الإلكتروني للبيانات الحكومية ومخاطره

هدف التعلم:

اكتساب المشاركين المعارف اللازمة حول بيئة تقنية المعلومات ومكوناتها، وأهم المخاطر المرتبطة بالتشغيل الإلكتروني للبيانات في القطاع العام

محاور الوحدة

- مفهوم العمل في بيئة تقنية المعلومات ومكوناته
- العنصر البشري خط الدفاع الأول
- المخاطر المرتبطة بتشغيل البيانات الإلكترونية

مكونات الوحدة

- مفهوم العمل في بيئة تقنية المعلومات ومكوناته
- العنصر البشري خط الدفاع الأول
- المخاطر المرتبطة بتشغيل البيانات الإلكترونية

محاور الجلسة

- مفهوم بيئة تقنية المعلومات
- مكونات منظومة عمل تقنية المعلومات
- التعاملات في ظل بيئة تقنية المعلومات

مفهوم بيئة تقنية المعلومات

تقنية المعلومات أو **تكنولوجيا المعلومات**

information technology

تتمثل في «دراسة، وتصميم، وتطوير، وتفعيل أو تسيير أنظمة المعلومات التي تعتمد على الحواسيب، وبشكل خاص تطبيقات وبنية عتاد الحاسوب»،

حسب تعريف مجموعة تقنية المعلومات الأمريكية ITAA

و تهتم تقنية المعلومات باستخدام الحواسيب والتطبيقات البرمجية لتحويل، وتخزين، وحماية، ومعالجة، وإرسال، والاسترجاع الآمن للمعلومات.

مفهوم بيئة تقنية المعلومات

تقنية المعلومات أو تكنولوجيا المعلومات

IT

التقنية technology	هي الطريقة التي يستخدمها الناس في اكتشافاتهم واختراعاتهم وكل تغيير وتطوير في كافة المجالات	التقنية الصناعية تقنيات التعلم التقنيات الصحية
المعلومات information	هي نتائج معالجة البيانات، مما يجعلها ذات معنى وقيمة ومرتبطة بسياق معين يدركه الإنسان	المعلومات التطويرية والنمائية المعلومات التعليمية المعلومات السياسية

مفهوم بيئة تقنية المعلومات

تقنية

المعلومات أو تكنولوجيا

المعلومات

IT

تتلخص حول ..

استخدام التقنيات الحديثة في إدارة ومعالجة الكم الهائل من المعلومات في شتى المجالات

بشكل مبسط ..

نستطيع القول بأن تقنية المعلومات هي كل ما يدخل في استخدام الحاسوب بأي شكل من الأشكال، وأن اختراع الحواسيب سبب رئيس في ظهور تقنية المعلومات، وأن توفير الانفتاح وتحقيق مجتمع المعلومات يتم بدمج المحتوى "المعلومات" و "التقنية" وهو جوهر مفهوم تقنية المعلومات

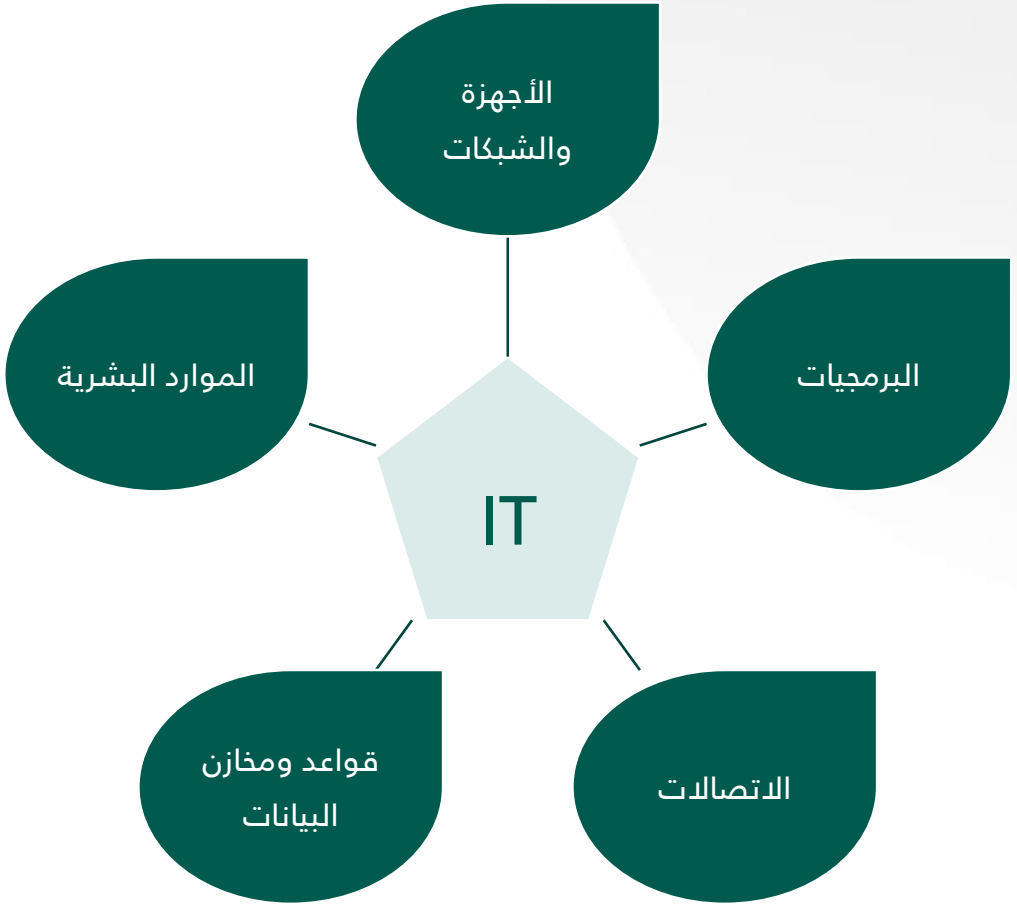
مفهوم بيئة تقنية المعلومات

خصائص المعلومات في بيئة عمل تقنية المعلومات

- القدرة على التشكيل أو إعادة الصياغة.
- إمكانيّة نقلها عبر مسارات مُحدّدة، أو بثّها للجميع.
- القدرة على دمج كمٍّ هائل من المعلومات معاً.
- الوفرة، ولذلك أخذ منتجوها يضعون القيود على انسيابها لجعلها سلعةً تخضع لقوانين العرض والطلب.
- عدم تأثُّرها بالاستهلاك، بل على العكس، فهي عادةً ما تنمو مع زيادة استهلاكها.
- سهولة النسخ بوسائل يسيرة وبسيطة، وتوجد في متناول يد الجميع، باستثناء المعلومات التي توضع عليها قيود كحقوقٍ للملكية.
- القدرة على تصحيح المعلومات الخاطئة من خلال تتبُّع المسارات التي مرّت بها قبل الوصول إلى النتائج النهائيّة، وتصحيح الخاطئ منها.
- عدم القدرة على الحكم القاطع بصحّة الكثير منها، فيشوبها عدم اليقين، والقابليّة للتغيير والنقض.

مكونات منظومة عمل تقنية المعلومات

البنية التحتية لمنظومة عمل تقنية المعلومات تتمثل في كل ما نحتاجه لإنشاء تطبيقات برمجية وتشغيلها في مؤسسة ما، وهي تشمل:



مكونات منظومة عمل تقنية المعلومات

الأجهزة والشبكات

جميع الأجهزة الموجود في نظام تكنولوجيا المعلومات، مثل أجهزة الحاسوب وملحقاتها، مثل لوحة المفاتيح، ومحركات الأقراص وأجهزة التوجيه أو الهواتف الذكية، حيث تعمل هذه الأجهزة على استقبال ونقل المعلومات مع وجود الإنترنت

مكونات منظومة عمل تقنية المعلومات

البرمجيات

برامج النظام وهي البرامج التي تساعد على إدارة الأجهزة والملفات والبرامج الأخرى

مكونات منظومة عمل تقنية المعلومات

الأجهزة والشبكات	البرمجيات	الاتصالات	قواعد ومخازن البيانات	الموارد البشرية
				

الاتصالات

هي الأداة التي تعمل على ربط وتوصيل الأجهزة ببعضها البعض، لتشكيل شبكة النظام، ويمكن أن تكون الاتصالات إما بواسطة الأسلاك مثل الألياف الضوئية أو الكابلات، أو الاتصالات اللاسلكية مثل شبكة Wi-Fi، كما تقسم الشبكات إلى شبكات محلية وشبكات واسعة النطاق بناءً على المنطقة التي تغطيها، كما يمكن اعتبار الانترنت شبكة من الشبكات

مكونات منظومة عمل تقنية المعلومات

الأجهزة والشبكات	البرمجيات	الاتصالات	قواعد ومخازن البيانات	الموارد البشرية
				

قواعد ومخازن البيانات

هي المادة الأساس والجزء الأهم من الأنظمة وهي عبارة عن مجموعة من البيانات المترابطة والمخزنة بشكل محمي لكي لا يتم التلاعب غير المصرح بها، وقد اكتسبت قواعد البيانات ومستودعات البيانات أهميةً أكبر في أنظمة المعلومات مع ظهور مفهوم "البيانات الضخمة"

مكونات منظومة عمل تقنية المعلومات

الأجهزة والشبكات	البرمجيات	الاتصالات	قواعد ومخازن البيانات	الموارد البشرية
				

الموارد البشرية

وهم الأشخاص الذي يشغلون ويديرون النظام، ويتّبعون الإجراءات التي تُحوّل المعرفة في قواعد البيانات الضخمة ومستودعات البيانات، كما يشمل النظام المبرمجين ومدخلين البيانات والمصممين ومحللي الأعمال، ومسؤولي أمن المعلومات وغيرهم، حيث يجب تدريب كافة الموظفين على الاستفادة القصوى من إمكانيات نظام المعلومات.

مكونات منظومة عمل تقنية المعلومات

الأجهزة والشبكات	البرمجيات	الاتصالات	قواعد ومخازن البيانات	الموارد البشرية
				

الأنظمة واللوائح والتشريعات

أدلة وإرشادات ونماذج العمل

المعايير وقواعد السلوك المهني

العملاء/ المستفيدون

التعاملات في ظل بيئة تقنية المعلومات

يتم استعمال تقنية المعلومات في مجالات واسعة في المجتمع، منها ما يلي:

الأعمال

غيّر ظهور تقنية المعلومات الآليّة التي تتم بها الأعمال تغيراً جذرياً، حيث يتم استخدامها في مختلف الأقسام مثل:

الأقسام الماليّة، والموارد البشريّة، والتصنيع، وحتى الأمن، والتي تتم كافّتها باستخدام الأجهزة والبرامج المختلفة.

التعاملات في ظل بيئة تقنية المعلومات

يتم استعمال تقنية المعلومات في مجالات واسعة في المجتمع، منها ما يلي:

التعليم

طوّر استخدام تقنية المعلومات من تواصل المعلمين، مع الطلاب، بالإضافة للمُساعدة على تعلّم أشياء جديدة، وسهولة وصول المعلومات للطلاب بعيداً عن الغرف الصفيّة، عبر استخدام الهاتف المحمول، والأجهزة اللوحية وغيرها.

التعاملات في ظل بيئة تقنية المعلومات

يتم استعمال تقنية المعلومات في مجالات واسعة في المجتمع، منها ما يلي:

التمويل

تُساعد تقنية المعلومات على فتح الأفق أمام الأشخاص وتُسهّل من التعاملات الماليّة والصفقات، من تدول، وشراء عبر الإنترنت حيث تحتفظ البنوك عادةً بسجلات تفنّد كافة المعاملات المالية والحسابات القائمة باستخدام أجهزة الكمبيوتر.

التعاملات في ظل بيئة تقنية المعلومات

يتم استعمال تقنية المعلومات في مجالات واسعة في المجتمع، منها ما يلي:

الرعاية الصحية

طوّر استخدام تقنية المعلومات في مجال الطب من سرعة تقديم الرعاية الصحيّة، إذ أصبح من السهل تقديم المعلومات بخصوص المرضى، والتواصل مع الخبراء بالإضافة لسهولة فحص المرضى وتقليل وقت إجراء الأعمال الورقيّة.

التعاملات في ظل بيئة تقنية المعلومات

يتم استعمال تقنية المعلومات في مجالات واسعة في المجتمع، منها ما يلي:

الحماية

وفّر استخدام تقنية المعلومات الأمان في إجراء المعاملات والاحتفاظ بسجلاتها عبر الإنترنت، من خلال وصول أشخاص مُعينين فقط للبيانات، ومنع أي شخص عشوائي من الوصول إليها، وذلك عبر الحفاظ على كلمات المرور، والسماح للأشخاص المخولين فقط بالوصول إليها واستخدامها.

التعاملات في ظل بيئة تقنية المعلومات

يتم استعمال تقنية المعلومات في مجالات واسعة في المجتمع، منها ما يلي:

التوظيف

خلق استخدام تقنية المعلومات في المؤسسات والشركات وظائف للأشخاص الخبراء بمجال تقنية المعلومات، وغيرها من المجالات عبر الاحتفاظ بقواعد بيانات للوظائف المتاحة، كما ساعدت في الحصول على دورات وورش تدريبيّة قصيرة في مجال تقنية المعلومات عبر الإنترنت لتزويد الأفراد الراغبين باتخاذها كمهنة بخلفيّة بسيطة قبل الشروع بالعمل ضمن مجالها

التعاملات في ظل بيئة تقنية المعلومات

العوائق التي تواجه التعاملات في بيئة تقنية المعلومات

الكميات الهائلة من البيانات التي يتم التعامل معها، والحاجة لسعة تخزينية عالية ومكلفة لتوفيرها.

الحاجة لزيادة مهارات العمل الجماعي والتواصل، وبشكل خاص لغرض تقديم الخدمة للمستخدمين الذين يفتقرون لمهارة استخدام أجهزة الحاسوب وتطبيقات تقنية المعلومات

الحماية ومشاكل الأمان، التي تُشكّل مصدر قلق للشركات ورجال الأعمال، والتي قد يؤدي أي حادث فيها للإضرار بسمعة الشركات وغيره من الأضرار المادية المترتبة على ذلك

حالة دراسية

برأيك منهم الأطراف المعنيين بالتعامل مع بيئة تقنية المعلومات في القطاع الحكومي؟

تعليمات حل التمرين:

التفكير المنفرد ٢ د

العمل ضمن المجموعة ٣ د

المناقشة والحل ١٠ د

التعاملات في ظل بيئة تقنية المعلومات

أصحاب المصلحة في بيئة تقنية المعلومات

- الإدارة العليا/ الإدارة
- المشغلون
- الموردون
- العملاء/المستخدمون
- المراقبون

مفهوم العمل في بيئة تقنية المعلومات ومكوناته

الخلاصة

- يتمثل مفهوم تقنية المعلومات في دراسة، وتصميم، وتطوير، وتفعيل أو تسيير أنظمة المعلومات التي تعتمد على الحواسيب، وهي تستخدم في العديد من المجالات من أهمها الأعمال، والتعليم، والرعاية الصحية، والتمويل، والحماية، والتوظيف.
- تتكون بيئة تقنية المعلومات من خمس عناصر، هي الأجهزة والشبكات، البرمجيات، الاتصالات، قواعد البيانات، الموارد البشرية، وهي تتعامل مع أطراف متعددة، منها الإدارة، ومشغلي تقنية المعلومات، والموردين، والعملاء أو المستفيدين، والمراقبين.

شكراً لكم

الديوان العام للمحاسبة
General Court of Audit

المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة
ARABOSAI

تخطيط وتنفيذ ومتابعة عمليات الرقابة في بيئة العمل الإلكتروني

(الوحدة الثالثة)

الوحدة الثالثة: تخطيط وتنفيذ ومتابعة عمليات الرقابة في بيئة العمل الإلكتروني

هدف التعلم:

اكتساب مهارات جديدة في التخطيط لعمليات الرقابة في بيئة تقنية المعلومات

محاور الوحدة

- فهم بيئة تقنية المعلومات والتخطيط لمهمات الرقابة على تقنية المعلومات.
- تصميم عملية تقييم الرقابة على تقنية المعلومات
- أساليب جمع وتحليل البيانات في بيئة تقنية المعلومات
- التوثيق وجمع الأدلة في بيئة تقنية المعلومات
- متابعة نتائج الرقابة

مكونات الوحدة

- فهم بيئة تقنية المعلومات والتخطيط لمهمات الرقابة على تقنية المعلومات.
- تصميم عملية تدقيق الرقابة على تقنية المعلومات
- أساليب جمع وتحليل البيانات في بيئة تقنية المعلومات
- التوثيق وجمع الأدلة في بيئة تقنية المعلومات
- متابعة نتائج الرقابة

الجلسة الأولى: فهم بيئة تقنية المعلومات والتخطيط لمهمات الرقابة على تقنية المعلومات.

محاور الجلسة

- تصميم عملية تدقيق الرقابة على تقنية المعلومات
- أساليب جمع وتحليل البيانات في بيئة تقنية المعلومات
- التوثيق وجمع الأدلة في بيئة تقنية المعلومات
- متابعة نتائج الرقابة

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

الخطوة ٤

الإبلاغ عن نتائج تدقيق تقنية المعلومات

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات	صياغة أهداف التدقيق لمهمة تدقيق تقنية المعلومات
	تحديد نطاق ومنهجية تدقيق تقنية المعلومات
	ضوابط عامة لتدقيق تقنية المعلومات والتطبيقات

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

صياغة أهداف التدقيق لمهمة تدقيق تقنية المعلومات

يمكن أن تختلف أهداف تدقيق تقنية المعلومات بناءً على مجموعة متنوعة من العوامل، مثل نوع المراجعة العام (أي الأداء أو المالي أو الامتثال)، أو المنظمة أو المنظمات قيد المراجعة، أو نوع عمليات تقنية المعلومات قيد المراجعة، أو المخاطر الرئيسة للمؤسسة أو المنظمات وعوامل أخرى.

بعض الأمثلة على أهداف المراجعة هي

- لتدقيق الأداء، للتأكد من أن موارد تقنية المعلومات تسمح بتحقيق الأهداف التنظيمية بكفاءة وفعالية، وأن الضوابط ذات الصلة فعالة في منع واكتشاف وتصحيح حالات الزيادة، وكذلك الإسراف وعدم الكفاءة في استخدام وإدارة نظم المعلومات؛
- بالنسبة لعمليات المراجعة المالي، لتقييم الضوابط ذات الصلة التي لها تأثير على موثوقية البيانات من أنظمة المعلومات، والتي بدورها لها تأثير على البيانات المالية للمنظمة المدققة؛ أو لتقييم العمليات التي تدخل في عمليات منطقة معينة، مثل نظام كشوف المرتبات أو نظام المحاسبة المالية؛ و
- لتدقيق الامتثال، لضمان امتثال عمليات نظم المعلومات للقوانين والسياسات والمعايير المطبقة على المنظمة الخاضعة للرقابة.

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

صياغة أهداف التدقيق لمهمة تدقيق تقنية المعلومات

قد يغطي نطاق عمليات تدقيق تقنية المعلومات مجالات محددة من تنفيذ تقنية المعلومات، مثل

- اقتناء وتطوير وتنفيذ أنظمة تقنية المعلومات،
- عمليات التشغيل والصيانة،
- إدارة التغيير،
- ادارة الوصول،
- أمن المعلومات واستمرارية الأعمال،
- القيمة مقابل المال المقدم من خلال أنظمة تقنية المعلومات، و
- تخطيط موارد المؤسسة أو أنظمة تقنية المعلومات المعقدة / المتخصصة الأخرى.
- تخطيط موارد المؤسسة أو أنظمة تقنية المعلومات المعقدة / المتخصصة الأخرى.

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

صياغة أهداف التدقيق لمهمة تدقيق تقنية المعلومات

إذا كان تدقيق تقنية المعلومات جزءًا من مهمة المراجعة، فيجب على الجهاز الأعلى للرقابة التأكد من أن فريق المراجعة ككل يعمل بطريقة متكاملة لتحقيق الهدف الشامل للتدقيق. على سبيل المثال، لتحقيق التكامل الفاعل، قد تنظر الأجهزة العليا للرقابة

- توثيق شامل للعمل الذي يتعين على مدققي تقنية المعلومات القيام به،
- صياغة بروتوكول لتبادل المعلومات بين مدققي تقنية المعلومات والمراجعين الآخرين، و
- تحديد أنظمة المعلومات وأهداف الرقابة التي تدخل في نطاق المراجعة.

بعد تطوير هدف (أهداف) المراجعة ونهجها، غالبًا ما يصيغ مدققو تقنية المعلومات أسئلة تدقيق محددة من شأنها توجيه أعمال المراجعة. يجب أن تنبثق أسئلة المراجعة من هدف (أهداف) المراجعة العام، وعادة ما تكون أكثر تحديدًا من حيث أنها تتناول الموضوعات التي ستصفها أو تقيمها أثناء المراجعة. الهدف هو أن تغطي أسئلة المراجعة جميع جوانب هدف (أهداف) المراجعة. أسئلة المراجعة إما وصفية (بمعنى أنها تصف حالة) أو تقييمية (بمعنى أنها تقيم حالة مقابل معايير ويمكن أن تكون معيارية أو تحليلية).

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

تحديد نطاق ومنهجية تدقيق تقنية المعلومات

مـا؟	• ما هي الأسئلة أو الفرضيات المعينة الجاري فحصها؟ • ما هي العمليات الرئيسة المتعلقة بعملية التدقيق الخاصة بك؟ • ما هو الموضوع الذي سيتم تقييمه والإبلاغ عنه؟ • ما هي المصادر المتاحة لإتمام عملية التدقيق؟
من ؟	• من هي الوكالات والمنظمات التي تتولى مسؤوليات أو لديها وجهات نظر متعلقة بعملية التدقيق؟ • في هذه الوكالات والمنظمات ذات الصلة، من الموظف الذي يشغل أفضل المناصب لتقديم الأدلة المناسبة والكافية للإجابة عن أسئلة عملية التدقيق؟ • من المسؤول عن ضمان موثوقية المعلومات والبيانات ذات الصلة بعملية التدقيق الخاصة بك؟
أين ؟	• ما هي المواقع الواجب تغطيتها؟ • أن الوثائق والسجلات التي يتعين فحصها؟
متى ؟	• ما هو الإطار الزمني الواجب تغطيته؟

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

تحديد نطاق ومنهجية تدقيق تقنية المعلومات

غالبًا ما يُطلب من مدقق تقنية المعلومات تقييم السياسات والإجراءات التي توجه البيئة العامة لتقنية المعلومات في المنظمة الخاضعة للرقابة، والتأكد من أن الضوابط المقابلة وآليات الإنفاذ في مكانها الصحيح. يشمل تحديد نطاق تدقيق تقنية المعلومات تحديد مدى تدقيق المراجعة؛ تغطية أنظمة تقنية المعلومات ووظائفها؛ عمليات تقنية المعلومات التي يتعين تدقيقها؛ مواقع أنظمة تقنية المعلومات التي سيتم تغطيتها بما في ذلك الأطراف الثالثة، مثل مقدمي الخدمات السحابية أو الخارجيين، الذين تشكل بيئات التحكم الخاصة بهم جزءًا من بيئة التحكم الخاصة بالكيان الخاضع للرقابة؛ والفترة الزمنية التي سيغطيها المراجعة.[30]

يجوز للأجهزة العليا للرقابة اختيار الفترة الزمنية لتحليل المراجعة (على سبيل المثال، سنة واحدة أو 3 سنوات) في تحديد نطاق ارتباط تدقيق تقنية المعلومات. قد تكون ثمة حاجة أيضًا لعملية تدقيق لتنتهي في تاريخ محدد. يجب اختيار فترة زمنية ذات صلة بالأهداف المحددة لارتباط المراجعة.

بمجرد تحديد نطاق المراجعة، تحدد فرق تدقيق تقنية المعلومات المنهجية أو الخطوات المحددة التي يخططون لاتخاذها لأداء أهداف المراجعة وفقًا للنطاق. من خلال تحديد تفاصيل المنهجية، تضمن فرق المراجعة بشكل أفضل أن الخطوات التي يخططون لاتخاذها ممكنة فيما يتعلق بالبيانات التي يخططون لجمعها، وأنهم لا يؤدون خطوات تدقيق خارجية، وأن نتائج خطوات المراجعة المتخذة ستسمح للفريق للتحدث عن أهداف المراجعة.

يجب إطلاع المنظمة الخاضعة للرقابة على النطاق والأهداف ومعايير التقييم الخاصة بالمراجعة التي يجب مناقشتها معهم حسب الضرورة. يجوز للجهاز الأعلى للرقابة، إذا لزم الأمر، كتابة خطاب الارتباط إلى المنظمة الخاضعة للرقابة حيث قد يحدد أيضًا شروط هذه الارتباطات.

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

الضوابط العامة لتدقيق تقنية المعلومات والتطبيقات

تستخدم الضوابط للتخفيف من المخاطر التي تتعرض لها المنظمة. وعلى وجه الخصوص، فهناك ثمة أنواع من المخاطر ذات الصلة بضوابط تدقيق تقنية المعلومات:

- تتكون **مخاطر التحكم** من احتمال فشل ضوابط تقنية المعلومات التي تم تبنيها من قبل المنظمة المدققة في التخفيف من الأثر السلبي الذي تم تصميمها استجابة له. على سبيل المثال، قد يعتمد نظام المعلومات المطلوب لضمان تقييد الوصول إلى البيانات السرية على الأفراد المصرح لهم التحكم في طلب تقديم اسم مستخدم وكلمة مرور من قبل الأفراد الذين يحاولون الوصول. تتمثل مخاطر التحكم في هذه الحالة في أن اسم المستخدم وكلمة المرور ليسا آمنين بشكل كاف ويمكن تخمينهما من قبل الأفراد غير المصرح لهم من خلال المحاولات المتكررة، مما يؤدي إلى فقدان السرية والتأثير السلبي المحتمل على المنظمة. المنظمة التي تصر على استخدام كلمات مرور آمنة وغير تافهة تحتوي على مزيج من الرموز الأبجدية والرقمية والخاصة وتضمن أن يمنع نظام المعلومات الوصول إلى اسم المستخدم بعد عدد معين من المحاولات الفاشلة للوصول سيكون أقل السيطرة على المخاطر من تلك التي لا تحتوي على هذه الميزات. يمكن أيضًا استخدام المصادقة متعددة العوامل لتقليل مخاطر التحكم في مثل هذه الحالة.
- تتكون **مخاطر الاكتشاف** من احتمال عدم اكتشاف المدقق لغياب أو فشل أو عدم كفاية ضوابط تقنية المعلومات المعتمدة من قبل المنظمة، والتي قد يكون لها تأثير سلبي محتمل على المنظمة.
- **المخاطر المتبقية** هي المستوى المتبقي من المخاطر بعد تطبيق الضوابط، ويمكن تقليلها بشكل أكبر من خلال تحديد تلك المجالات التي تتطلب المزيد من السيطرة. يمكن تحديد مستوى مقبول من هدف المخاطر من قبل الإدارة (قابلية المخاطرة).

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

الضوابط العامة لتدقيق تقنية المعلومات والتطبيقات

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

الضوابط العامة لتدقيق تقنية المعلومات والتطبيقات

مناطق العناصر الحرجة لعناصر التحكم العامة على مستوى التطبيق هي:

- إدارة الأمن
- التحكم في الوصول / الفصل بين وصول المستخدم
- إدارة التكوين / إدارة التغيير،
- إدارة العمليات،
- و • التخطيط للطوارئ.

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

الضوابط العامة لتدقيق تقنية المعلومات والتطبيقات

مناطق العناصر الحرجة لعناصر التحكم العامة على مستوى التطبيق هي:

- إدارة الأمن
- التحكم في الوصول / الفصل بين وصول المستخدم
- إدارة التكوين / إدارة التغيير،
- إدارة العمليات،
- و • التخطيط للطوارئ.

مراحل تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

تصميم عملية تدقيق تقنية المعلومات

الضوابط العامة لتدقيق تقنية المعلومات والتطبيقات

تعمل ضوابط التطبيق على المعاملات الفردية أو المجموعات وتضمن أن المعاملات يتم إدخالها ومعالجتها وإخراجها بشكل صحيح. يؤثر تصميم وفعالية تشغيل ضوابط تقنية المعلومات العامة بشكل كبير على مدى إمكانية الاعتماد على ضوابط التطبيق من قبل الإدارة لإدارة الخاطر

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

- جمع أدلة المراجعة
- التواصل مع الجهة الخاضعة للرقابة
- توثيق إجراءات تدقيق تقنية المعلومات
- المراجعة الإشرافية

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

جمع أدلة المراجعة

يجب أن تكون نتائج المراجعة مدعومة بالأدلة، لذا فإن كمية ونوعية الأدلة التي تم الحصول عليها مهمة. هذا يعني أن مدقق تقنية المعلومات سيحتاج إلى دراسة وتقييم الأدلة التي يخططون للحصول عليها، أو التي حصلوا عليها، للتأكد من كفايتها وملاءمتها. تشير الكفاية إلى كمية الأدلة التي تم جمعها. الملاءمة تشير إلى جودة الأدلة، وما إذا كانت موثوقة وذات صلة. يمكن للمدققين تقييم ما إذا كانت الأدلة ملائمة وموثوقة من خلال مراعاة، من بين أمور أخرى، طبيعة مصدر الدليل وسمعة المصدر؛ الضوابط التي تديرها الجهة الخاضعة للرقابة، ووجود أدلة متناقضة أو مؤكدة، والطرق والنماذج والافتراضات المستخدمة في إعداد المعلومات في الدليل.

تعتبر مصفوفة نتائج المراجعة إحدى الأدوات المفيدة لتقييم أدلة المراجعة وتطوير الاستنتاجات والتوصيات. تتيح هذه الأداة للمدققين تحديد ما إذا كانت النتائج والتوصيات، إن وجدت، تستند إلى أدلة كافية ومناسبة. يقدم الشكل 5 مثالاً على نموذج مصفوفة نتائج المراجعة.[33]

شكل5 : قالب مصفوفة نتائج المراجعة

النتيجة	بيان النتيجة (الموقف المكتشف)	معظم الأحداث ذات الصلة التي تم التعرف عليها في إطار العمل.
	المعايير	المعلومات المستخدمة لتحديد إذا ما كان الأداء المتوقع لهدف عملية التدقيق مُرضٍ، يتجاوز التوقعات، أو غير مُرضٍ.
	الأدلة والتحليل	نتيجة تطبيق طرق تحليل البيانات أو تقييم الأدلة. يمكن الإشارة إلى الأساليب المستخدمة لمعالجة المعلومات التي تم جمعها في إطار العمل والنتائج المتحققة.
	الأسباب	الأسباب وراء الحادث المكتشف. ربما يكون متعلقًا بعملية التشغيل أو التصميم للهدف من عملية التدقيق. ربما يكون خارجا عن سيطرة المدير. يجب أن تكون أي توصية ذات صلةٍ بالأسباب.
	التأثيرات	الأسباب المتعلقة بالأسباب والأدلة المتوافقة ربما يكون أداة القياس لأهمية النتائج.
هل النتائج كافية (نعم/لا)؟ وإذا لم، ما هو العمل المتبقي الضروري لمعالجة أي فجوات في الدليل؟		خذ الدليل الذي لديك بعين الاعتبار لكل عنصر للنتيجة وإذا ما كان كافيًا ومناسبًا. إذا لم يكن الدليل الحالي كافيًا لكل عنصر، ، ما هو العمل المتبقي الضروري لمعالجة أي فجوات في الدليل؟
الممارسات الجيدة		الأعمال التي تم تحديدها والتي تؤدي إلى الأداء الجيد. ربما تدعم التوصيات.
التوصيات		المقترحات لمعالجة الأسباب (أو أوجه القصور) التي تم تحديدها.

ملحوظة: يهدف هذا الشكل إلى تقديم مثال توضيحي ويجب تكييفه مع ارتباطات المراجعة الفردية.

المصدر: Adapted from U.S. GAO and SAI Brazil.

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

التواصل مع الجهة الخاضعة للرقابة

لمـــــــاذا ؟

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

التواصل مع الجهة الخاضعة للرقابة

- توصي المعايير الدولية للأجهزة الرقابية بأن يقوم المدققون بإنشاء اتصال فعال طوال عملية الراجعة وإبقاء المنظمة الخاضعة للرقابة على علم بجميع الأمور المتعلقة بالمراجعة
- بالنسبة لتدقيق تقنية المعلومات، قد يطلب المدققون التعاون والدعم اللازمين من المنظمة الخاضعة للتدقيق في استكمال الراجعة،
- بما في ذلك الوصول إلى السجلات والمعلومات.
- قد يحدد المدققون طريقة الوصول إلى البيانات الإلكترونية بالصيغة اللازمة للسماح بالتحليل، بالتشاور مع المنظمة الخاضعة للرقابة. سيكون أسلوب الوصول إلى البيانات خاصاً بالجهاز

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

توثيق إجراءات تدقيق تقنية المعلومات

- توثيق تدقيق نظم المعلومات هو سجل أعمال الراجعة المنفذة والأدلة الداعمة للنتائج والاستنتاجات.
- يجب ضمان الحفاظ على النتائج والأدلة من قبل مدققي تقنية المعلومات بحيث تتوافق مع متطلبات الموثوقية والاكتمال والكفاية والصحة.
- من المهم أيضاً لمدققي تقنية المعلومات التأكد من الحفاظ على عملية المراجعة لتمكين التحقق اللاحق من إجراءات التحليل.

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

توثيق إجراءات تدقيق تقنية المعلومات

ما الذي يتعين على المدقق الخبير أن يفهمه من توثيق عملية التدقيق؟

- ✓ النتائج التي تم التوصل إليها نتيجة للأمور المهمة السابقة.
- ✓ القرارات المهمة أو الرئيسة التي اتخذت للتوصل إلى هذه النتائج.
- ✓ طبيعة ووقت ونطاق العمل المؤدى
- ✓ نتائج عملية التدقيق والأدلة المتاحة
- ✓ الأمور المهمة التي تنشأ خلال عملية التدقيق (على سبيل المثال، التغييرات في نطاق أو منهج التدقيق والقرارات المتعلقة بعامل المخاطرة الجديد الذي يتم تحديده خلال التدقيق والإجراءات المتخذة كنتيجة لعدم الاتفاق بين الكيان المدقق والفريق، إلخ).

ملحوظة: يهدف هذا الشكل إلى تقديم مثال توضيحي ويجب تكييفه مع ارتباطات المراجعة الفردية.

المصدر: Performance Audit Subcommittee Development Team.

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

المراجعة الإشرافية

الإشراف والتوجيه

- يجب الإشراف على عمل موظفي المراجعة بشكل صحيح أثناء الراجعة، ويجب مراجعة العمل الموثق من قبل أحد كبار موظفي المراجعة.
- كما يجب على كبار موظفي المراجعة تقديم التوجيه اللازم، والتدريب، ودور التوجيه أثناء المراجعة

مراحل تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

إجراء عملية تدقيق تقنية المعلومات

المراجعة الإشرافية

الإشراف والتوجيه

- يجب الإشراف على عمل موظفي المراجعة بشكل صحيح أثناء الراجعة، ويجب مراجعة العمل الموثق من قبل أحد كبار موظفي المراجعة.
- كما يجب على كبار موظفي المراجعة تقديم التوجيه اللازم، والتدريب، ودور التوجيه أثناء المراجعة

مراحل تدقيق تقنية المعلومات

الخطوة ٤

الإبلاغ عن نتائج تدقيق تقنية المعلومات

الإبلاغ عن نتائج تدقيق تقنية المعلومات

مراحل الإبلاغ عن نتائج تدقيق تقنية المعلومات

المتابعة واستيفاء استنتاجات وتوصيات التدقيق

مراحل تدقيق تقنية المعلومات

الخطوة ٤

الإبلاغ عن نتائج تدقيق تقنية المعلومات

الإبلاغ عن نتائج تدقيق تقنية المعلومات

مراحل الإبلاغ عن نتائج تدقيق تقنية المعلومات

المتابعة واستيفاء استنتاجات وتوصيات التدقيق

مراحل تدقيق تقنية المعلومات

الخطوة ٤

الإبلاغ عن نتائج تدقيق تقنية المعلومات

الإبلاغ عن نتائج تدقيق تقنية المعلومات

مراحل الإبلاغ عن نتائج تدقيق تقنية المعلومات

تعتمد تقارير تدقيق تقنية المعلومات على تقاليد الأجهزة العليا للرقابة المالية والمحاسبة وبيئاتها القانونية.

وغالباً ما يتكون إعداد التقارير خلال عملية المراجعة من مراحل مثل:

١. مسودة مشروع التقرير

٢. الرسالة الإدارية (خطاب الجهاز)

٣. تقرير المراجعة النهائي، بعد استلام التعليقات من الإدارة الخاضعة للرقابة

٤. صياغة الاستنتاجات والتوصيات

٥. القيود والقيود على تدقيق تقنية المعلومات

مراحل تدقيق تقنية المعلومات

الخطوة ٤

الإبلاغ عن نتائج تدقيق تقنية المعلومات

الإبلاغ عن نتائج تدقيق تقنية المعلومات

المتابعة واستيفاء استنتاجات وتوصيات التدقيق

حالة دراسية

في عام ٢٠١٨ أطلق صندوق الخدمة الاجتماعية منصة **(عــون)** لتقديم الخدمات لمستحقي الدعم والإعانات الاجتماعية، والتي من خلالها يتم تقديم الطلبات وإظهار حالة استحقاق الدعم، والإشعار بالاستبعاد النهائي/ المؤقت، وتقديم الاعتراض على حالات عدم الاستحقاق/ مبلغ الدعم المستحق.

خلال فهم الموضوع تبين أن الشركة المصممة لمشروع المنصة هي لا تزال في علاقة تعاقدية مع الجهة بسبب عدم كفاية الموظفين المختصين لإدارة وتشغيل المنصة، وفي الأشهر الثلاثة الأخيرة أظهرت التقارير الداخلية ارتفاع في عدد الاعتراضات المرفوعة من قبل المستفيدين، كما أظهرت التعليقات على موقع الصندوق في منصات التواصل الاجتماعي تذمر العديد من المشاركين في تلك التعليقات من عدم وضوح آلية استحقاق الدعم، والتأخر في البت في الاعتراضات المقدمة.

تعليمات الحل

قم بصياغة هدف المراجعة، مع تحديد نطاق المراجعة المتوقع، والأسئلة الفرعية الممكنة؟

حدد إجراءات الفحص الأساسية التي يتم من خلالها الإجابة على أحد الأسئلة الفرعية

تعليمات حل التمرين:

التفكير ضمن المجموعة ١٥ د، المناقشة والحل ٢٠ د

شكراً لكم

الديوان العام للمحاسبة
General Court of Audit

المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة
ARABOSAI

تخطيط وتنفيذ ومتابعة عمليات الرقابة في بيئة العمل الإلكتروني

(الوحدة الثالثة)

الوحدة الثالثة: تخطيط وتنفيذ ومتابعة عمليات الرقابة في بيئة العمل الإلكتروني

هدف التعلم:

اكتساب مهارات جديدة في التخطيط لعمليات الرقابة في بيئة تقنية المعلومات

محاور الوحدة

- فهم بيئة تقنية المعلومات والتخطيط لمهمات الرقابة على تقنية المعلومات.
- تصميم عملية تقييم الرقابة على تقنية المعلومات
- أساليب جمع وتحليل البيانات في بيئة تقنية المعلومات
- التوثيق وجمع الأدلة في بيئة تقنية المعلومات
- متابعة نتائج الرقابة

مكونات الوحدة

- فهم بيئة تقنية المعلومات والتخطيط لمهمات الرقابة على تقنية المعلومات.
- تصميم عملية تدقيق الرقابة على تقنية المعلومات
- أساليب جمع وتحليل البيانات في بيئة تقنية المعلومات
- التوثيق وجمع الأدلة في بيئة تقنية المعلومات
- متابعة نتائج الرقابة

محاور الجلسة

- ماهية تدقيق تقنية المعلومات
- مراحل تدقيق تقنية المعلومات
- التخطيط لمهمات تدقيق تقنية المعلومات

ماهية تدقيق تقنية المعلومات

تدقيق تقنية المعلومات

هي فحص لجوانب استخدام المنظمة لتقنية المعلومات، بما في ذلك البنية التحتية لتقنية المعلومات والسياسات والإجراءات والتطبيقات واستخدام البيانات، كما تتضمن عمليات تدقيق تقنية المعلومات بانتظام تحليل الأنظمة والضوابط للتأكد من أنها تلبي احتياجات أعمال المنظمة دون الساس بالأمان والخصوصية والتكلفة وعناصر العمل الهامة الخرى.

وغالباً ما تتضمن عمليات تدقيق تقنية المعلومات أيضاً الحصول على تأكيد بشأن ما إذا كان تطوير أنظمة تقنية المعلومات وتنفيذها وصيانتها يلبي أهداف العمل، ويحمي أصول المعلومات، ويحافظ على سلمة البيانات. غالباً ما تتضمن عمليات تدقيق تقنية المعلومات تحديد حالات الانحراف عن المعايير، والتي تم تحديدها بناءً على نوع مهمة المراجعة (أداء، مالية، التزام)

ماهية تدقيق تقنية المعلومات

تدقيق تقنية المعلومات

تختلف عملية تدقيق تقنية المعلومات بناءً على أنواع عمليات المراجعة التي يتم إجراؤها، على سبيل المثال:

- في سياق المراجعة المالية، يمكن أن يكون تدقيق تقنية المعلومات على سبيل المثال فحصاً للضوابط العامة التي تضمن تشغيل أنظمة المعلومات التي تكمن وراء العمليات المالية للكيان، وفق ما هو موضح في بياتها المالية.
- في سياق تدقيق الأداء، يمكن أن يكون أحد الأمثلة على تدقيق تقنية المعلومات هو تحديد إلى أي مدى أدى اعتماد الجهة للتقنية الجديدة إلى تحقيق فوائد قابلة للقياس على مستوى الحوكمة ووفورات في التكاليف.
- في سياق تدقيق الالتزام، يمكن أن يكون تدقيق تقنية المعلومات على سبيل المثال فحصاً لفعالية أنظمة المعلومات التي تنتج تقارير الامتثال، مما يمكن الموظفين من إدارة عمليات الكيان والتحكم فيها.

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

الخطوة ٢

تصميم عملية تدقيق تقنية المعلومات

الخطوة ٣

إجراء عملية تدقيق تقنية المعلومات

الخطوة ٤

الإبلاغ عن نتائج تدقيق تقنية المعلومات

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة	التخطيط الاستراتيجي
	التخطيط الكلي أو السنوي
	التخطيط الجزئي أو على مستوى المنظمة.

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الاستراتيجي

إن الخطة الاستراتيجية للجهاز الأعلى للرقابة المالية والمحاسبة هي عبارة عن تنبؤ طويل المدى ٣ – ٥ سنوات لأهداف وغايات الرقابة، بما في ذلك أنظمة تقنية المعلومات والمنظمات ذات الصلة الخاضعة لسلطة الجهاز، ففي بعض الأجهزة العليا للرقابة، قد يتم تضمين قائمة فقط من مجالات تقنية المعلومات الجديدة والناشئة للتدقيق في خططهم الاستراتيجية، كما يمكن أن يشمل ذلك النظر في الأساليب الجديدة لتطوير النظام، أو الاستحواذ أو الحوسبة السحابية في القطاع العام، أو اعتماد تقنيات جديدة، مثل الذكاء الاصطناعي أو بلوكتشين.

توفر عملية التخطيط الاستراتيجي والخطة الاستراتيجية للجهاز الأعلى للرقابة الأسلوب والاتجاه لأهداف تدقيق تقنية المعلومات في الجهاز للمستقبل.

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الكلي أو السنوي

يتم إجراء المستوى الكلي لتخطيط المراجعة عادة على أساس دورة سنوية على مستوى الجهاز الأعلى للرقابة لاختيار مجالات المراجعة، يتم صياغة عملية لتحديد المجالات التي سيتم تدقيقها سنوياً مع الانتشار السريع لأنظمة تقنية المعلومات الحديثة عبر الحكومات ومحدودية الموارد المتاحة للأجهزة العليا للرقابة

سيكون النهج القائم على المخاطر تحديد الأولويات واختيار المواضيع المناسبة مناسبا. وبالإضافة إلى اعتبارات اختيار أنظمة تقنية المعلومات للمراجعة، عند اتخاذ قرار بشأن موضوعات المراجعة، يجب أيضاً مراعاة المعلومات الأخرى مثل النفقات الإجمالية لتقنية المعلومات، والاتصال بالكيانات الخارجية الأخرى، ونضج عمليات تقنية المعلومات والحوكمة. .

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط الكلي أو السنوي

التخطيط لعمليات المراجعة

مثال: خطوات تدقيق وفق نهج قائم على المخاطر

- تحديد مجتمع المراجعة الذي سيشمل قائمة بجميع الجهات أو الوحدات الخاضعة للرقابة التي تخضع لاختصاص الجهاز الأعلى للرقابة المالية والمحاسبة.
- وضع قائمة بنظم المعلومات المستخدمة في الجهة/ الوحدات الخاضعة للتدقيق.
- تحديد العوامل التي تؤثر على أهمية النظام للجهة للقيام بوظائفها وتقديم الخدمة.
- تخصيص وزن للعوامل الحرجة، يمكن القيام بذلك بالتشاور مع المنظمة الخاضعة للرقابة.
- تجميع المعلومات لجميع الأنظمة عبر جميع الجهات ذات الصلة، و بناءً على الدرجات التراكمية، ومن وضع قائمة للجهات في ترتيب حسب الأولوية للتدقيق.

إعداد خطة تدقيق سنوية تحدد الأولوية والنهج والجدول الزمني لعمليات تدقيق تقنية المعلومات.

يمكن تطبيق ذلك على فترات سنوية وبالتالي يمكن أن يكون ضمن خطة متكررة

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الجزئي أو على مستوى المنظمة.

يتضمن التخطيط الجزئي وضع خطة تدقيق مفصلة لمنظومة المراجعة، بدءً من تحديد أهداف المراجعة، وستساعد خطة المراجعة المدققين في إعداد برنامج تدقيق تقنية المعلومات، وستكون الخطوة الأساسية في تطوير برنامج تدقيق المعلومات هي الحصول على فهم واضح للمؤسسة وأنظمة تقنية المعلومات الخاصة بها.

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الجزئي أو على مستوى المنظمة.

- فهم الجهة محل التدقيق
- تقييم الضوابط العامة لتقنية المعلومات
- اعتبارات تخصيص الموارد والموظفين

مراحل تدقيق تقنية المعلومات

الخطوة ا

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الجزئي أو على مستوى المنظمة.

فهم الجهة محل التدقيق

لمعرفة المنظمة والعمليات التي يتطلبها تدقيق تقنية المعلومات يتم النظر إلى حد كبير إلى طبيعة المنظمة ومستوى التفاصيل التي يتم تنفيذ أعمال المراجعة فيها.

سيكون هناك اختلاف في عمليات تدقيق تقنية المعلومات، بناءً على نطاق ما يتم تدقيقه من نظام تقنية المعلومات.

يجب أن تشمل المعرفة بالمنظمة الأعمال والمخاطر المالية والمتأصلة في التي تواجه المنظمة أو أنظمة تقنية المعلومات الخاصة بها.

يجب أن يشمل أيضاً مدى اعتماد المنظمة على الاستعانة بمصادر خارجية لتدقيق أهدافها، وإلى أي مدى تم تخطيط عمليات الجهة في بيئة تقنية المعلومات.

يجب على المدقق استخدام هذه المعلومات في تحديد المشكلة المحتملة، وصياغة الأهداف وانطاق العمل، وأداء العمل، والنظر في إجراءات الإدارة التي يجب التفطن لها.

مراحل تدقيق تقنية المعلومات

الخطوة I

التخطيط لعملية تدقيق تقنية المعلومات

شكل2 : تخطيط نموذجي لنظام تقنية المعلومات في مؤسسة

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الجزئي أو على مستوى المنظمة.

فهم الجهة محل التدقيق

قبل الشروع في تقييم الضوابط في نظام المعلومات، يجب على المدققين تطوير فهم لهيكل النظام والبيانات الأساسية ومصادرها بغية تحديد أدوات وتقنيات المراجعة المطلوبة.

وبناءً على فهم مدققي تقنية المعلومات لنظام المعلومات والأنظمة الخاضعة للرقابة، قد يقررون نهجهم في تدقيق تقنية المعلومات

يمكن أن تشمل أنشطة المراجعة الأخرى التي يمكن أن تكون مفيدة في فهم الأنظمة الخاضعة للرقابة الآتي:

- رسم خرائط العمليات التجارية للجهة الخاضعة للرقابة
- تحديد تفاعل الكيان مع أقرانه أو البيئة الخارجية
- سرد الأنشطة التجارية التي تعتبر بالغة الأهمية لأهداف وغايات المنظمة الخاضعة للرقابة
- سرد جميع حلول تقنية المعلومات التي يستخدمها الكيان

مراحل تدقيق تقنية المعلومات

الخطوة ا

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الجزئي أو على مستوى المنظمة.

فهم الجهة محل التدقيق

يجب كذلك النظر إلى الأهمية النسبية أو الملاءمة والأهمية، ويجب تحديد قضايا تدقيق تقنية المعلومات ضمن الإطار العام للجهاز العلى للرقابة لتقرير سياسة الأهمية النسبية لتقرير المراجعة.

قد يختلف منظور الأهمية النسبية اعتماداً على طبيعة ارتباط تدقيق تقنية المعلومات.

يجب على المدقق النظر في الأهمية النسبية للأمر في سياق تقنية المعلومات والجوانب المالية وغير المالية، كطبيعة المنظمة أو النشاط.

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الجزئي أو على مستوى المنظمة.

تقييم الضوابط العامة لتقنية المعلومات

يجب على مدقق تقنية المعلومات تحديد ما إذا كان أي نقص في تقنية المعلومات يمكن أن يصبح جوهرياً.

يجب تقييم أهمية الضوابط العامة لتقنية المعلومات فيما يتعلق بتأثيرها على ضوابط التطبيق، بمعنى ما إذا كانت الضوابط التطبيق غير فعّالة أيضاً.

مراحل تدقيق تقنية المعلومات

الخطوة ١

التخطيط لعملية تدقيق تقنية المعلومات

التخطيط لعمليات المراجعة

التخطيط الجزئي أو على مستوى المنظمة.

اعتبارات تخصيص الموارد والموظفين

يتطلب تدقيق تقنية المعلومات تخصيصاً محدداً للموارد، خاصة الموظفين الذين هم على دراية جيدة بأنظمة وعمليات وآليات تقنية النموذجية التي تحكم التنفيذ الناجح لتقنية المعلومات.

بالإضافة إلى موارد الموظفين المناسبة، الميزانية المناسبة والبنية التحتية الممكنة، وأي متطلبات أخرى يتم تحديدها يجب توفيرها أيضاً.

يجب تحديد الجدول الزمني للمراجعة، إن أمكن، بالتشاور مع المنظمة الخاضعة للرقابة.

قد تضمن الأجهزة العليا للرقابة أن فريق المراجعة يتكون من أعضاء يتمتعون مجتمعين بالكفاءة لإجراء عمليات تدقيق تقنية المعلومات لتحقيق الأهداف المرجوة.

يمكن اكتساب المعرفة والمهارات والكفاءات اللازمة من خلال مزيج من بناء القدرات، مثل التدريب أو زياد الخبرة أثناء العمل؛ تجنيد؛ ومشاركة الوارد الخارجية، وفقاً للخطة الاستراتيجية للجهاز.

شكراً لكم

الديوان العام للمحاسبة
General Court of Audit

العنصر البشري خط الدفاع الأول

الديوان العام للمحاسبة

المركز السعودي للمراجعة المالية والرقابة على الأداء

إدارة الأمـن السيبرانـي

مكونات العرض

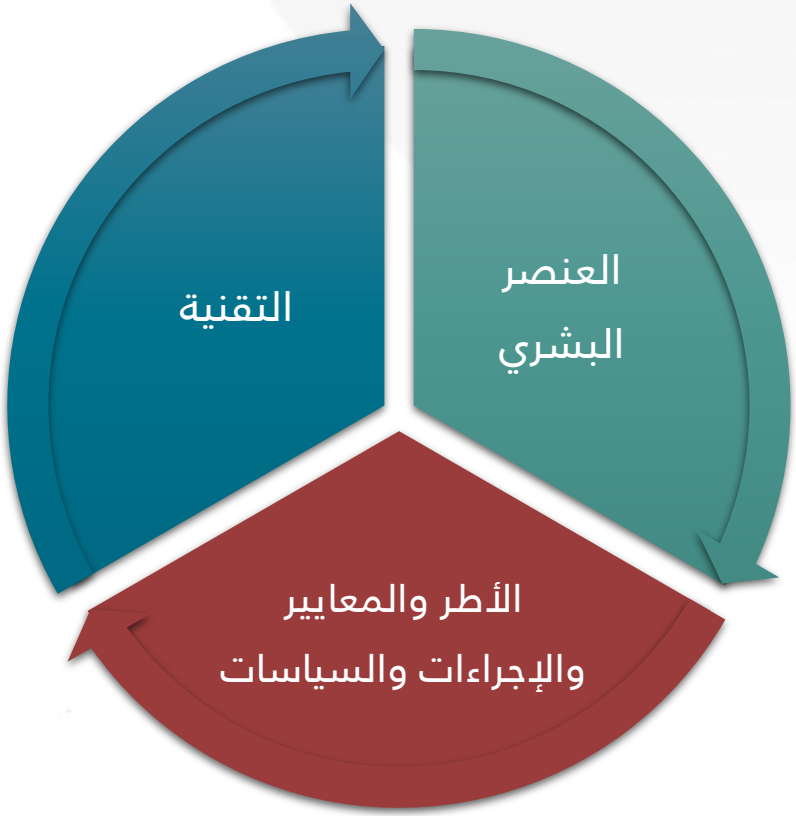
- الأمن السيبراني
- الهجمات الإلكترونية
- سرية البيانات
- الأمن المادي
- وسائل التخزين
- أمان الأجهزة المحمولة
- وسائل التواصل الاجتماعي
- التصفح الآمن
- أمان العمل عن بعد
- النسخ الاحتياطي
- كلمة المرور
- التحديثات

الأمن السيبراني

- **تعريف الأمن السيبراني**

حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع، لضمان استمرارية وسلامة عمل المنظومة.

عناصر الأمن السيبراني

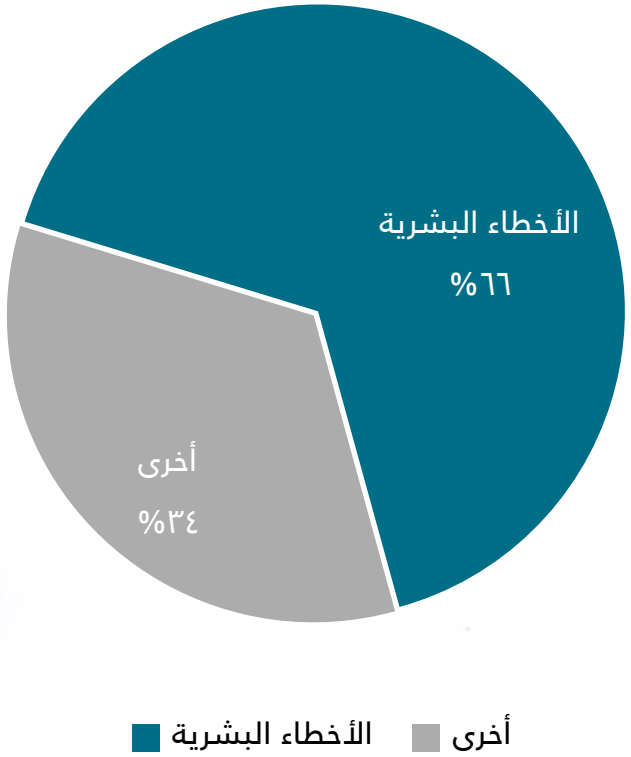


يمثل العنصر البشري ركيزة أساسية في الأمن السيبراني

العنصر البشري

- العنصر البشري هو أضعف عناصر الأمن السيبراني وأكثرها خطورة

نسبة الحوادث التي ساهمت فيها الأخطاء البشرية تعادل أكثر من ٦٦%



أمثلة لحوادث بسبب خطأ بشري

في (٢٠٠٨) تعرضت أحد شبكات القوات المسلحة لسرقة بياناتها الحرجة بسبب ذاكرة فلاش تحوي برمجيات خبيثة

في (٢٠١٧) سرقت معلومات أكثر من (١٤٠) مليون عميل من أحد الشركات الائتمانية

الهجمات السيبرانية

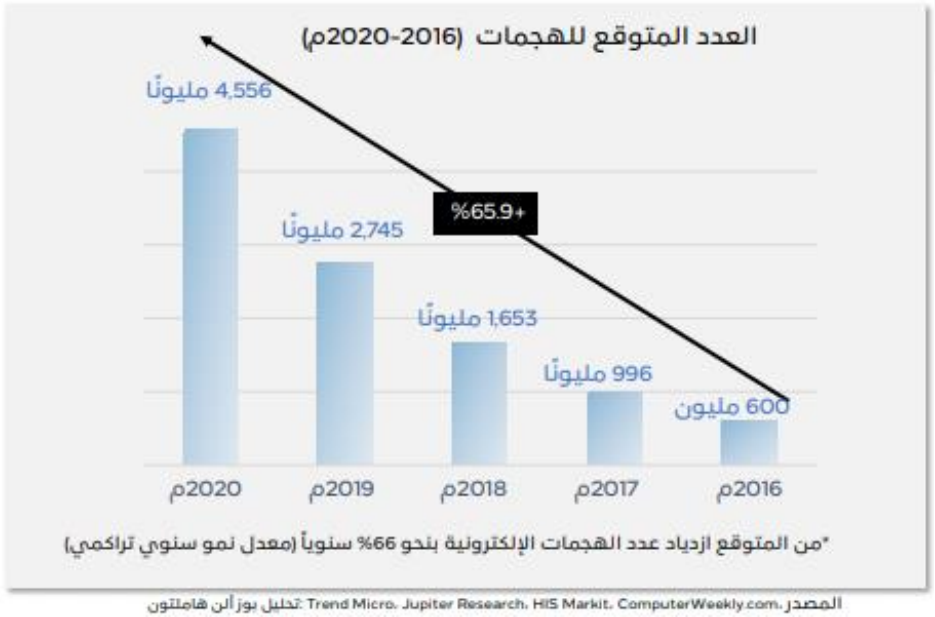
تعريف الهجمات السيبرانية:

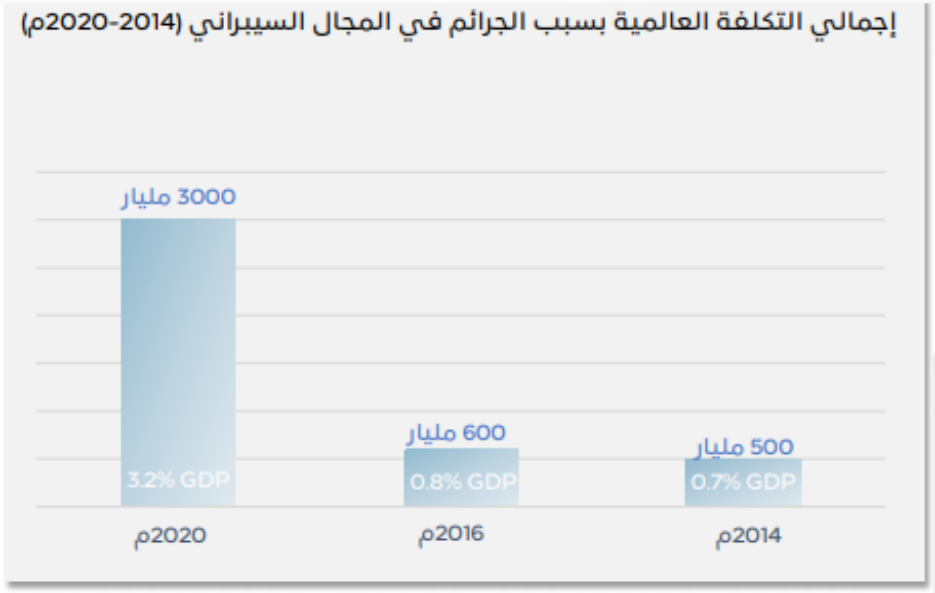
هي محاولة متعمدة يقوم بها فرد أو منظمة، بهدف اختراق نظام المعلومات الخاص بفرد أو مؤسسة أخرى، وغالبًا ما يسعى من ينفذ تلك الهجمات إلى الحصول على فائدة جراء الهجوم على الطرف الآخر وتعطيل شبكته.

أهداف الهجمات السيبرانية:

- أهداف تخريبية وتدميرية للأنظمة والبنية التحتية.
- أهداف سياسية مثل: الحرب السيبرانية والتجسس السيبراني.
- أهداف شخصية مثل: سرقة المعلومات الشخصية وانتحال الهوية.
- أهداف تجارية ومالية.

- أصبح الفضاء السيبراني مصدر تهديد عالي الخطورة لاقتصاد وأمن الدول والمنظمات.
- ويزداد حجم المخاطر المتعلقة بالأمن السيبراني بشكل مستمر.
- **أثبتت الدراسات بأن أكثر من نصف الحوادث السيبرانية في المنظمات حدثت بسبب الموظفين.**





أمثلة على حوادث سيبرانية حول العالم

في (٢٠١٦) تمت سرقة (٨١) مليون دولار من خلال التلاعب بأحد أنظمة المعاملات

في (٢٠١٨) تعرض أحد الفنادق العالمية لسرقة معلومات أكثر من (٥٠٠) مليون عميل

في (٢٠٢٠) تعرضت شركة Software AG الألمانية لهجمة أدت إلى توقف النظام الداخلي، ثم سرقة البيانات، مما أدى إلى دفع (٢٠) مليون دولار لاستعادة البيانات

في (٢٠٢١) دفعت شركة لحوم برازيلية (١١) مليون دولار لاستعادة بياناتها بعد أن سرقت بواسطة فيروس الفدية

في (٢٠٢١) دفعت الشركة التقنية Acer (٥٠) مليون دولار لاستعادة بياناتها بعد أن سرقت بواسطة فيروس الفدية

بعض المفاهيم الخاطئة

الاعتقاد الخاطئ بأن أمن المعلومات وحماية البيانات مسؤولية متخصصي التقنية والأمن السيبراني فقط

تساهل المستخدم واعتقاده بأنه لن يحدث أي اختراق من خلاله

الاعتقاد الخاطئ بأن الإبلاغ عن الأنشطة المشبوهة ليست من مسؤوليتي وأن هناك أشخاص اخرين سوف يبلغون عنها

الاعتقاد الخاطئ بأنه لن يكون هناك اختراق لجهازك بسبب عدم وجود أي معلومات سرية مخزنة لديك

الهجمات الإلكترونية

أساليب الهجمات الإلكترونية

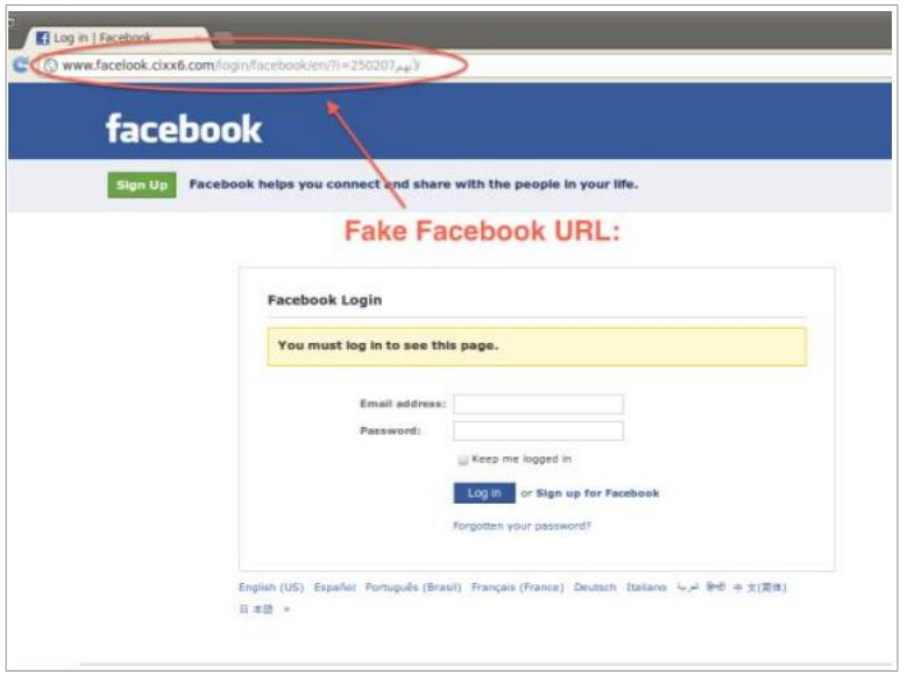
- **التصيد الاحتيالي والهندسة الاجتماعية**

هو انتحال المخترق أو المحتال لهوية شخص أو جهة رسمية موثوقة مثل خدمة العملاء لدى شركة ما، وذلك لسرقة بيانات المستخدم الشخصية.

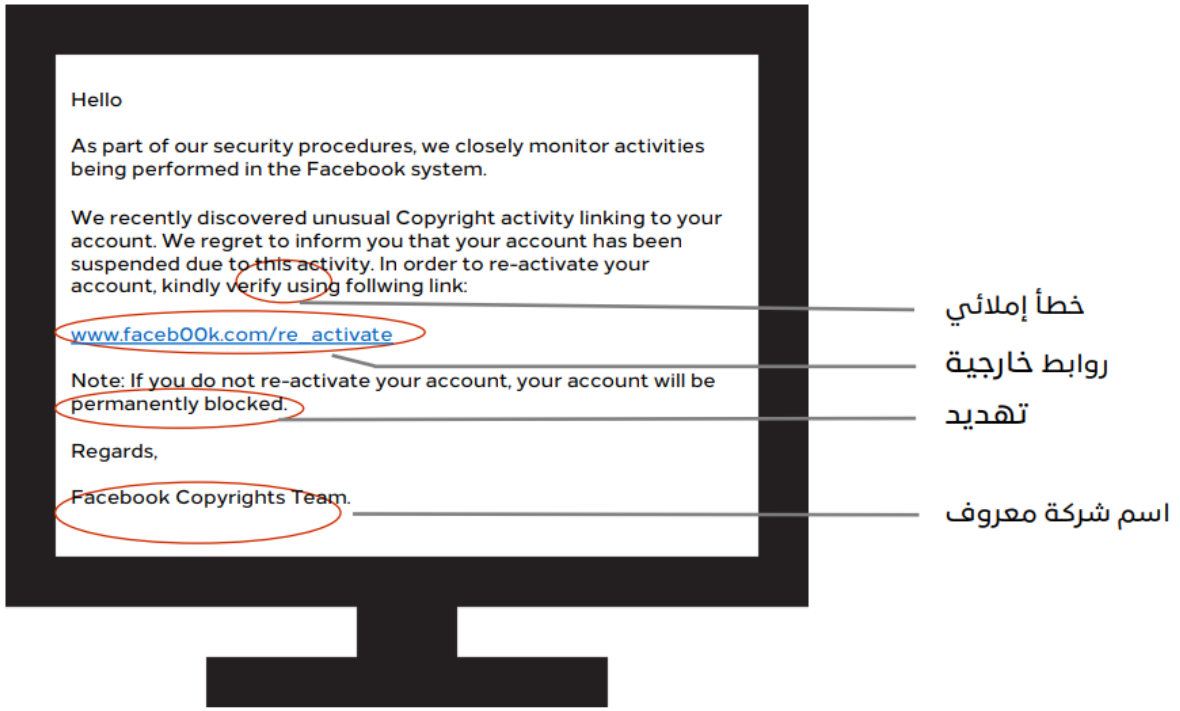
- **تنصت الكتف**

هو المصطلح المستخدم لوصف شخص يراقب شاشة الكمبيوتر أو الجهاز المحمول الخاص بشخص آخر للحصول على معلومات حساسة، يمكن إجراءه ببساطة عن طريق النظر من فوق كتف شخص ما.

التعرف على التصيد الاحتيالي



موقع وهمي صمم لسرقة اسم المستخدم وكلمة المرور



ايميل وهمي صمم ليخدع المستخدم ويجعله ينقر على الرابط المرفق

البرمجيات الخبيثة

- الفيروسات (Viruses)

وهي برامج خبيثة تصيب الأنظمة والبرامج والملفات الموجودة على الجهاز مما قد يؤدي إلى تلف وسرقة البيانات بالإضافة إلى خلل في عمل البرامج والأنظمة المصابة.

- الديدان (Worms)

وهي برامج خبيثة تعمل ذاتياً وتكون قادرة على استنساخ نفسها إلى الحواسيب الأخرى عبر الشبكة بسرعة وبدون تدخل المستخدم، وذلك بالاعتماد على أحد الثغرات الأمنية الموجودة في تلك الشبكة أو أحد البرامج التي تعمل بها.

- التجسس (SPY)

وهي برامج خبيثة تقوم بالتجسس على المستخدم ومراقبته وجمع معلومات عنه وسرقة بياناته، وإرسال هذه المعلومات لجهة أخرى من دون علم المستخدم.

البرمجيات الخبيثة

- **حصان طروادة (Trojan Horse)**

وهي برامج حاسوبية تظهر وكأنها تطبيقات مفيدة، ولكنها في الواقع برمجيات خبيثة تعمل على سرقة البيانات وإتلاف الجهاز بدون علم المستخدم، غالباً ما تصيب المستخدم بسبب تنزيل برامج مجانية أو غير معروفة أو غير مصرح بها.

- **فيروس الفدية (Ransomware)**

وهو نوع من البرمجيات الخبيثة يقوم بتشفير وحجب كافة الملفات والبيانات في جهاز المستخدم، وبالتالي يجعل جهاز الحاسب أو ملفاته غير صالحين للاستخدام حتى يتم دفع مبلغ معين من المال للمخترق.

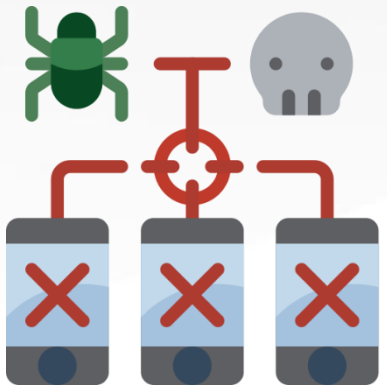
المخاطر المتعلقة بالهجمات الإلكترونية

المخاطر

- سرقة الهوية
- سرقة واستبدال أو حذف المعلومات الشخصية
- إصابة الجهاز بالبرمجيات الخبيثة
- الاستخدام الغير المصرح لجهاز أو نظام
- فقدان الخصوصية والتي تؤدي إلى سرقة المعلومات

طرق انتشار البرمجيات الخبيثة

- وسائل التخزين القابلة للإزالة : USBs و CDs
- مرفقات البريد الإلكتروني
- مواقع الويب التي تحتوي على برامج خبيثة
- مضمنة داخل بعض البرامج والتطبيقات
- تبادل الملفات
- البرامج التي تم قرصنتها
- وسائل التواصل الاجتماعي



سرية البيانات

تمثيل البيانات والمعلومات

- **البيانات:** هي مجموعة من الحروف، أو الكلمات، أو الأرقام، أو الرموز، أو الصور (الخام) المتعلقة بموضوع معين، مثل بيانات الموظفين (الأسماء – الأرقام الوظيفية – المهن – الصور) بدون ترتيب، وينتج عن هذه البيانات بعد المعالجة ما يطلق عليه مصطلح معلومات.

- وتكون البيانات والمعلومات مخزنة أو متوفرة في عدد من النماذج، مثل:

أنظمة تصنيف البيانات

عام
Public

البيانات التي يمكن الإفصاح عنها بشكل عام كالمواد التسويقية وبيانات التواصل

داخلي
Internal

بيانات داخلية يمكن تبادلها داخل المنظمة ولا يمكن الإفصاح عنها خارجه، كالمخططات التنظيمية والوثائق الداخلية

سري
Confidential

بيانات حساسة يمنع الإفصاح عنها وفي حال تم تسريبها يمكن أن تؤثر بشكل سلبي على نشاط المنظمة

مقيد
Restricted

بيانات المنظمة الحساسة للغاية والتي في حال تعرضها للسرقة قد تتعرض المنظمة للمخاطر المالية والقانونية

طرق تسريب البيانات

سرقة الجهاز الشخصي أو القرص الصلب أو الفلاش **USB**

إرسال رسالة بريد إلكتروني إلى مستخدم غير مقصود

مشاركة المعلومات مع شخص غير مصرح به

أثار تسريب البيانات السرية

01

الكشف عن معلومات المنظمة الحساسة مما يؤدي لإضرار بسمعة المنظمة أو الدولة

02

فقدان أو تلف البيانات الحساسة

03

دعاوى قضائية وعقوبات تنظيمية

04

سرقة الهوية

الحفاظ على سرية البيانات

يجب الحفاظ على سرية ونزاهة البيانات السرية والمقيدة من خلال:

الحرص على تخزين البيانات باستخدام طرق آمنة وموثوقة

الحرص على مشاركة ونقل البيانات السرية بشكل آمن بواسطة الطرق المصرحة

التأكد من التخلص من البيانات السرية الورقية والإلكترونية بطرق آمنة وصحيحة

الأمن المادي

الأمن المادي

- **تعريف الأمن المادي:**

حماية الأصول المعلوماتية والتقنية للمنظمة من الوصول المادي الغير مصرح به والفقدان والسرقة والتخريب.

- **سياسة المكتب النظيف:**

هدفها هو حماية المعلومات والبيانات الحساسة الموجودة على سطح مكتب الموظف، ومن ذلك:

- تفعيل شاشة توقف جهاز الكمبيوتر عند الخروج من المكتب.
- إزالة جميع الوثائق والملفات من المكتب ووضعها في خزائن آمنة ومحكمة الإغلاق.

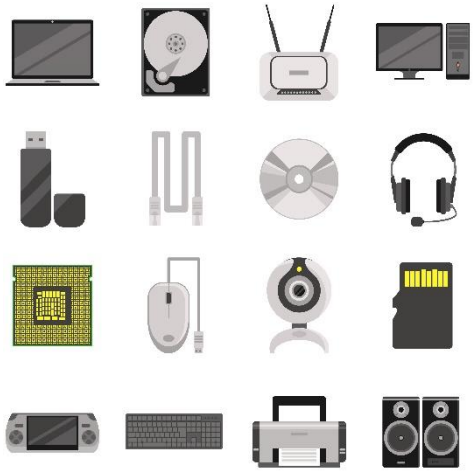
إتلاف الأصول

الأصول الورقية

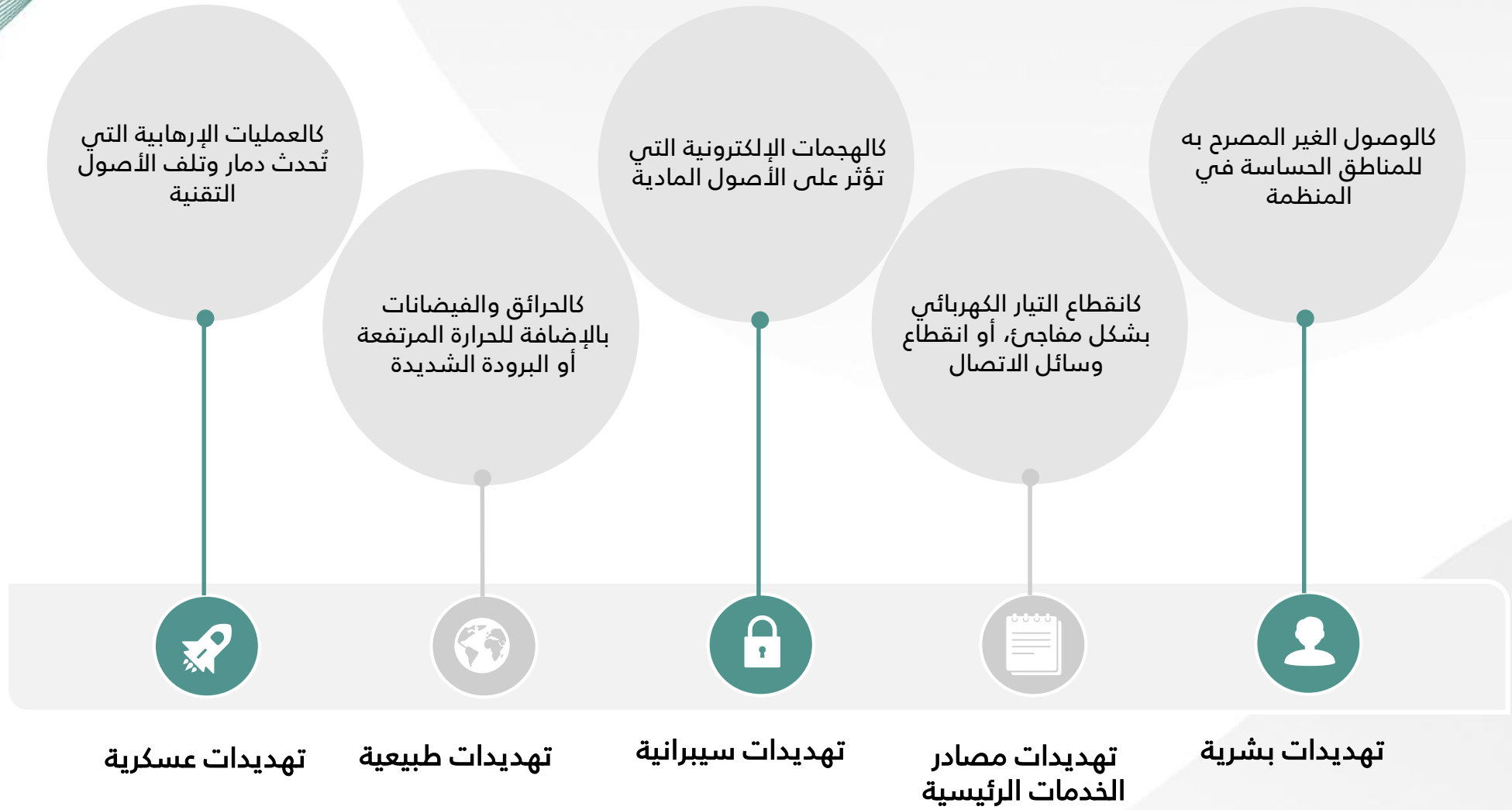
استخدام قطاعة الورق

الأصول التقنية

تسليمها لإدارة تقنية المعلومات للتخلص منها بأمان



تهديدات الأمن المادي



وسائل التخزين والطباعة

حماية وسائط التخزين

حفظها في مكان آمن، والحرص عليها من السرقة والتلف

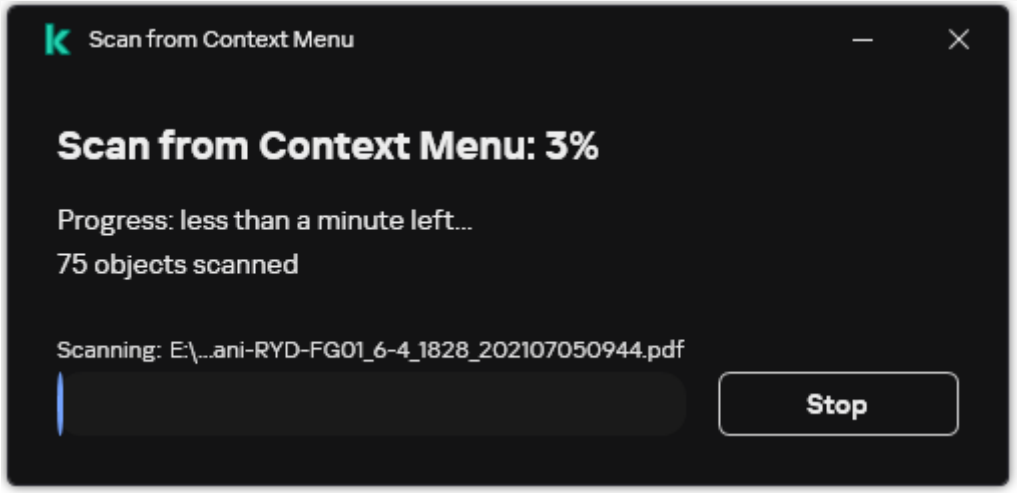
التأكد من خلوها من الفيروسات، وذلك بفحصها قبل استخدامها، وقبل نقل البيانات منها وإليها

التأكد من كونها مشفرة، لحماية سرية البيانات المخزنة فيها

إخراجها بشكل صحيح قبل فصلها من الجهاز لحماية سلامة البيانات

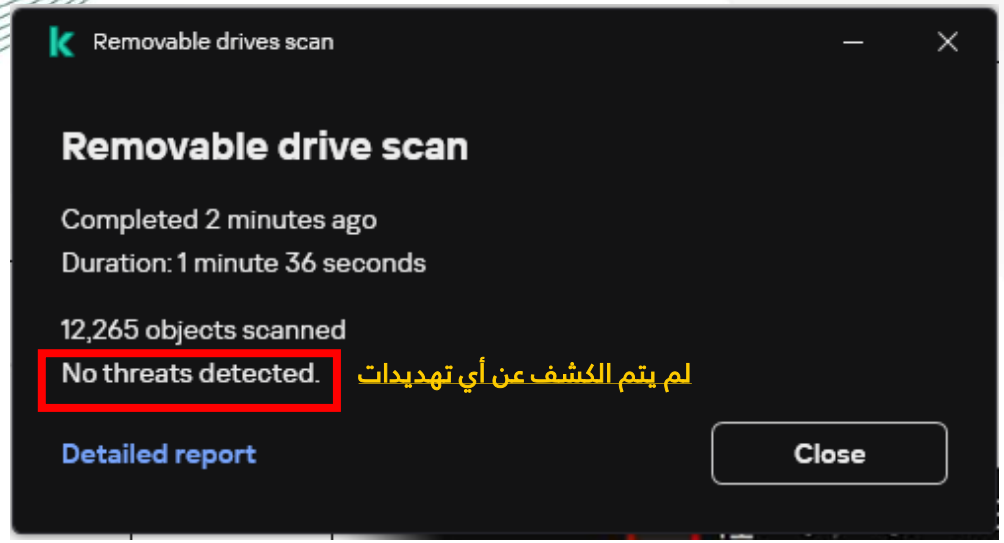
طلب الصلاحيات اللازمة من إدارة الأمن السيبراني قبل استخدام وسائط التخزين المتنقلة مثل ذاكرة الفلاش USB

فحص وسائط التخزين قبل استخدامها



١. عند توصيل ذاكرة الفلاش في الجهاز سيبدأ الفحص تلقائياً

للذاكرة، ويجب عليك الانتظار حتى يكتمل الفحص

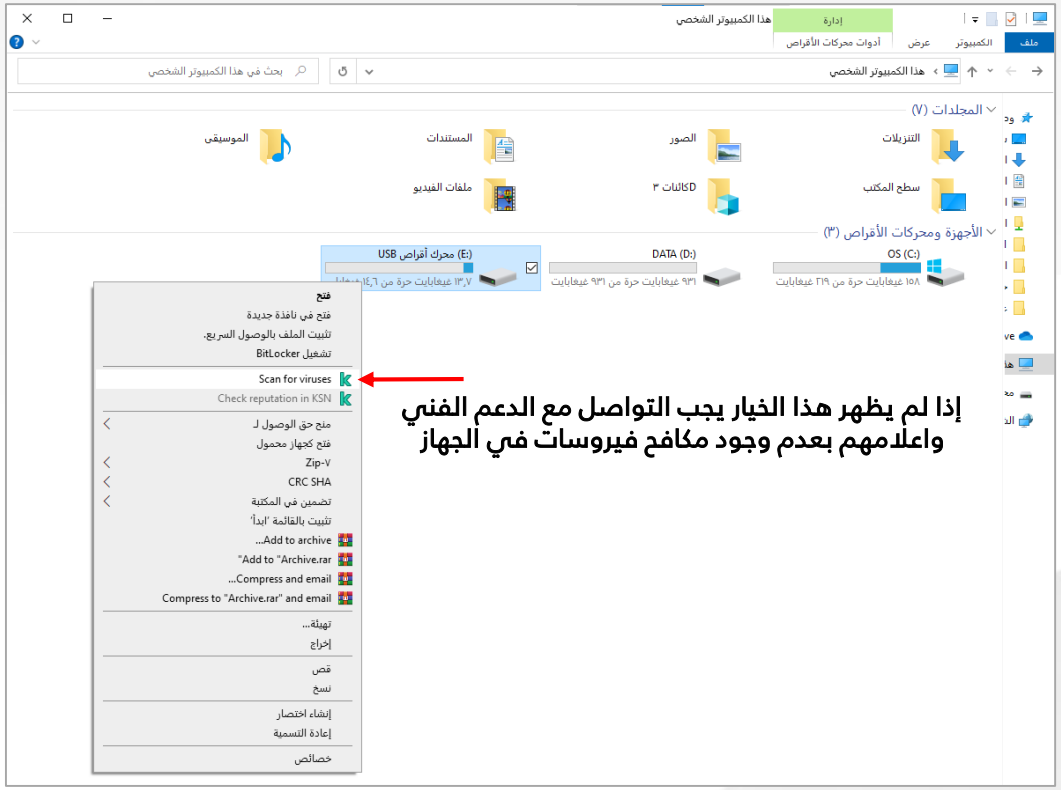


٢. بعد اكتمال الفحص تأكد من ظهور الجملة الموضحة، بعد ذلك

ستتمكن من استخدام الذاكرة بأمان

فحص وسائط التخزين قبل استخدامها

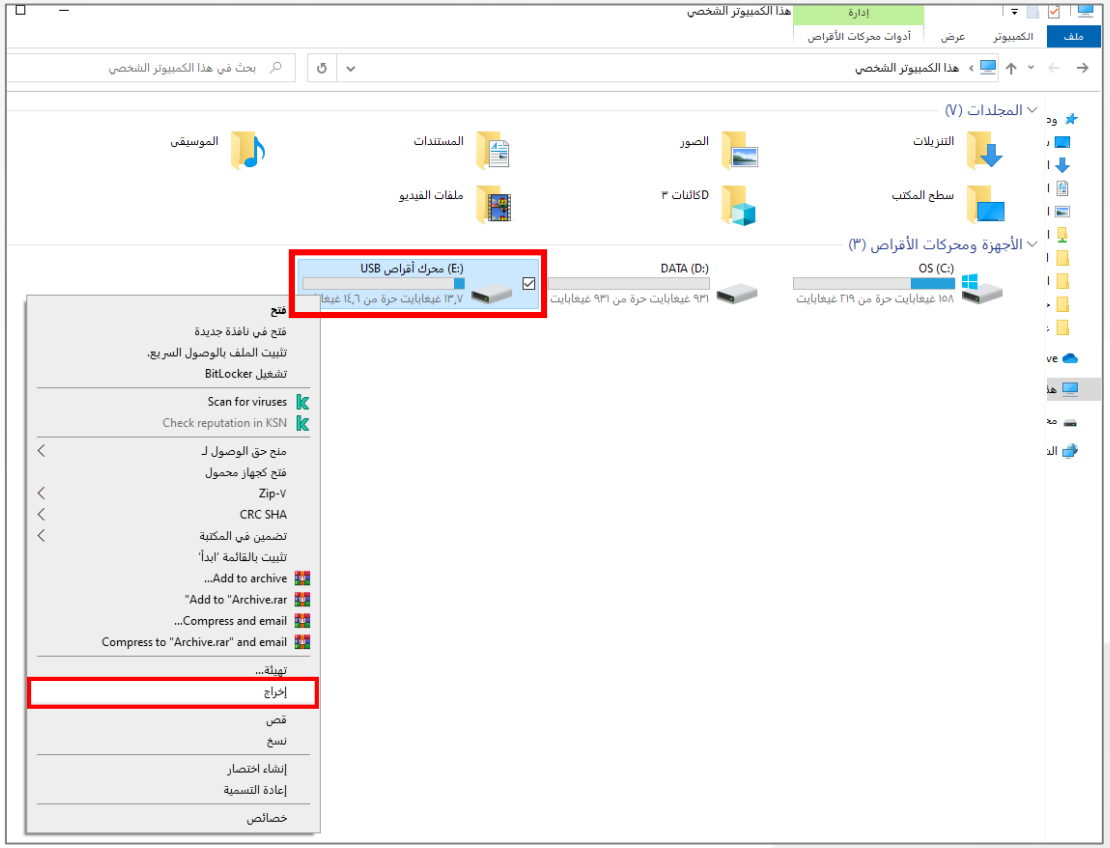
في حال لم تظهر لك نافذة الفحص يجب أن تقوم بعمل الفحص بالطريقة التالية



١. فتح ملف الكمبيوتر الشخصي
٢. النقر على الزر الأيمن في الماوس على ملف الذاكرة المدخلة
٣. الضغط على scan for viruses

٤. سيبدأ الفحص مباشرة، وعند اكتمال الفحص تأكد من ظهور الجملة الموضحة في الصورة، ثم يمكنك استخدام الذاكرة

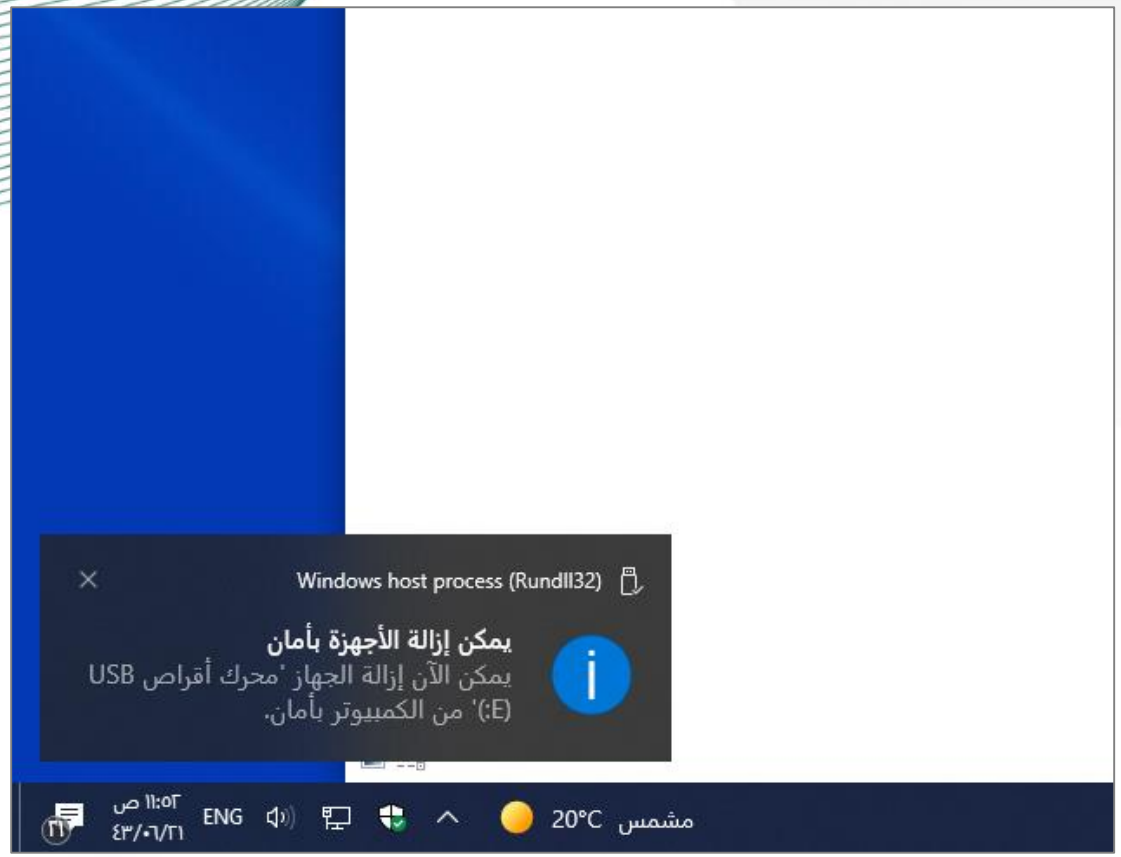
كيف يتم إخراج وسائط التخزين بأمان؟



١- فتح ملف الكمبيوتر الشخصي

٢- النقر بالزر الأيمن في الماوس على ملف الذاكرة المدخلة

٣- اختيار خيار "إخراج" من القائمة



٤- عند ظهور الرسالة الموضحة في الصورة يمكنك بعدها إزالة ذاكرة الفلاش من الجهاز

أمن وسائل التواصل الاجتماعي

حماية وسائل التواصل الاجتماعي ا

- استخدم كلمات مرور قوية، لا تحتوي على معلومات شخصية أو أرقام وحروف متسلسلة، واحرص على تغييرها باستمرار.
- تجنب نشر المعلومات الشخصية أو الوثائق والمعلومات المتعلقة بالمنظمة.
- تجنب فتح الروابط أو الرسائل المشبوهة، حتى لو نشرت من قبل شخص أو جهة موثوقة.
- استخدم كلمة مرور مختلفة لكل حساب في وسائل التواصل الاجتماعي.

حماية وسائل التواصل الاجتماعي ٢

- تجنب استخدام شبكات الانترنت العامة الغير آمنة.
- تجاهل التفاعل مع أي رسالة تطلب تغيير كلمة المرور بدون طلب مسبق منك.
- تجنب الإفصاح عن أي معلومات أو بيانات تخص المنظمة سواء بشكل شخصي أو عن طريق وسائل التواصل الاجتماعي.
- تجنب استخدام بريد الديون لأغراض شخصية مثل التسجيل في المواقع والتطبيقات.
- تجنب نشر هويات الدخول في وسائل التواصل الاجتماعي.

التصفح الآمن

أفضل ممارسات التصفح الآمن

استخدم متصفح آمن، واحرص على تحديثه باستمرار

استخدم جدار حماية، وبرامج قوية لمكافحة الفيروسات، وتأكد من تحديثها باستمرار

تأكد من صحة وأمان روابط المواقع والتطبيقات قبل فتحها

تأكد بأن نسخة نظام التشغيل أصلية ومحدثه

تجنب الدخول أو ادخال معلومات شخصية أو سرية في المواقع المشبوهة

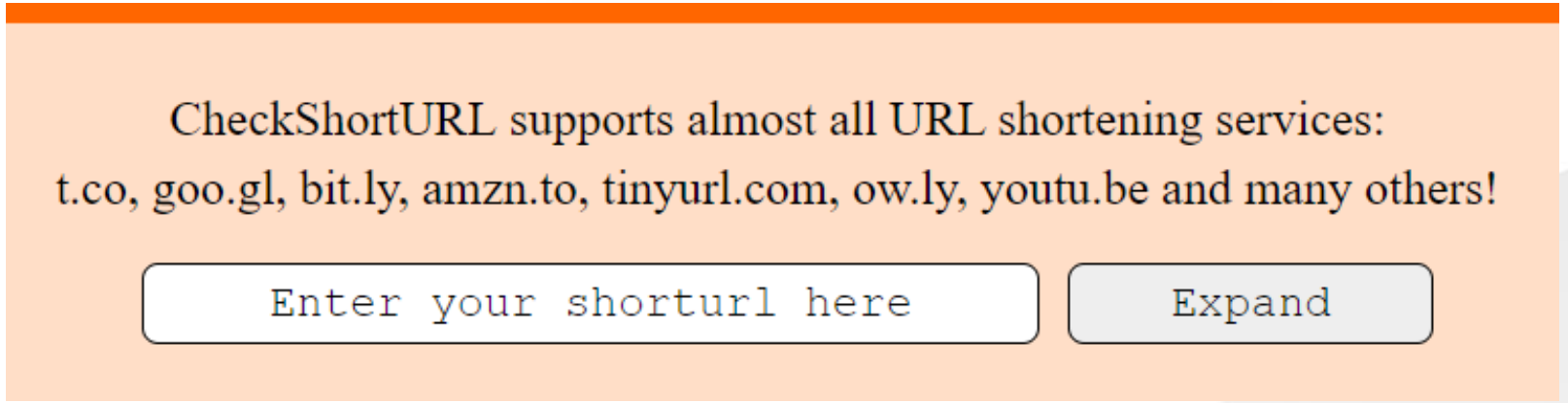
تأكد من أن الموقع يستخدم https وليس http

الروابط

- قبل استخدام الرابط يجب التأكد من صحته ومن أمانه، عبر اتباع الخطوات التالية:

❑ **أولاً:** يتم استخدام الروابط المختصرة بشكل كبير عبر الانترنت لذلك يجب التحقق من الرابط الأصلي ويمكن ذلك

عن طريق العديد من المواقع التي تظهر الرابط الأصلي قبل الاختصار مثل موقع: www.checkshorturl.com



الروابط

- **ثانياً:** التأكد من صحة كتابة الرابط، فالعديد من المواقع المشبوهة تستخدم روابط مقاربة ومشابهة لروابط مواقع موثوقة، ولكنها في الواقع مواقع مليئة بالثغرات، وتستخدم لخداع المستخدمين لسرقة بياناتهم ومعلوماتهم،

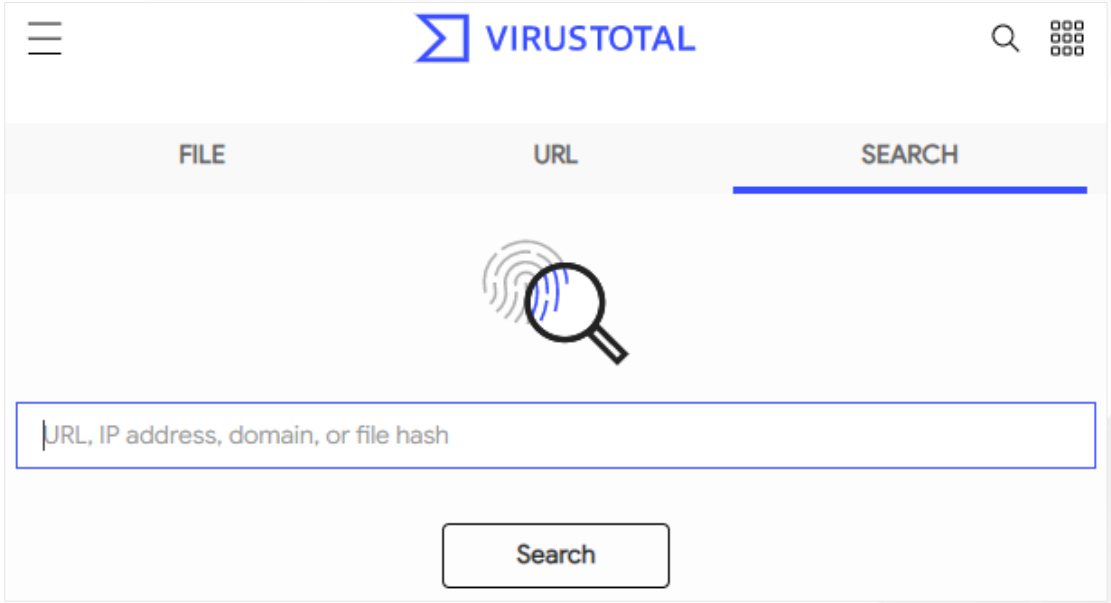
مثال توضيحي:

- **الرابط الأصلي لموقع فيسبوك -> www.facebook.com**
- **الرابط المزيف لموقع فيسبوك -> www.faceb00k.com**

كما هو موضح فقد تم التلاعب بالحروف لذلك تغير الرابط تماماً، وقد يتم التلاعب بالرموز والأرقام وأسماء النطاقات

الروابط

❑ **ثالثاً:** التأكد من أمان الرابط ويتم ذلك عبر فحص الرابط بواسطة المواقع المختصة بفحص الروابط والعناوين، مثل موقع: www.virustotal.com



أمان العمل عن بعد

العمل عن بعد

- تشهد المملكة اليوم تحولاً تاريخياً واسع النطاق باستخدام الفضاء السيبراني وما يوفره من إمكانيات للعمل عن بعد، ما يستوجب علينا جميعاً التكاتف لرفع جاهزية العمل عن بعد في المنظمة، واستخدام أفضل الممارسات الأمنية التي من شأنها تحقيق استمرارية أعمال المنظمة وحماية أصولها من المخاطر السيبرانية، وتحقيق الاستفادة المثلى من هذه التقنيات مع تجنب مخاطرها.

- كشف تقرير عالمي بأن 80% من المؤسسات تعرضت لهجمات إلكترونية نتيجة تأدية الموظفين أعمالهم عن بعد.

تحصين الحاسب الشخصي أثناء العمل عن بعد

نظام التشغيل

- استخدم برامج وأنظمة تشغيل أصلية، وتأكد من تحديثها بشكل دوري.

مكافحة الفيروسات

- فعل خواص الحماية ومكافحة الفيروسات في جهازك، مثل برامج الحماية الشاملة التي تحتوي على جدار حماية وبرنامج قوي لمكافحة الفيروسات، واحرص على تحديثهم.

خدمات المشاركة

- أطفئ خواص المشاركة الشبكية وخدمات الاتصالات الغير ضرورية، مثل NFC و Bluetooth.

تشفير الأقراص

- احرص على تشفير الأقراص الداخلية لجهازك لحماية البيانات في حال سرقته.

الأمن المادي

- احرص على وضع أجهزة العمل عن بعد في أماكن آمنة ومحمية وحافظ عليها من السرقة والضياع والاتلاف والوصول غير المصرح به.

أمان شبكة العمل عن بعد

خطوات تحصين الشبكة

- فعل الاتصالات اللاسلكية المشفرة من خلال تفعيل خاصية WPA3، أو WPA2
- غير اسم الراوتر لمنع المخترقين من التعرف على نوع وموديل الراوتر
- غير كلمة سر الراوتر المصنعية لكلمة سر قوية
- احرص على تحميل تحديثات المصنع للراوتر المنزلي بصفة دورية
- تجنب استخدام الشبكات أو الأجهزة العامة خلال العمل عن بعد

حماية البيانات خلال العمل عن بعد

- تشفير الملفات التي تحتوي على بيانات مقيدة وسرية أو ذات أهمية عالية.
- عدم تخزين كلمات السر في الهاتف أو الكمبيوتر أو مشاركتها مع الآخرين.
- الحرص على النسخ الاحتياطي باستمرار للبيانات المهمة والسرية.
- تحويل الأقراص الصلبة للأجهزة القديمة إلى "غير قابل للقراءة".
- الحرص على إغلاق الجهاز عند الانتهاء من العمل.
- استخدام أداة لحذف البيانات بشكل آمن وكامل.
- الحرص على تحميل نظام وتطبيقات اصلية وتحديثها باستمرار.

الاجتماعات الافتراضية

- الحرص على التسجيل باستخدام بريد المنظمة الأصلي لحضور الاجتماعات الرسمية والمرتبطة بالعمل.
- الحرص على تحميل تطبيقات الاجتماعات الأصلية من مصدرها الأصلي وتحديثها باستمرار.
- وضع كلمة مرور قوية لحسابك في تطبيقات ومواقع الاجتماعات الافتراضية وعدم مشاركتها.
- استخدام ميزة المصادقة الثنائية.
- إعداد اعدادات الأمان والحماية عند انشاء الحساب وعند انشاء جلسة اجتماع.
- عدم استخدام وسائل التواصل الاجتماعي لمشاركة روابط الاجتماعات ومشاركتها عبر برامج المشاركة المصرحة من المنظمة مثل البريد الرسمي.
- وضع كلمة مرور للاجتماعات المهمة وعالية السرية.
- تفعيل ميزة "غرفة الانتظار" للتحكم والتأكد من الأشخاص الحاضرين للاجتماع.

أمان الأجهزة المحمولة

تهديدات الأجهزة المحمولة

- التطبيقات ومواقع الويب الضارة
- برامج طلب الفدية على الأجهزة المحمولة
- التصيد الاحتيالي والهندسة الاجتماعي
- الروابط الضارة التي تنتشر عبر وسائل التواصل الاجتماعي
- هجمات الوسيط
- كسر الحماية
- برامج التجسس

حماية الأجهزة المحمولة

- تأكد من اغلاق هاتفك بعد الانتهاء من استخدامه
- أنشئ كلمة مرور قوية لهاتفك وتطبيقاتك
- الحذر من الرسائل النصية وخصوصا الاحتيالية
- تأكد من تحميل التطبيقات والبرامج من المصادر الامنة والموثوقة
- حافظ على تحديث نظام التشغيل والتطبيقات
- سجل الخروج من المواقع بعد أي عملية دفع
- أوقف تشغيل شبكة Wi-Fi و Bluetooth عندما لا تكون قيد الاستخدام
- استخدم تطبيق مكافحة فيروسات محدث

التحديثات

التحديثات

يجب التأكد بأن نظام التشغيل والمتصفحات والبرامج محدثة بأحدث النسخ

أولاً

تجنب فصل سلك الشبكة من جهازك، وذلك لاستقبال التحديثات الدورية من تقنية المعلومات

ثانياً

تجنب إيقاف تشغيل الجهاز، وتأكد من تأمين الجهاز بدلاً من ذلك

ثالثاً

وافق مباشرة على النوافذ التي تطلب إجراء تحديث للبرمجيات وأنظمة التشغيل

رابعاً

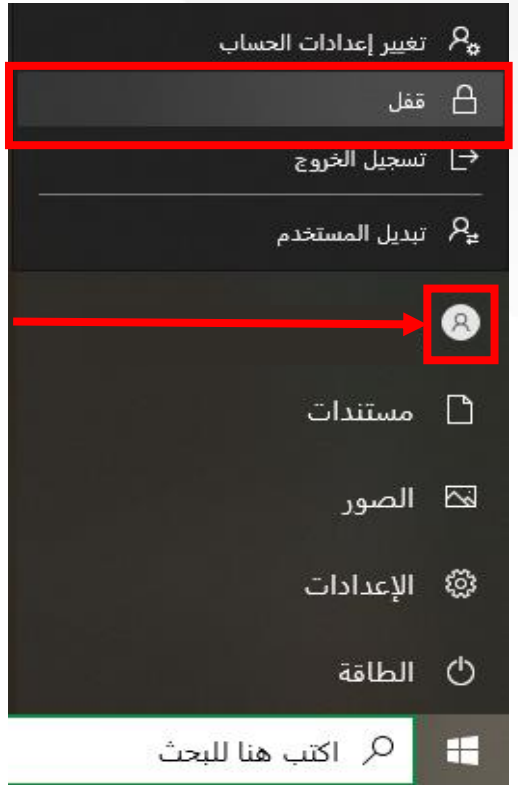
تواصل مع الدعم الفني إذا واجهتك مشكلة أو تعذر عليك معرفة طريقة التحديث

سلك منفذ الشبكة
"كابل الاتصال بالإنترنت"

جميع أجهزة العمل في المنظمة (الكمبيوتر واللاب توب) يجب أن تكون مرتبطة بالشبكة بواسط سلك منفذ الإنترنت، ولا يجب فصله أبدا لأنه بواسطته يتم تحديث الأجهزة والبرامج وتنزيل مكافحات الفيروسات

كيفية قفل الجهاز من دون إيقاف تشغيله؟

١. النقر على زر البدء



٢. النقر على الصورة الشخصية

٣. اختيار قفل

النسخ الاحتياطي

النسخ الاحتياطي

- قد تفشل الأنظمة وأجهزة الكمبيوتر بشكل مفاجئ وقد تفقد السجلات والنظم ومنتجات العمل بشكل لا رجعة فيه إذا تم تخزينها فقط على تلك الأنظمة وأجهزة الكمبيوتر، لذا تكمن أهمية النسخ الاحتياطي لجميع البيانات المهمة.

- **أهمية النسخ الاحتياطي:**

السماح باستعادة البيانات عند الحاجة في حالة حدوث كارثة أو فشل في النظام.

النسخ الاحتياطي

- يجب على كافة الموظفين أخذ نسخ احتياطية للملفات والبيانات الهامة بوضعها في مجلدات المشاركة في المنظمة، بدلاً من الاقتصار على تخزينها في أجهزة الموظفين

لماذا؟

لأن النسخ الاحتياطي مطبق على مجلدات المشاركة، فيمكن لموظفي الدعم استرجاع بياناتك من الخوادم عند فقدك لها

الشبكات العامة

الشبكات العامة

هي أحد أنواع الشبكات التي تسمح للعديد من المستخدمين المختلفين باستخدامها في الأماكن العامة للاتصال بالإنترنت، ونظراً لانعدام القيود عليها، واتاحه استخدام العديد من المستخدمين لنفس الشبكة فإنها من أكبر الأسباب المعرضة للمخاطر والهجمات السيبرانية.

أمثلة على الشبكات العامة

المطاعم والمقاهي

الفنادق

المطارات

كلمة المرور والأسئلة الأمنية

حماية كلمة المرور

يجب أن تتكون من أحرف وأرقام ورموز وألا يقل طولها عن ٨ خانات

أنشئ كلمة مرور مختلفة لحساباتك وتأكد من تغييرها بشكل دوري

لا تبنها على معلومات معروفة أو بيانات شخصية متوقعة

لا تدخلها في أجهزة غير موثوقة أو عبر شبكة عامة وغير آمنة

لا تكتبها في مكان ظاهر للأخرين ولا تشاركها مع أحد

بلّغ عن أي بريد يطلب تغيير كلمة المرور لأي من حساباتك

الأسئلة الأمنية

التأكد من اختيار أسئلة أمنية معقدة وغير معروفة أجوبتها للأخرين.

لا تشارك أجوبة الأسئلة الأمنية مع الأخرين.

لا تكتب الأسئلة الأمنية وجوبتها في مكان ظاهر للأخرين.

مثال على كلمة مرور قوية

I have joined General Court of Audit on 2nd Aug 2020 at Riyadh

I have joined General Court of Audit on 2nd Aug 2020 at Riyadh

تم إنشاء كلمة المرور التالية من الجملة السابقة

IhjGCoAo2A2@R

شكراً لكم

الديوان العام للمحاسبة
General Court of Audit

المخاطر المرتبطة بتشغيل البيانات الإلكترونية

مكونات العرض

- تعريف المخاطر للأمن السيبراني.
- تصنيف مخاطر الأمن السيبراني للبيانات.
- أمثلة على مخاطر الأمن السيبراني للبيانات.
- مخاطر الأمان.
- مخاطر الامتثال.
- مخاطر التشغيل.
- إدارة مخاطر الأمن السيبراني للبيانات.

مخاطر الأمن السيبراني

- **تعريف مخاطر الأمن السيبراني:**

هـي احتمـال وقـوع حـدث ضـار يمكـن أن يـؤدي إلـى فقـدان، أو تلـف، أو تعطيـل البيانـات ،أو الأنظمـة، أو الشبكات. يمكن أن تنشأ مخاطر الأمن السيبراني من مجموعة متنوعة من المصادر.

- **مصادر المخاطر:**

مخاطر الأمن السيبراني للبيانات

أنواع مخاطر الأمن السيبراني للبيانات

مخاطر الأمان

مخاطر الامتثال

مخاطر التشغيل

مخاطر الأمن السيبراني للبيانات

أولاً: مخاطر الأمان:

هي مخاطر تنشأ من إمكانية الوصول غير المصرح به إلى البيانات أو تغييرها أو تدميرها، ويمكن أن تؤدي مخاطر الأمان إلى فقدان البيانات أو تلفها أو تعطيل العمليات.

أمثلة على مخاطر الأمان:

- انتهاكات البيانات
- هجمات القرصنة
- برامج الفدية
- الوصول غير المصرح به

مخاطر الأمن السيبراني للبيانات

ثانياً: مخاطر الامتثال:

هي مخاطر تنشأ من عدم الامتثال والالتزام بقوانين ولوائح وارشادات الأمن السيبراني، ويمكن أن تؤدي مخاطر الامتثال إلى فرض عقوبات مالية أو قانونية على المؤسسات والجهات.

أمثلة على مخاطر الامتثال:

- عدم الامتثال للقوانين واللوائح
- عدم الامتثال للمعايير الدولية
- عدم الامتثال لسياسات الجهة

مخاطر الأمن السيبراني للبيانات

ثالثاً: مخاطر التشغيل:

هي مخاطر تنشأ من عدم القدرة على الوصول إلى البيانات أو استخدامها أو معالجتها، ويمكن أن تؤدي مخاطر التشغيل إلى تعطيل العمليات وانخفاض إنتاجية الجهة.

أمثلة على مخاطر التشغيل:

- الأداء البطيء
- التوقف عن العمل
- فقدان البيانات

أمثلة على مخاطر الأمن السيبراني للبيانات

- اختراق البيانات الشخصية لعملاء المؤسسة
- فقدان البيانات المالية للمؤسسة
- تعطيل نظام المعلومات للمؤسسة
- انتشار الفيروسات أو البرامج الضارة في نظام المؤسسة

إدارة مخاطر الأمن السيبراني للبيانات

يمكن للمؤسسات إدارة مخاطر الأمن السيبراني للبيانات من خلال مجموعة من الإجراءات، بما في ذلك:

أولاً
التقييم المستمر للمخاطر

ثانياً
تنفيذ تدابير التحكم

ثالثاً
اختبار تدابير التحكم

رابعاً
إجراء عمليات التدقيق

إدارة مخاطر الأمن السيبراني للبيانات

أولاً: التقييم المستمر للمخاطر:

هو عملية تقييم المخاطر المحتملة التي قد تواجهها المؤسسة، ويجب على المؤسسات إجراء تقييمات للمخاطر بشكل دوري لضمان أنها على دراية بالمخاطر المحتملة واتخاذ الخطوات المناسبة لإدارة هذه المخاطر.

ثانياً: تنفيذ تدابير التحكم:

تدابير التحكم هي إجراءات أو تقنيات مصممة لتقليل مخاطر الأمن السيبراني، يمكن أن تتضمن تدابير التحكم أشياء مثل:

- التحكم في الوصول.
- التشفير.
- النسخ الاحتياطي.
- التدريب على أمن المعلومات.

إدارة مخاطر الأمن السيبراني للبيانات

ثالثاً: اختبار تدابير التحكم:

يجب على المؤسسات اختبار تدابير التحكم الخاصة بها للتأكد من أنها تعمل بشكل صحيح، يمكن أن يساعد اختبار تدابير التحكم المؤسسات في تحديد أي نقاط ضعف في نظام الأمن السيبراني الخاص بها.

رابعاً: إجراء عمليات التدقيق:

عمليات التدقيق هي عملية فحص نظام الأمن السيبراني للمؤسسة، يمكن أن تساعد عمليات تدقيق المؤسسات في تحديد نقاط الضعف في نظام الأمن السيبراني الخاص بها.

شكراً لكم

الديوان العام للمحاسبة
General Court of Audit

المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة
ARABOSAI

أساليب ووسائل الغش في بيئة تقنية المعلومات

(الوحدة الثانية)

الوحدة الثانية: أساليب ووسائل الغش في بيئة تقنية المعلومات

هدف التعلم:

تعريف الغش والاحتيال في بيئة تقنية المعلومات والوسائل المساعدة على اكتشافه

محاور الوحدة

الغش والاحتيال في بيئة تقنية المعلومات

الوسائل المساعدة في اكتشاف الغش والاحتيال في بيئة تقنية المعلومات

مكونات الوحدة

- مفهوم الغش والاحتيال الرقمي
- الغش والاحتيال في بيئة تقنية المعلومات

محاور الجلسة

- الغش والاحتيال الرقمي
- صور الغش والفساد في بيئة تقنية المعلومات
- وسائل كشف الغش في بيئة تقنية المعلومات

الغش والاحتيال الرقمي

ظهور ظاهرة الغش والاحتيال الرقمي	يعتبر الغش والاحتيال من المخاطر التي تواجهها مختلف مؤسسات القطاعين العام والخاص، وقد تفاقمك هذه الظاهرة خاصة عندما اتجهت الجهات الحكومية لتعزيز عمليات التحول الرقمي معتمدة في ذلك على التقدم التقني الذي يشهده العالم وعلى ازدياد الكفاءات التقنية.
الغش والاحتيال التقليدي	الغش والاحتيال هو استخدام أساليب المراوغة والغش كأداة لكسب وتحقيق منفعة غير مشروعة تكون عادة مالية. أما نوع الغش والاحتيال فيعتمد بشك كل كبير على عمليات المؤسسة وأصولها المهمة التي تعتمد عليها لضما استدامتها التشغيلية.
الغش والاحتيال الرقمي	والذي ينشأ عن استخدام المحتالين للبريد الإلكتروني أو المواقع الإلكترونية، أو البرمجيات الخبيثة، أو غيرها من الأدوات، للحصول على المعلومات الشخصية للمستخدم، أو خداع المستخدم لتقديم معلوماته الشخصية، وذلك لاستثمارها في تحقيق غايات عديدة، ومنها غايات مالية غير مشروعة.

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- تطور الغش والاحتيال الرقمي بالتزامن مع تطور الحكومة الرقمية وخلال المراحل التالية:

- قدمت منظمة التعاون الاقتصادي والتنمية OCED تعريفا لمفهوم الحكومة الإلكترونية بأنها استخدام للتقنيات القائمة على الإنترنت في التعامل مع أعمال الحكومة بما يضمن تقديم الخدمات للمستفيدين وبشكل مستمر وعلى مدار الساعة دون الحاجة لزيارة مقر الجهة، وبالتالي ضمان كفاءة الانفاق وخفض التكلفة وتقليل الوقت والجهد.
- تساهم الحكومة الإلكترونية في سهولة توفير تقارير الاستخدام والمعلومات الحكومية الأخرى التي كان من الصعب الحصول عليها بسبب عدم توفر المعلومات الكافية عن المستخدمين أو حجم الاستخدام، وكأنك تعتمد بشكل أو بآخر على مساحات الدردشة أو الاستفتاءات العامة التي تنشر عبر الإنترنت للحصول على المعلومات.
- في هذه المرحلة، كان مفهوم الغش والاحتيال الرقمي بسيط جداً، والذي كان مرتبطا في الغالب بالمخاطر التقنية الأساسية مثل الفيروسات وأحصنة طروادة، وكان في وقتها من السهل اكتشافها وحلها.

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- تطور الغش والاحتيال الرقمي بالتزامن مع تطور الحكومة الرقمية وخلال المراحل التالية:

- تعزز الرقمنة العمليات الإدارية والتنظيمية والتشغيلية بين مختلف الجهات الحكومية في انتقالها إلى التحول الرقمي الشامل للسماح بالوصول السهل والفعال إلى المعلومات والخدمات الرقمية الحكومية.
- شملت هذه المرحلة توفير خصائص وميزات ضمن الخدمات الحكومية مثل دمج تطبيقات التواصل الاجتماعي، والسماح للمستخدمين بإضافة بعض المحتويات، كما أن تزايد الاهتمام بالبيانات وبالأخص المفتوحة منها والسماح بمشاركة واستخدام بيانات المستخدمين أدى إلى توفير خدمات أكثر فائدة وتناسب مع حاجة المستفيدين.
- تطور مفهوم الغش والاحتيال الرقمي خلال مرحلة الرقمنة ليشمل مخاطر مثل مخاطر سرقة بيانات الهوية، ومع تقدم التقنية وأدوات كشف الغش والاحتيال الرقمي أصبح المحتال وأمام بعد التحديات التي تحد من القدرة على تنفيذ الهجمات، ومنها الوقت اللازم لتنفيذ مثل هذه الهجمات، مما يتيح إمكانية أكبر لاكتشاف واحتواء الهجمات قبل أن تؤثر بشكل كبير على المستخدم.

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- تطور الغش والاحتيال الرقمي بالتزامن مع تطور الحكومة الرقمية وخلال المراحل التالية:

- التحول الرقمي يعنى بتحويل نماذج الأعمال وتطويرها بشكل استراتيجي، لتكون نماذج رقمية مستندة على بيانات وتقنيات وشبكات الاتصالات.
- في هذه المرحلة يتم استخدام التقنيات الناشئة وغيرها من التقنيات المبتكرة مثل (البلوكتشين والبيانات الضخمة والذكاء الاصطناعي) لاتخاذ القرارات وصناعة السياسات المبنية على البيانات والأدلة، إضافة إلى تقديم خدمات حكومية متخصصة بناءً على احتياجات كل مستفيد.
- في هذه المرحلة أصبح مفهوم الغش والاحتيال الرقمي متقدماً، ومعقدا جدا لما يتضمنه من تهديدات متقدمة أصبحت في متناول يد المحتالين نتيجة لتوفر المصادر وإمكانية الوصول إلى هذه المصادر، وبالطبع مع مرور الوقت استطاع هؤلاء تطوير مهاراتهم للتأكد من تعقيد المحاولات الاحتيالية مما يجعل من الصعب اكتشاف هذه المحاولات الاحتيالية والتعامل معها قبل تحقيق المحتالين أهدافهم غير المشروعة.

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- تطور الغش والاحتيال الرقمي بالتزامن مع تطور الحكومة الرقمية وخلال المراحل التالية:

إن التقدم الذي حصل على مستوى البيئة التقنية على مستوى العالم ساهم بشكل كبير في تعزيز الارتباط والتواصل بين جميع الأطراف، الأمر الذي أتاح للحكومات فرصاً أكبر لتطوير خدماتها ومعاملاتها لتصبح "حكومات رقمية"، غير أن ذلك تزامن مع استغلال جهات أخرى لهذا التطور والتقدم التقني لتشكيل تهديدات أقوى، حيث قامت بتطوير مهاراتها وإضفاء المزيد من التعقيدات على هجماتها لتتمكن من مضاعفة أثرها، والحد من فرص الكشف عنها واحتواء عمليات الاحتيال بأقصى سرعة ممكنة

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- الغش والاحتيال الرقمي والتحول الرقمي

- تشمل جرائم الإنترنت مجموعة واسعة من الأنشطة الإجرامية التي يتم فيها استهداف الأفراد أو الشركات أو والمنتجات الحكومية باستخدام الحواسيب أو شبكات الاتصالات، وتشمل هذه الأنشطة التحرش الإلكتروني، والتحيز الإلكتروني، والاحتيال الرقمي.
- تتوسع مجالات جرائم الإنترنت باستمرار، مما يفتح فرصاً كبيرة للتحول الرقمي بسبب إمكانياته العالية وطبيعته المتصلة بشكل كبير، فتعتبر البيانات المادة الخام الأساسية للتحول الرقمي، وقد نما حجم البيانات، خاصة في التطبيقات الصناعية، بشكل هائل مع التقدم السريع للتقنيات الرقمية مثل تقنيات الحوسبة، وتقنية المعلومات والاتصالات، والاتصال اللاسلكي، وأجهزة الاستشعار والتحكم، والإنترنت، والذكاء الاصطناعي، والحوسبة السحابية، وتعلم الآلة، وغيرها، ويترتب على هذا التقدم تطور وتعقيد العصر الرقمي، وبالتالي يدفع عملية التحول الرقمي إلى الأمام.
- يعتمد التحول الرقمي على التقنيات والمهارات المتقدمة والذكية لتعزيز الابتكار والذكاء والكفاءة للعمليات الحكومية والصناعية والاجتماعية، ويتجاوز التحول الرقمي كونه مجرد تحويل العمليات القائمة إلى الشكل الرقمي، إذ إنها تهدف إلى الاستفادة من التقنية الرقمية لإعادة تشكيل تلك العمليات إلى أنظمة ذكية، وضمن الاتصال المستمر للأجهزة مع قابلية للوصول والتحكم والتخصيص بشكل كبير، وبالتالي، تصبح الكفاءات المتقدمة في الأنظمة الرقمية وعمليات الشبكات والفهم الشامل للتقنيات الرقمية ضرورية لدفع وإدارة التحول الرقمي بفعالية، ويجب أن تكون الكفاءات المتقدمة متاحة على نطاق واسع ومتاحة ومعترف بها كعناصر أساسية في مجال التحول الرقمي

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- الغش والاحتيال الرقمي والتحول الرقمي

- يعد التحول الرقمي عامل أساسي في تغيير سلوك الأعمال والعمليات الصناعية والسلوك المجتمعي. وبالتالي، فإن تأثير التحول الرقمي سيحول العمليات التقليدية المعزولة إلى عمليات متكاملة ومترابطة بالكامل تعتمد على البيانات وتتجاوز الحدود، سوف تتميز هذه العمليات باللامركزية، والتحسين الذاتي للأنظمة والمكونات، ويتطلب تحقيق ذلك استخدام التقنيات اللاسلكية لتمكين الاتصال الرقمي السلس في الأنظمة السيبرانية لضما عمليات فعالة.
- ولتحقيق التطور في الاقتصاد الرقمي بالاعتماد على التقنيات الحديثة، يجب أن تمتلك المؤسسات التجارية والحكومة والصناعية والمجتمع القدرة على التنبؤ بالأحداث والاستجابة بسرعة للتحديات والفرص. وتبعا لذلك تصبح مسألة حماية البيانات أمراً ضرورياً في التحول الرقمي، حيث يعد الأمن السيبراني أمراً بالغ الأهمية للحماية من التهديدات السيبرانية، ومع ذلك، فإن تنفيذ التحول الرقمي عبر المؤسسات الحكومية والخاصة والمجتمع سيتطلب وقتاً، وذلك وفقا للنماذج الحديثة والعمليات التي تعتمد على الذكاء الاصطناعي والتعلم الآلي، والآلات الذكية المترابطة، والواقع المعزز، ونظم جمع وإدارة البيانات، ومختلف التطورات التقنية الأخرى.
- فيصبح اكتساب المعرفة والكفاءات العملية والتقنية أمرا بالغ الأهمية لقيادة التحول الرقمي بفعالية باختلاف المستويات.

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- الغش والاحتيال الرقمي والتحول الرقمي

وفقا لتقرير نشره البنك الدولي، تشكل الأنشطة الاحتيالية ما يقارب ٤٠% من جميع الجرائم الجنائية المسجلة، مما يؤدي إلى تكلفة سنوية تقدر بـ ١٣٠ مليار جنيه إسترليني لاقتصاد المملكة المتحدة. والجدير بالذكر أن ١% فقط من الحالات المبلغ عنها يم حلها قانونيا، علاوة على ذلك، لا يتم الإبلاغ عن جزء كبير من هذه الحوادث والتي تشكل حوالي ٨٥% منها، ويعود السبب إلى عوامل منها الإحراج، والفشل في تحديد وقوع الجريمة، وضعف الإلمام بقنوات الإبلاغ المناسبة. من المهم أن ندرك أن الاحتيال أبعد ما يكون عن جريمة لا ضحايا لها، فغالباً يتأثر المتعرضون للاحتيال للقلق الشديد والتوتر واضطرابات النوم وحتى التفكير بإيذاء النفس.

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- الغش والاحتيال عبر بيانات المستفيدين

المعلومات الشخصية هي البيانات التي تكشف عن، أو تشير إلى، هوية الشخص، والتي تمكّن الحكومات من تحديد الاحتياجات والاهتمامات والأولويات الشخصية لكل مستفيد. وبالتالي، تحاول العناصر الإجرامية استغلال هذه البيانات لتحقيق مكاسب مالية غير مشروعة، أو قد يستخدم المجرمون البيانات الشخصية المسروقة لأغراض مختلفة مثل التشهير والابتزاز والتحييد السياسي وغيرها، مما يتسبب في تأثير سلبي على سلامة وأمان المستفيد. على سبيل المثال، يمكن استخدام البيانات الشخصية المسروقة لتشويه سمعة الأفراد أو المؤسسات عن طريق نشر معلومات خاطئة أو محرجة عنهم، ويمكن استخدام البيانات الشخصية للابتزاز لتحقيق مكاسب مالية أو لأغراض أخرى، ففي حين أن معلومات المستفيد ضرورية للتحول الرقمي، إلا أنها يمكن أن تمثل أيضاً بعض المخاطر والتحديات المتعلقة بالاحتيال الرقمي.

الغش والاحتيال الرقمي

مراحـــل تطـــور الغش والاحتيال الرقمي

- الغش والاحتيال عبر بيانات المستفيدين

الغش والاحتيال الرقمي

صور الغش والفساد في بيئة تقنية المعلومات

الاحتيال في مجال الرعاية الاجتماعية	يهدف المحتال للحصول على مكاسب وفوائد الرعاية الاجتماعية؛ إما لغاية استهداف الجهات الحكومية، أو لتحقيق مكاسب شخصية. مثال: الاحتيال بالتلاعب ببيانات الأنظمة الحكومية: يمكن للمحتالين التلاعب بالرقم القياسي للمستفيد للحصول على مساعدات مالية أو خدمات اجتماعية غير مستحقة.
الاحتيال في مجال الرعاية الصحية	يستهدف المحتال أنظمة الرعاية الصحية بغرض الحصول على مكاسب أو مبالغ غير نظامية. مثال: الاحتيال بالتلاعب بالتأمين الصحي فيمكن للمحتالين تزوير بوليصية التأمين الصحي للحصول على امتيازات أو مال بطرق غير مشروعة.
الاحتيال المالي	الاحتيال أو السرقة بهدف سرقة المال، أو تحويله إلى حساب المحتال، أو كلاهما. مثال: استغلال البيانات الشخصية المالية أو بيانات المؤسسات المالية مثل بيانات المحافظ الاستثمارية أو القوائم المالية والميزانيات بهدف استغلال الثغرات المالية وتحقيق مكاسب غير مشروعة.

الغش والاحتيال الرقمي

صور الغش والفساد في بيئة تقنية المعلومات

الاحتيال بتزوير الهوية

الاحتيال من خلال استخدام هوية وهمية أو مسروقة في تنفيذ عمل غير نظامي بهدف الحصول على سلع أو خدمات بطريقة غير نظامية.

مثال: يشكل استغلال بيانات الهوية الشخصية خطراً كبيراً خصوصا مع الأفراد، فتستغل في تنفيذ محاولات احتيال غير مشروعة مثل الاحتيال المالي أو الاستفادة من الخدمات الاجتماعية والخدمات الحكومية أو تشكل تهديدا سياسياً عليهم عند استخدام بياناتهم في محاولات اجرامية دولية.

الاحتيال بوسائل الاتصال

استغلال وسائل الاتصال لسرقة الأموال من العملاء أو مزوّدي خدمة الاتصالات أو كلاهما.

مثال: استخدام رقم الجوال في التواصل مع الأفراد وخداعهم بأنهم ممثلوا خدمة العملاء لدى البنوك أو بعض شركات مزودي الخدمات بهدف التهديد والابتزاز وسرقة الأموال والمعلومات الشخصية.

تُنفّذ غالبية حالات الاحتيال الرقمي على يد محتالين يُقدمون على أفعالهم لدوافع متباينة.

الغش والاحتيال الرقمي

تعطي عوامل الخطر التالية المحتالين الفرصة لاستثمار التهديدات الممكنة وتنفيذ الاحتيال الرقمي:

عوامل الخطر التي تُسهم في الاحتيال الرقمي:

عوامل الخطر السيبرانية

استخدام الثغرات في الضوابط الأمنية التي من شأنها أن تضمن وجود حماية فعّالة ضد المحتوى الخبيث والإجرامي الذي يُمكن استخدامه لتنفيذ الاحتيال الرقمي

عوامل الخطر الثقافية في المؤسسة

عدم وجود ضبط وحوكمة ودعم كافٍ من الإدارة العليا للحماية ضد الهجمات السيبرانية، وضعف التركيز على أهمية الأمن ضد الاحتيال الرقمي

عوامل الخطر الضمنية في إجراءات الأعمال

الاحتيال الرقمي هو خطرٌ ضمني يُرافق خطوات التحوُّل الرقمي للعمليات والإجراءات التي تهدف إلى دعم التحول الرقمي الحكومي.

عوامل الخطر المالية

عدم توزيع الموارد والميزانيات على نحوٍ يُعزّز المستوى الأمني بشكلٍ كافٍ لمواجهة الاحتيال الرقمي

الغش والاحتيال الرقمي

التهديدات التي تنتج عن استغلال عوامل الخطر:

التصيّد الإلكتروني

تهديد يتم تنفيذه من خلال التلاعب النفسي لحثّ المستخدم على إعطاء معلوماتٍ حساسة

تهديدات فنية

تهديدات مختلفة تتيح لعناصر الاحتيال الوصول إلى معلوماتٍ حساسة والتأثير على قدرة الجهات على تقديم خدمات رقمية

تهديدات مادية

تهديدات تنتج عن التلاعب بالممتلكات المادية والعقلية، أو إلحاق الضرر بها، أو سرقتها، أو الوصول إليها دون تصريح

تهديدات غير مقصودة

تصرُّف يُلحق ضرراً بالأصول نتيجةً لتصرّف خاطئ من موظف ما ولكن من دون أن يكون له نية خبيثة

الغش والاحتيال الرقمي

ينتج الاحتيال الرقمي الآثار التالية التي لها نتائجها المباشرة على تجربة ورضا المستفيد:

الإضـرار بالخـدمات والمُنتجـات الحكومية

يحُدّ الاحتيال الرقمي الجهات الحكومية من قـدرتها علـى تقـديم خـدماتٍ تركّـز علـى المستفيد وتحقيق النتائج المرجوّة

أثر على السمعة

يـؤثر الاحتيـال الرقمـي علـى الجهـات الحكومية تأثيراً سلبياً على سمعتها نتيجةً لما سيتم تداوله في وسائل الإعلام حول هذه الحادثة، مما سيؤدي إلى انخفاض ثقة المستفيد بهذه المؤسسات

خلل في الضوابط الأمنية

ينجم عن الاحتيال الرقمي في القطاع العام تعـرّض المعلومـات الشخصـية للمستفيدين لخطر الكشف والتي يُمكن أن تُستخدم لتنفيذ هجمات مادية تُهدّد أمن الوطن والمستفيدين

عواقب على عمل القطاعات

ينتج عن الاحتيال الرقمي في القطاع العام انعكاسات تطال القطاعين العام والخاص معاً نتيجةً للروابط التي تجمع بينهما.

توقّف أو بطء إجراءات العمل

يؤثر الاحتيال الرقمي على أداء الجهات لأنه يودي إلى تكبّدها تكاليف مالية نتيجةً لعمليات كشف مثل هذه الحالات والتحقيق فيها وحلّها

الغش والاحتيال الرقمي

2.1 الرعاية الصحية

مساهمات التحوّل الرقمي

طوّرت منظمة الصحة العالمية الاستراتيجية العالمية للصحة الرقمية بهدف تعزيز الرعاية الصحية الإلكترونية وتعزيز الصحية الرقمية بأسلوبٍ أخلاقي وسليم وآمن وموثوق وعادل ومستدام بما يضمن وجود خدمات عامة تركّز على المستفيد.

لماذا يتعرض قطاع الرعاية الصحية للاحتيال الرقمي؟

خلال جائحة كورونا، أصبح قطاع الرعاية الصحية معرّضاً بشكلٍ خاص للاحتيال الرقمي بسبب معالجة المعلومات الصحية المحمية والسجلات الطبية الخاصة بالمستفيدين، والتي تُعتبر بياناتٍ سريةً يجب أن تكون محميةً بموجب نظام خصوصية البيانات الشخصية. ولكن المحتالين استغلوا البيانات التي تم تخزينها لمساندة الخدمات الصحية الإلكترونية لينفذوا معاملاتٍ مُزيّفة مُرتبطة بجائحة كورونا ليتمكّنوا من الوصول إلى مصادر البيانات التي يُمكن استغلالها لتحقيق مكاسب مالية مع إضفاء صفة نظامية على هذه العمليات (اختبارات مُزيّفة، سجلات تطعيم مُزيّفة). وقد استغلّ المحتالون السجلات الطبية وبيانات الهوية الوطنية المتوفرة لارتكاب جريمة تزوير الهوية، والحصول على فوائد التأمين الطبي بشكلٍ مزيّف، أو طلب فدية مقابل منع الإفصاح عن المزيد من المعلومات.

المعلومات والبيانات التي تتم معالجتها

بيانات المستفيد داخل الأنظمة الحكومية المالية، التعليمية، الصحية.	رقم الهوية الوطنية
البيانات البيومترية	العنوان

الغش والاحتيال الرقمي

أنواع الاحتيال الشائعة في قطاع الرعاية الصحية

يتأثر قطاع الرعاية الصحية بالأنواع التالية من الاحتيال:

- **الاحتيال من خلال الرعاية الاجتماعية:** يتأثر قطاع الرعاية الصحية بهذا النوع من الاحتيال من خلال سعي المحتالين إلى استخدام أساليب الاحتيال للحصول على مكاسب مثل التأمين الطبي.
- **الاحتيال من خلال الرعاية الصحية:** هناك ارتباط وثيق بين قطاع الرعاية الصحية وهذا النوع من الاحتيال على اعتبار أن القطاع يملك السجلات الطبية التي تخص المستفيدين.
- **الاحتيال المالي:** خلال جائحة كورونا بشكلٍ خاص، استغل المحتالون كميةً كبيرة من المعلومات الصحية المحمية التي تم تسجيلها ومعالجتها لتعزيز مستوى الصحة الإلكترونية مقابل الحصول على عوائد مالية.
- **الاحتيال من خلال تزوير الهوية:** يتأثر هذا القطاع بهذا النوع من الاحتيال على اعتبار أن المحتالين قد يستخدمون المعلومات الخاصة المحمية التي تعود للمستهدفين لطلب خدمات طبية.

الآثار المحتملة

أهم الآثار المترتبة عن الاحتيال الرقمي على قطاع الرعاية الصحية:

الإضرار بالخدمات والمُنتجات الحكومية

بسبب توقف العمليات خلال التحقيقات المستمرة، الأمر الذي ينعكس على جودة خدمات الرعاية الصحية المقدّمة للمستفيدين.

تعطل عمل القطاعات

تأثر القطاع الصحي من محاولات الاحتيال الرقمي من خلال ارتباط خدمات الصحة الإلكترونية لخدمات الرعاية الصحية الإلكترونية مع مختلف القطاعات التي تستخدم بيانات الرعاية الصحية مثل شركات التأمين.

الغش والاحتيال الرقمي

2.2 الخدمات المالية

مساهمات التحوّل الرقمي

يتجلّى التحوُّل الرقمي في القطاع المالي خاصّة من خلال ظهور التقنيات المالية. وينصب التركيز حالياً في القطاع المالي على تمكين التقنية من خلال دمج عدد من التقنيات الناشئة، مثل البلوكتشين والذكاء الاصطناعي، لتقديم خدمات مخصصة بشكلٍ أكبر.

لماذا يتعرض قطاع الخدمات المالية للاحتيال الرقمي؟

يُعتبر قطاع الخدمات المالية واحداً من أكثر القطاعات المستهدفة للاحتيالات الرقمية بسبب ضخامة حجم بيانات التعاملات التي يمكن استغلالها بطرق احتيالية لتحقيق مكاسب مالية. وقد تمكّن المحتالون بشكلٍ أكبر من استهداف القطاع المالي بنجاح نتيجةً لزيادة نشاط التجارة الإلكترونية خلال فترة الجائحة.

وموخراً ازداد الاعتماد على التسوّق الإلكتروني كونه وسيلةٍ مناسبة وسهلة للشراء، ونتيجة لذلك سَعَت المؤسسات لتأمين تجربة سلسة للمستخدم من خلال تسهيل عملية التحقُّق من هوية المستخدم لإتمام عملية الشراء، لا سيّما إذ أصبحت خاصية تخزين المعلومات الحيوية وسيلةً أسهل لإثبات الهوية. وعليه، فإن الجمع بين التدابير الأمنية من جهة والسهولة والراحة من جهةٍ أخرى تجعل القطاع أكثر عُرضةً للاحتيال الرقمي.

المعلومات التي تتم معالجتها

رقم البطاقة الائتمانية	رقم الهوية الوطنية
البيانات البيومترية	العنوان

الغش والاحتيال الرقمي

أنواع الاحتيال الشائعة في قطاع الخدمات المالية

يتأثر قطاع الخدمات المالية بأنواع الاحتيال التالية:

- **الاحتيال المالي:** هناك ترابط وثيق بين قطاع الخدمات المالية والاحتيال المالي؛ بسبب امتلاك قطاع الخدمات المالية لبيانات المعاملات التي تعود للمستفيدين، والتي يُمكن استخدامها لتنفيذ معاملات مزوّرة.
- **الاحتيال من خلال تزوير الهوية:** من المُرجّح أن يتأثر قطاع الخدمات المالية بهذا النوع من الاحتيال في حال استطاع المحتالون استخدام المعلومات الشخصية، مثل: رقم الهوية الوطنية والعنوان والبيانات البيومترية، لتسهيل معاملات الاحتيال والتزوير، وفتح حسابات مصرفية مُزيّفة.

الآثار المحتملة

أهم الآثار المترتبة عن الاحتيال الرقمي على قطاع الخدمات المالية:

أثر على السمعة

يتميّز قطاع الخدمات المالية بمكانته الخاصة عند المستفيد كونه يسهل عليه إدارة أمواله الشخصية. وبالتالي فإن الاحتيال الرقمي سينعكس على ثقة المستفيد بالمؤسسة ونظرته إلى كفاءتها، لا سيما إذا انتشر خبر الحادثة.

توقّف أو بطء إجراءات العمل

يؤثر الاحتيال المالي بشكلٍ كبير على إجراءات العمل نتيجة حصول الأفراد المتأثرين من الاحتيال بالحوادث عادةً على تعويضات مالية. كما تتكبّد الجهات المستهدَفة تكلفة تنفيذ التحقيقات، وتكلفة تطبيق الضوابط الأمنية اللازمة.

الغش والاحتيال الرقمي

2.3 الاتصالات وتقنية المعلومات

مساهمات التحوّل الرقمي

قطاع الاتصالات هو عامل التمكين الرئيس للحكومة 3.0 كونه الداعم الأساسي للقطاعات في رحلة التحوُّل. كما أن هذا القطاع مسؤول عن تهيئة البيئة الداعمة لاعتماد التقنيات الناشئة وتقنيات الحوسبة السحابية.

لماذا يتعرض قطاع الاتصالات وتقنية المعلومات للاحتيال الرقمي؟

يعد قطاع الاتصالات معرّضاً بشكلٍ كبير للاحتيال الرقمي؛ كونه يرتبط ارتباطاً وثيقاً بتقنيات الحوسبة السحابية التي تخزّن وتعالج كميات هائلة من البيانات. كما أن تنفيذ نموذج العمل عن بُعد خلال الجائحة قد أدى إلى ظهور أنشطة تستغل طرق الوصول إلى المعلومات التشغيلية والمعلومات الحسّاسة الخاصة بالشركات نتيجةً لتخزينها في المستودعات السحابية وتبادلها عبر منصات إلكترونية على الشبكة. وبالتالي سلّط قطاع الاتصالات الضوء على أهمية الأمن السيبراني في وقتٍ يسعى فيه المحتالون إلى تطوير مهاراتهم حتى تُناسب التقدّم الذي تشهده أحدث التقنيات ويتمكّنوا من تحديد الفرص لتنفيذ هجمات معقدة جداً دون أن يتم كشفهم.

يمكن للمحتالين استغلال الثغرات في قطاع الاتصالات للحصول على البيانات الخاصة ببطاقات الائتمان، أو استخدام معلومات بطاقات الائتمان المسروقة للقيام بأنشطة احتيالية يمكن تيسيرها عبر شبكات الاتصالات، مثل التسوق عبر الإنترنت أو الدفع الالكتروني.

المعلومات التي تتم معالجتها

- رقم البطاقة الائتمانية
- رقم الهوية الوطنية
- البيانات البيومترية
- العنوان

الغش والاحتيال الرقمي

أنواع الاحتيال الشائعة في قطاع الاتصالات وتقنية المعلومات

يتأثر قطاع الاتصالات بأنواع الاحتيال التالية:

- **الاحتيال من خلال وسائل الاتصال:** يتأثر قطاع الاتصالات بشكلٍ مباشر بالاحتيال من خلال وسائل الاتصال؛ لأن المحتالين يستهدفون مباشرةً أجهزة الاتصال على البيانات التي يمكن استخدامها بطرق غير مشروعة لتحقيق مكاسب مالية.
- **الاحتيال من خلال تزوير الهوية:** يتأثر قطاع الاتصالات بهذا النوع من الاحتيال نظراً لقدرة المحتالين على استخدام شرائح خطوط الجوال المسروقة أو التي تم الحصول عليها بهوية مُزيّفة لتحقيق مكاسب مالية غير مشروعة أو أغراض أخرى منها الإساءة للأفراد. وقد أصبح هذا النوع من الاحتيال أكثر شيوعاً خلال جائحة كورونا حيث انتحل المحتالون صفة مدراء تنفيذيين للوصول إلى معلومات حسّاسة بالشركات.

الآثار المحتملة

أهم الآثار المترتبة من الاحتيال الرقمي على قطاع الاتصالات وتقنية المعلومات:

عواقب على عمل القطاعات

في حال تعرّض قطاع الاتصالات للاحتيال الرقمي سيكون عُرضةً لتوقف أو بطء العمليات الخاصة بقطاعات أخرى تعتمد على خدمات الحوسبة السحابية التي يدعمها قطاع الاتصالات، وذلك لعدم توفر البيانات اللازمة.

خلل في الضوابط الأمنية

إذا تعرّض قطاع الاتصالات للاحتيال الرقمي فإن ذلك سيؤثر على الإجراءات الأمنية للمؤسسات؛ لأن التقنيات الرقمية وتقنيات الحوسبة السحابية التي تحتوي على معلومات شخصية حسّاسة يُمكن أن تتعرض للاستغلال لأغراض غير مشروعة تؤثر على راحة المستفيدين وأمنهم.

الغش والاحتيال الرقمي

2.4 التجارة الإلكترونية

مساهمات التحوّل الرقمي

أتاحت التجارة الإلكترونية إمكانية بيع وشراء السلع والخدمات عبر الانترنت والتي فتحت أفاق جديدة للأفراد والمؤسسات ودعمت الاقتصادات الدولية ومن أهمها قطاع السياحة والسفر والذي يسعى إلى تأمين تجربةٍ مخصصة للمسافرين من خلال استخدام التقنيات الناشئة لإتاحة الفرص للحجز أو التخطيط الذاتي، وتقديم توصيات تحقّق أفضل تجربة ممكنة للمسافر طوال رحلته.

لماذا يتعرض قطاع التجارة الإلكترونية للاحتيال الرقمي؟

قطاع التجارة الإلكترونية من القطاعات الجاذبة بالنسبة للمحتالين؛ نظراً لكمية البيانات الشخصية الهائلة المتوفرة في مواقع وتطبيقات الشراء والبيع والتداول وعلى سبيل المثال برامج السفر ومنصات حجز الطيران والفنادق. كما يُعتَبر هذا القطاع هدفاً سهلاً لهذه الجهات؛ كونه قطاعاً سريع التطور، الأمر الذي يقلل من احتمالية اكتشاف هوية المحتال، وبالتالي يتجنّب المساءلة والمحاسبة عن أفعاله.

لذا يستغل المحتالون جميع المكاسب المُرتبطة للحصول على منافع مالية أو تهديدات شخصية غير نظامية.

المعلومات التي تتم معالجتها

- بيانات المستفيد داخل الأنظمة الحكومية المالية، التعليمية، الصحية.
- رقم البطاقة الائتمانية
- رقم الهوية الوطنية وجواز السفر والبيانات البيومترية
- العنوان

الغش والاحتيال الرقمي

أنواع الاحتيال الشائعة في قطاع التجارة الإلكترونية

يتأثر قطاع التجارة الإلكترونية بأنواع الاحتيال التالية:

- **الاحتيال المالي:** يرتبط قطاع التجارة الإلكترونية بالاحتيال المالي حيث يُمكن للمحتالون الحصول على منتجات وخدمات كتذاكر السفر وحجوزات الفنادق من خلال التزوير باستخدام بيانات الدفع لضحاياهم دون أن يضطروا إلى الحضور شخصياً لتنفيذ عملية الشراء. كما يُمكنهم إعادة بيع السلع مره أخرى فيحققوا لأنفسهم مكاسب مالية غير مشروعة.
- **الاحتيال من خلال تزوير الهوية:** يُمكن أن يتأثر قطاع التجارة الإلكترونية بالاحتيال من خلال تزوير الهوية؛ نظراً لقدرة المحتالين على استغلال المعلومات الشخصية، مثل: رقم الهوية وسجلات الشراء والعناوين والبيانات البيومترية، لإصدار هوية مُزيّفة لتنفيذ مختلف المشتريات.

الآثار المحتملة

أهم الآثار المترتبة من الاحتيال الرقمي على قطاع التجارة الإلكترونية :

الإضرار بالخدمات والمُنتجات الحكومية

يؤدي الاحتيال الرقمي إلى الحد من قدرة الجهات الحكومية على تقديم خدمات تركّز على المستفيد؛ بسبب التكاليف المالية التي قد يتكبدها، وذلك لأن المستفيد قد يستثمر مبالغ كبيرة من المال في مشتريات يتبين فيما بعد أنها سلع ومنتجات مزوّرة.

خلل في الضوابط الأمنية

يؤثر الاحتيال الرقمي بشكلٍ كبير على الأمن الوطني؛ كونه يُعطي المجرمين الذين صدرت بحقهم أحكام نظامية فرصاً لاستغلال البيانات المتوفرة لإصدار بطاقة هوية مزوّرة، واستخدامها للسفر إلى الخارج؛ لتجنب المساءلة والمحاسبة.

المساهمات الدولية لمعالجة الغش والاحتيال الرقمي

الدولة	الجهة	نوع الاحتيال الرقمي	أبرز التدابير المتخذة
	وزارة العمل ومعاشات التقاعد بالمملكة المتحدة	الاحتيال في مجال الرعاية الاجتماعية / الاحتيال بسرقة الهوية	ركّزت الحكومة البريطانية على التعامل مع تزايد محاولات الاحتيال الرقمي التي تهدف إلى الاستيلاء على الأموال التي تم جمعها كجزء من الخطة الطارئة للاستجابة للجائحة
	وزارة الشؤون الداخلية بجمهورية الهند	الاحتيال بوسائل الاتصال / الاحتيال المالي	ركزت الهند بشكلٍ رئيس على معالجة تزايد محاولات الاحتيال من خلال وسائل الاتصال والاحتيال المالي
	وزارة العمل بالولايات المتحدة	الاحتيال في مجال الرعاية الاجتماعية / الاحتيال بسرقة الهوية / الاحتيال في مجال الرعاية الصحية/الاحتيال المالي	وجّهت الحكومة الأميركية جهودها نحو التركيز على سن التنظيمات والتشريعات لتحسين قدرتها على كشف محاولات ارتكاب الاحتيال المالي
	وزارة الشؤون الداخلية بجمهورية إستونيا	الاحتيال المالي	عملت إستونيا على تعزيز الأمن السيبراني على مستوى الدولة
	هيئة تنظيم الاتصالات والحكومة الرقمية بدولة الإمارات	الاحتيال المالي	ركّزت حكومة دولة الإمارات على إرساء الأُسس اللازمة لتعزيز الأمن السيبراني واحتواء الأثر الذي يمكن أن ينتج عن الاحتيال المالي
	الحكومة الكندية	الاحتيال المالي	ركّزت الحكومة الكندية جهودها على تطوير توجّه استراتيجي ووضع الخطط اللازمة للتعامل مع الاحتيال المالي

المساهمات الدولية لمعالجة الغش والاحتيال الرقمي

3.1 المملكة المتحدة

الجهة	نوع الاحتيال
وزارة العمل ومعاشات التقاعد	الاحتيال من خلال الرعاية الاجتماعية / تزوير الهوية

الوضع

- شهدت الجائحة تزايداً كبيراً لحالات الاحتيال بعد أن حدّدت الوزارة المستفيدين ذوو الأولوية ممن هم بحاجة للدعم المالي، وذلك ضمن إطار الخطة الطارئة للاستجابة للجائحة. ووصل حجم الاحتيال من خلال الرعاية الاجتماعية إلى 6.3 مليارات جنيه استرليني في عام 2021، بزيادة وصلت قيمتها إلى 2.1 مليار جنيه عن العام السابق.
- كما سعى بعض الأفراد والمجموعات إلى استغلال الإجراءات المؤقتة المُطبّقة والأنظمة الإلكترونية، حيث سجّل بعض الأفراد معلومات مُزيّفة، وكوّنوا فرقاً للاحتيال بهدف سرقة هويات الأفراد وسرقة مليارات الجنيهات.

المساهمات الدولية لمعالجة الغش والاحتيال الرقمي

3.1 المملكة المتحدة

الجهة	نوع الاحتيال
وزارة العمل ومعاشات التقاعد	الاحتيال من خلال الرعاية الاجتماعية / تزوير الهوية

الحل

لمعالجة الوضع، ركّزت الوزارة على ثلاث استراتيجيات والتزمت بها؛ لخفض خطر الاحتيال.

1. الاستثمار في كوادر الخطوط الأمامية لمكافحة الاحتيال وتحليل المعلومات
2. تشكيل أُطر نظامية جديدة للتحقيق في حالات الاحتيال المُحتملة ومعاقبة المحتالين، وتقديمها للحصول على الموافقة البرلمانية
3. تكوين فريق من الكفاءات في القطاعين العام والخاص للعمل على معالجة الوضع وتوفير حلول فعّالة لمواجهة الخطر.

الأثر

حدّت الحكومة من الوصول إلى حوالي 1.9 مليار جنيه استرليني إلى المجموعات الإجرامية المنظّمة التي سرقت هويات مستفيدين متسببة في تضليل الحكومة في تحديد حالة الدفع لكل مستفيد.

أجرت الحكومة مراجعةً بأثرٍ رجعي على مُجمل المطالبات التي وردت في بدايات الجائحة لتحديد حالات الاحتيال. وفي عام 2020/2021 انخفض حجم الخسائر المُحتملة إلى حوالي 3 مليارات جنيه استرليني.

المساهمات الدولية لمعالجة الغش والاحتيال الرقمي

3.5 الإمارات العربية المتحدة

الجهة	نوع الاحتيال
هيئة تنظيم الاتصالات والحكومة الرقمية	الاحتيال المالي

الوضع

- ازدياد حالات الاحتيال الإلكتروني ولّد مخاوف لدى الحكومة الإماراتية، لا سيما في ظل تسريع وتيرة جهود التحوُّل الرقمي على مستوى الدولة.
- وقد خسر ضحايا الجرائم السيبرانية في الإمارات بين العامين 2018 و2020 حوالي 746 مليون دولار أميركي سنوياً. وقد سجلت الإمارات خلال تلك الفترة 166,667 ضحية لجريمة سيبرانية.
- كما أدركت دولة الإمارات أنها بحاجة إلى بذل الجهود لتعزيز سلامة البنية التحتية التقنية في الدولة.

المساهمات الدولية لمعالجة الغش والاحتيال الرقمي

3.5 الإمارات العربية المتحدة

الجهة	نوع الاحتيال
هيئة تنظيم الاتصالات والحكومة الرقمية	الاحتيال المالي

الحل

1. بالاشتراك مع منصة أقدر للتعلم الإلكتروني، أطلق الفريق الوطني للاستجابة لطوارئ الحاسب الآلي مبادرة "سالم"، وهو مستشار إلكتروني في الأمن السيبراني، لنشر التوعية حول الأمن السيبراني والانتقال إلى ثقافة التعامل الآمن في البيئة السيبرانية.
2. في عام 2019، حدّثت دولة الإمارات استراتيجيتها الوطنية للأمن السيبراني حيث أطلقت 60 مبادرة تهدف إلى توحيد منظومة الأمن السيبراني في الدولة.

الأثر

حققت الاستراتيجية الوطنية المحدثة للأمن السيبراني في دولة الإمارات إنجازًا عالميًا بفعل مستوى السلامة الجديد الذي أوجدته ضمن الفضاء السيبراني بالدولة:

تمثّل أثر المُبادرات والاستراتيجية في تحسين تصنيف دولة الإمارات في المؤشر العالمي للأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات

في العام 2020، حلت دولة الإمارات في المرتبة الخامسة على المؤشر العالمي للأمن السيبراني متقدمّة من المرتبة 33 في العام 2019.

المساهمات الدولية لمعالجة الغش والاحتيال الرقمي

3.3 الولايات المتحدة الأمريكية

الجهة	نوع الاحتيال
وزارة العمل بالولايات المتحدة	الاحتيال في مجال الرعاية الاجتماعية، الاحتيال من خلال تزوير الهوية، الاحتيال المالي، الاحتيال من خلال الرعاية الصحية

الوضع

- في الولايات المتحدة الأميركية، تم سرقة 382 مليون دولار في عمليات نصب واحتيال مُرتبطة بجائحة كورونا، كانت في الأغلب على يد محتالين سجلوا من خلال هويات مسروقة للاستفادة من شيكات الحوافز وإعانات البطالة.
- تكرّرت مشكلة تزوير الهوية للاستفادة من إعانات البطالة خلال الجائحة، ووصل مجموع البلاغات عن سرقة الهوية الوطنية، والواردة للجنة التجارة الاتحادية، إلى حوالي 60 ألف بلاغ في عام 2021.

المساهمات الدولية لمعالجة الغش والاحتيال الرقمي

3.3 الولايات المتحدة الأمريكية

الجهة	نوع الاحتيال
وزارة العمل بالولايات المتحدة	الاحتيال في مجال الرعاية الاجتماعية، الاحتيال من خلال تزوير الهوية، الاحتيال المالي، الاحتيال من خلال الرعاية الصحية

الحل

طرح الكونغرس مشروع نظام للحد من سرقة الهويات الوطنية الإلكترونية للمواطنين، ويهدف النظام إلى "تحسين الهوية الإلكترونية"، وإرساء معايير توجّه الهيئات الحكومية خلال عمليات تقديم خدمات مُرتبطة بالهوية الإلكترونية، وتحديث الأنظمة القائمة، فضلاً عن تطوير أدوات للتحقُّق من الهويات الرقمية تربط بين الأنظمة.

سيساهم هذا النظام في مساعدة المواطن الأميركي على إثبات هويته إلكترونياً من خلال خدمة التحقّق من الهوية، الأمر الذي سيدعم حلول الهوية الرقمية والتحقق منها في القطاع الخاص.

الأثر

في أواخر شهر يوليو من العام 2022، راجعت لجنة الرقابة والإصلاح بالمجلس مسودة النظام، ويُتوقع أن تتم الموافقة عليه.

الجهود الوطنية في المملكة للحد من الاحتيال الرقمي

التطبيقات في المملكة العربية السعودية

تهدف الجهود المبذولة ضمن برنامج التحوُّل الوطني لتحقيق أهداف رؤية المملكة 2030 حيث تستهدف بعض هذه الجهود وضع تدابير لمكافحة الفساد بهدف الحد من الاحتيال الرقمي.

رؤية المملكة 2030 والتحوّل الرقمي في المملكة

- مجتمع حيوي
- اقتصاد مزدهر
- وطن طموح

عززت جهود التحوُّل الرقمي في المملكة، ورؤية المملكة 2030، من الحاجة إلى وجود معايير أعلى لضبط الأمن السيبراني لتواكب النمو المتسارع للبيئة الرقمية في المملكة.

جهود المملكة في الحد من الغش ولاحتيال الرقمي

جهود المملكة في الحد من الغش والاحتيال الرقمي

وضعت الجهود المبذولة لتطبيق رؤية الملمكة 2030 وبرنامج التحوُّل الوطني المملكة أمام تغيرٍ إيجابيٍ كبير على صعيد التحوُّل الرقمي.

وقد حلّت المملكة في المرتبة الثانية عالمياً في المؤشر العالمي للأمن السيبراني لعام 2020، وهو مؤشر عن مدى التزام الدول بمتطلبات الأمن السيبراني. وقد أحرزت المملكة تقدماً هائلاً من المرتبة 46 في عام 2017 إلى المرتبة 13 في عام 2018 نتيجةً لالتزامها المتزايد بسنّ تشريعات جديدة وإطلاق البرامج حيث تم إلزام مؤسسات الخدمات المالية بتحسين جوانب الأمن السيبراني لديها والحفاظ على الحد الأدنى من المعايير، وهو ما يمثل واحدة من الجهود الرئيسة للمملكة في مكافحة الاحتيال الرقمي.

جهود المملكة في الحد من الغش والاحتيال الرقمي

البنك المركزي السعودي
Saudi Central Bank
SAMA

الخدمة	المستهدف
خدمة شكاوى الاحتيال الإلكترونية	المواطنون والمقيمون

نظرة عامة

يقدّم البنك المركزي السعودي خدمة إلكترونية تُتيح للمستفيدين من الخدمة تقديم شكاوى حول حالات الاحتيال المالي البنكية، ويتولى البنك الذي يستضيف حساب صاحب الشكوى، تنفيذ الأبحاث والدراسات وتحليل الشكوى من الناحيتين التقنية والنظامية.

الأثر المتوقع

من خلال تقديم خدمة توفّر للأفراد تقديم شكاوى عن حالات الاحتيال، سيتمكّن البنك الذي تم تقديم الشكاوي تجاهه من دراسة هذه الشكاوى المقدّمة ضمن الأُطر الزمنية المناسبة قبل أن تتفاقم حدّتها وأثرها. ويمكن أن يتم استخدام الشكاوى كمصدر للبيانات في التحقيقات الجنائية. وبالتالي يمكن استخدام البيانات لتحديد الأنماط المُستخدمة واعتمادها لتطبيق التدابير الوقائية المناسبة لخفض احتمالية تنفيذ جرائم الاحتيال مستقبلاً. كما يمكن استخدام هذه البيانات لمعرفة المحتالين الذين ارتكبوا جرائم الاحتيال بشكلٍ متكرر للتأكُّد من اتخاذ التدابير النظامية اللازمة بحقهم ومحاسبتهم عن أفعالهم.

جهود المملكة في الحد من الغش والاحتيال الرقمي

البنك المركزي السعودي
Saudi Central Bank
SAMA

مبادرة
تحذيرات بشأن الاحتيال الرقمي

المستهدف
المواطنون والمقيمون والأفراد

نظرة عامة

يحذر البنك المركزي السعودي باستمرار المستفيدين من الاحتيال السيبراني ويحثهم على توخي الحذر بشأن بياناتهم والتأكد من أن المواقع التي يستخدمونها جديرة بالثقة.

يتم مشاركة التحذيرات بشكلٍ متواصل في ظل تكرار روايات الاحتيال وتكبّد الخسائر المالية.

الأثر المتوقع

العامل المشترك الذي يعتمد عليه المحتالون لتنفيذ جرائمهم الاحتيالية هو جهل المستخدم بالتهديدات مثل الاحتيال وتأثيره. فيستخدم المحتالون استراتيجيات ذات طابع واقعي لإضفاء إحساس الشرعية في التفاعل الرقمي مع المستخدم وكسب ثقتهم.

وبالتالي، يعتبر إرسال التحذيرات، رغم بساطة الجهد المطلوب في ذلك، إجراءً فعالا يزود المستخدمين بالمعلومات الكافية اللازمة لحماية هويتهم ضد المحاولات المحتملة التي تهدف إلى تنفيذ جرائم احتيالية.

جهود المملكة في الحد من الغش والاحتيال الرقمي

جهود المملكة في الحد من الغش والاحتيال الرقمي

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

مبادرة

نظام حماية البيانات الشخصية

المستهدف

كافة الجهات والمنشآت خارج وداخل المملكة التي تعالج بيانات المستفيدين

نظرة عامة

نظام حماية البيانات الشخصية هو نظام حماية البيانات الرئيس في المملكة العربية السعودية، ويتضمن بعض المواد واللوائح الخاصة بقطاع الأمن السيبراني، والتي تتناول حماية البيانات، وبعض المجالات التي تعتبر ذات صلة بالاحتيال، وتشمل: الأمن السيبراني وإنترنت الأشياء والاتصالات.

الأثر المتوقع

يضمن تطبيق نظام حماية البيانات الشخصية التعامل مع البيانات بشكلٍ مناسب، مما يُساهم في الحد من الفرص المتاحة أمام المحتالين. والسبب هو أن تنظيمات حماية الخصوصية تفرض عواقب تنظيمية على الجهات في حال عدم القدرة على تأمين وحماية البيانات التي تملكها بشكل كافٍ. ومع هذا الإجراء، سيواجه المحتالون صعوبة أكبر في الوصول إلى المعلومات واستغلالها لتنفيذ الأنشطة الاحتيالية.

جهود المملكة في الحد من الغش والاحتيال الرقمي

على مستوى الحكومات حول العالم، ترتكز الجهود التي تبذلها الجهات للتعامل مع الاحتيال الرقمي على العنصر البشري والقوانين والأنظمة المستخدمة.

01 الاستثمار في العنصر البشري

في دولة الإمارات، تستخدم الحكومة مبادرة سالم كأداة للتوعية تهدف إلى تعزيز مستوى الوعي بالاحتيال الرقمي لدى المستفيدين، وتقديم إرشادات حول سُبل حماية البيانات.

أما في الهند، فإن البوابة الوطنية للتبليغ عن الجرائم السيبرانية تتيح للناس تبليغ السلطات على الفور عن أي احتيال رقمي. وقد استطاعت السلطات المعنية أن ترصد اتجاهات الهجمات، وبالتالي ستكون قادرة على مساعدة المواطنين عند وقوع مثل هذه الحوادث قبل فوات الأوان.

02 تعزيز البيئة التشريعية والتنظيمية

أعادت الإمارات وكندا ترتيب أولوياتهما الحكومية من خلال وضع استراتيجيات للأمن السيبراني لإطلاق مُبادرات وخطط دقيقة لتطوير بيئات آمنة لجميع الجهات المعنية في العالم الرقمي. أما الولايات المتحدة الأميركية فتستخدم القوانين لتحسين معايير الهوية الرقمية للمساهمة في التقليل من آثار خطر الاحتيال الرقمي من خلال تزوير الهوية الشخصية.

في الهند، تم تشكيل لجنة من عدة جهات للاستفادة من الخبرات في عدة مجالات، والعمل معاً على طرح الأفكار، ومحاربة مخاطر الاحتيال الرقمي.

03 تطوير المنظومة الرقمية

في إطار مكافحة الغش الانتخابي، أعادت إستونيا تقييم نظام أمن المعلومات الحالي فيها واستبداله بمعيار جديد لأمن المعلومات، مما أبرز الحاجة إلى تحديث البنية التحتية الرقمية بشكلٍ دائم لمواكبة آخر التطورات، والتأكُّد من تبني أحدث المعايير الأمنية بناءً على قدرات وتقنيات المحتالين.

هيئة الحكومة الرقمية
Digital Government Authority

الاعتبارات المستقبلية

مع تغير طبيعة محاولات الاحتيال، فإن المنهجية التي تعتمدها المؤسسات، في القطاعين العام والخاص، يمكن أن تختلف وتتراوح ما بين النهج التفاعلي والنهج الاستباقي:

المنهجية التفاعلية

عدم تحديد المخاطر وعدم توضيحها جيداً؛ حيث يجهل المسؤولون حجم المخاطر المحتملة

نادراً ما يتم تحديث تقييمات المخاطر نظراً لأنّ المؤسسة تبذل جهوداً كبرى لتحديد المخاطر، ولكن لا يتم تحديث هذا التقييم إلا في حال ظهرت مشكلة معينة

ضعف الشمولية لكافة المخاطر الممكنة وفهم المخاطر بالكامل وضعف تحديد أولوياتها أثناء مرور المؤسسات أو الحكومات بتغييرات كبرى ويكون لديها أولويات أخرى، مثلا نوصي بتطوير تطبيق كلنا أمن لبلاغات الاحتيال الرقمي ليشمل كافة المخاطر الممكنة ويتم التبليغ عنها من كافة شرائح المجتمع من أفراد ومؤسسات.

هناك مستوى عالٍ من التغاضي، حيث لا توجد قيادة واضحة وتعتمد الفرق فقط على مدراء الأقسام لتصويب الأمور

المنهجية الاستباقية

يتم تحديد المخاطر بشكلٍ جيّد، ولكن يكمن التحدي الرئيس في تصميم وتطبيق الأنظمة بشكلٍ صحيح، والتأكد من تطبيق الضوابط والثقافة في مختلف أرجاء المؤسسة.

إجراء مراجعة لتقييمات المخاطر بشكلٍ منتظم، مع وجود حوار داخلي حول سُبل الوقاية المستقبلية من المخاطر بدلاً من محاولة احتواء المخاطر المعروفة في الوقت الحاضر فقط

وجود قيم واضحة وثقافة قوية لمكافحة الاحتيال، ويمكن التعلّم من أخطاء الماضي والحرص على عدم تكرارها مستقبلاً

إجراء تدقيق واسع ووضع تحدّيات أكبر. ويتم تقسيم المهام / قنوات المسؤوليات، مع تقديم تقارير منتظمة إلى الفريق القيادي

هيئة الحكومة الرقمية
Digital Government Authority

شكراً لكم

الديوان العام للمحاسبة
General Court of Audit

المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة
ARABOSAI

أساليب ووسائل الغش في بيئة تقنية المعلومات

(الوحدة الثانية)

الوحدة الثانية: أساليب ووسائل الغش في بيئة تقنية المعلومات

هدف التعلم:

التعرف على مفهوم الفساد وأساليب الغش في بيئة تقنية المعلومات

محاور الوحدة

مفهوم الفساد وأشكاله

أساليب الغش في بيئة تقنية المعلومات

مكونات الوحدة

- مفهوم الفساد وأشكاله
- أساليب الغش في بيئة تقنية المعلومات

محاور الجلسة

- مفهوم الفساد وبعض أهم تعريفاته
- أشكال الفساد الإداري وصوره
- أهم أسباب الفساد الإداري
- العوامل التي تساعد على الحد من الفساد الإداري

مفهوم الفساد وبعض أهم تعريفاته

اتفاقية الأمم المتحدة لمكافحة الفساد	هذه الاتفاقية تعد الصك العالمي الوحيد الملزم قانونيًا لمكافحة الفساد، إذ تهدف إلى تبادل الخبرات والأمثلة الناجحة في مكافحة الجرائم المالية والفساد.
الشفافية والإنفاذ	يتضمن ذلك تعزيز شفافية العمليات المالية، وإنفاذ قوانين مكافحة الفساد، وحرمان الأفراد الفاسدين من الملاذات الآمنة.
تطوير ثقافة النزاهة	يشمل ذلك نشر التوعية حول مخاطر الفساد وتعزيز التدابير الوقائية.

مفهوم الفساد وتعريفاته

الفساد

صندوق النقد الدوليIMF

وهو مؤسسة مالية دولية تتخذ من واشنطن العاصمة مقرًا لها، ويضم ١٩٠ دولة عضواً

يهدف إلى تحقيق النمو والرخاء المستدام لجميع دوله الأعضاء من خلال دعم السياسات الاقتصادية، وتعزيز الاستقرار المالي، وتعزيز التعاون في المجال النقدي على مستوى العالم

يسعى صندوق النقد إلى تحقيق استدامة النمو وتحسين حياة المواطنين في جميع أنحاء العالم

مفهوم الفساد وتعريفاته

الفساد

المراقبة والتقييم	يقوم بتقديم تقارير دورية حول الاقتصادات المختلفة، ويحدد التحديات والنقاط الضعيفة في النظام المالي والاقتصادي.
التوجيه والإصلاح	يقدم توجيهًا فنيًا للدول الأعضاء لتحسين سياساتها المالية والنقدية، وتعزيز الشفافية والمساءلة.
برامج التمويل	يوفر تمويلًا للدول المتأثرة بأزمات مالية أو اقتصادية، مع شروط تعزز من مكافحة الفساد.

مفهوم الفساد وتعريفاته

الفساد

إعلان لجنة وضع السياسات التابعة لمجلس مديري صندوق النقد الدولي المتعلق بالشراكة من أجل التنمية العالمية المستدامة

في عام ١٩٩٦م

المتضمن التشديد على أهمية تعزيز الحكمة الرشيدة في جميع جوانبها

- المساءلة
- الاستقرار السياسي وغياب العنف
- فاعلية الحكومة
- الجودة التشريعية
- سيادة القانون
- الحد من الفساد

مفهوم الفساد وتعريفاته

الفساد

سوء استخدام الصلاحيات الممنوحة للحصول على منافع شخصية

حسب تعريف منظمة الشفافية الدولية

سوء استخدام الأموال العامة و/أو المنصب من أجل مكاسب شخصية أو سياسية

التعريف العلمي حسب تعريف مجموعة البنك الدولي

مفهوم الفساد وتعريفاته

الفساد

طلب أو عرض أو تقديم أو قبول رشوة أو أي منافع غير مستحقة أو وعد بذلك على نحو مباشر أو غير مباشر، والتي من شأنها أن تشوه الأداء الصحيح لأي واجب أو سلوك مطلوب من متلقي تلك الرشوة، أو المنفعة غير المستحقة أو الوعد بذلك

حسب التعريف الوارد في اتفاقية القانون المدني حول الفساد المبرمة من قبل المجلس الأوروبي

أشكال الفساد الإداري وصوره

الفساد الإداري

يعرف بأنه انتهاك القوانين والانحراف عن تأدية الواجبات الرسمية في القطاع العام لتحقيق مكسب مالي شخصي، ويفهم من خلال هذا التعريف الواسع بأنه الإخلال بشرف الوظيفة ومهنيتها وبالقيم والمعتقدات التي يؤمن بها الشخص، وكذلك هو إخضاع المصلحة العامة للمصالح الشخصية.

أشكال الفساد الإداري وصوره

الفساد الإداري

تختلف أنواع الفساد الإداري والمالي تبعا للزاوية التي تنظر له منها ويختلف طبقا للحيثيات المرتبطة بها وكالاتي:

ا-أنواع الفساد من حيث الحجم

أ- الفساد الصغير (فساد الدرجات الوظيفية الدنيا): وهو الفساد الذي يمارس من فرد واحد دون تنسيق مع الآخرين لذا نراه ينتشر بين صغار الموظفين عن طريق استلام رشاوي من الآخرين

ب- الفساد الكبير (فساد الدرجات الوظيفية العليا من الموظفين): والذي يقوم به كبار المسؤولين والموظفين لتحقيق مصالح مادية أو اجتماعية كبيرة وهو أهم واشمل وأخطر لتكليفه الدولة مبالغ ضخمة.

أشكال الفساد الإداري وصوره

الفساد الإداري

٢-أنواع الفساد من حيث الانتشار

أ- فساد دولي، وهذا النوع من الفساد يأخذ مدى واسعاً عالميا يعبر حدود الدول وحتى القارات ضمن ما يطلق عليها (بالعولمة) بفتح الحدود والمعابر بين البلاد وتحت مظلة ونظام الاقتصاد الحر، وترتبط المؤسسات الاقتصادية للدولة داخل وخارج البلد بالكيان السياسي أو قيادته لتمرير منافع اقتصادية نفعية يصعب الفصل بينهما لهذا يكون هذا الفساد أخطبوطياً يلف كيانات واقتصادات على مدى واسع ويعتبر الأخطر نوعاً.

ب - فساد محلي، وهو الفساد الذي ينتشر داخل البلد الواحد في منشأته الاقتصادية وضمن المناصب الصغيرة، من الذين لا ارتباط لهم خارج الحدود (مع شركات أو كيانات كبرى أو عالمية).

أشكال الفساد الإداري وصوره

بعض أشكال الفساد الإداري

١- استغلال المنصب العام	حيث يلجأ البعض لاستغلال الوظيفة العامة في الحصول على امتيازات خاصة، وتبرز بشكل واضح في احتكار شخصيات متنفذة وذوي مناصب عليا في السلطة بعض الخدمات والسلع والمواد الأساسية، وحصول آخرين على بعض الوكالات التجارية، ومشاركة رجال أعمال وتجار ومستثمرين من الباطن، إضافة إلى التصرف بالأملاك العامة بطريقة غير قانونية.
٢-الاعتداء على المال العام	من خلال الحصول على إعفاءات ضريبة وجمركية أو تراخيص لأشخاص أو شركات بشكل غير قانوني وبدون وجه حق. كما تم في حالات أخري أخذ أموال عامة تحت مسميات إعانات أو مساعدات مباشرة وغير مباشرة بدون وجه حق.
٣-تهريب الأموال	عن طريق قيام بعض المسئولين بتهريب الأموال العامة التي تم الاستيلاء عليها بشكل غير قانوني وبدون وجه حق إلي الخارج.

أشكال الفساد الإداري وصوره

بعض أشكال الفساد الإداري

٤- غياب النزاهة والشفافية في العطاءات الحكومية	من خلال إحالة عطاءات حكومية بطرق غير شرعية لشركات ذات علاقة بمسئولين كبار في السلطة أو لأقربائهم. إضافة إلي استخدام بعض الوسائل غير القانونية والحيل في ترسيه المشتريات الحكومية ومواصفاتها.
٥-مخالفة قانون الخدمة المدنية	تمثل في قيام العديد من المسئولين وأصحاب المناصب العليا بالتعيينات العشوائية في أجهزة السلطة دون حاجة حقيقية، إضافة إلي تعيينات في مناصب دون مؤهلات مما أدي إلي إهدار المال العام وترهل الجهاز الإداري وتضخمه وضعف الأداء العام.

من الأمثلة على الفساد الإداري

أهم أسباب الفساد الإداري

أهم أسباب الفساد الإداري

١- أسباب بيولوجية وفيزيولوجية	وهي جميع الأسباب التي دافعها الأولي والأساسي هو ما اكتسبه الفرد عن طريق الوراثة وكل ما يتعلق بالخلفية السابقة من حياته وما تركته من آثار على سلوكياته وتصرفاته.
٢-أسباب سياسية	يقصد بالأسباب السياسية هي غياب الحريات والنظام الديمقراطي، ضمن مؤسسات المجتمع المدني، ضعف الأعلام والرقابة.
٣-عدم استقلالية القضاء	يعد استقلال القضاء من المبادئ الهامة والأساسية التي تقوم عليها الدولة وتتجلى اهميتها في وجود سلطة قضائية نزيهة تمارس عملها بشكل عادل وتمتلك سلطة الردع للمخالفين للقانون دون تمييز وتعمل على إشاعة العدل بين أفراد المجتمع، أما في حالة وصول الفساد للسلطة القضائية فان ذلك يمثل نسف للجهود الرامية للحد من هذه الظاهرة وبالتالي ينبغي العمل على تدعيم القضاء والمحافظة على استقلالية ليكون بمثابة صمام الأمان للمجتمع ورادعا قويا لكل من يحاول الاعتداء على حقوق وممتلكات الآخرين.

أهم أسباب الفساد الإداري

أهم أسباب الفساد الإداري

٤- أسباب هيكلية

تُعزى الأسباب الهيكلية إلى وجود هياكل قديمة للأجهزة الإدارية لم تتغير على الرغم من التطور الكبير والتغير في قيم وطموحات الأفراد، هذا كان الأثرة الكبير في دفع العاملين إلى اتخاذ مسالك وطرق تعمل تحت ستار الفساد الإداري بغية تجاوز محدودية الهياكل القديمة وما ينشأ عنها من مشاكل تتعلق بالإجراءات وتضخم الأجهزة الإدارية المركزية.

٥- أسباب اجتماعية

يتمثل بالحروب وأثارها ونتائجها في المجتمع والتدخلات الخارجية، الطائفية والعشائرية والمحسوبيات، القلق الناجم من عدم الاستقرار نتيجة الأوضاع والتخوف من المجهول القادم لذا استدعى. جمع المال بأي وسيلة لمواجهة هذا المستقبل والمجهول الغامض

أهم أسباب الفساد الإداري

أهم أسباب الفساد الإداري

٦- أسباب أخرى

قلة الوعي الحضاري وانتشار الجهل والتخلف والفقر والتفاوت من الدخول بين الأفراد

التخلف البنيوي في الهياكل المعنية بإدارة اقتصاد الدولة، فضلا عن التخلف التقني والتكنولوجي

محدودية دور وسائل الإعلام وضعف قدرتها على فضح الفساد

عدم وجود الشفافية في محيط العمل

العوامل التي تساعد على الحد من الفساد الإداري

الجوانب الاقتصادية الداعمة للحد من الفساد الإداري

من أبرز العوامل التي تساعد في الحد من انتشار الفساد الإداري ما يلي:

- الأجور الجيدة وتناسبها مع الأداء المقدم من قبل العاملين في القطاعين العام والخاص.
- نظام الخدمة لمستند إلى الكفاءة.
- استخدام مبدأ التعويضات للعاملين (الأمن الوظيفي) بما يضمن مستوى معيشي لائق.
- الاستقرار الاقتصادي الكلي.
- توزيع الموارد بصورة أكثر عدالة.
- تفضيل القطاعات التي تخلق فرص عمل جيدة وتزيد الإنتاجية (قطاع الخدمات).

العوامل التي تساعد على الحد من الفساد الإداري

البيئة التشريعية والإدارية والتنظيمية

أما على صعيد الأطر التشريعية والتنظيمية، فمن أهم العوامل ما يلي:

وجود قوانين صارمة ترتكز على سلسلة من الإجراءات العقابية وهياكل قوية ومنظمة.

أن تكون أجهزة الدولة بصورة بيروقراطية مستندة إلى الكفاءة.

أن تكون الإدارة ذات أداء عالي تقدم الفرص بالتساوي لجميع الأهداف.

إيجاد نظام حوافز يوفر الإطار الملائم للعمل بالنسبة للموظفين كالمراجعة الدورية لسلم الأجور وغيرها من الإجراءات المحفزة.

حالة دراسية

حسن مراجع داخلي في الشركة الوطنية للخدمات الاجتماعية، طلب منه مدير عام المراجعة دراسة بعض البيانات المستخرجة من النظام المالي للشركة عن السنوات الخمس الماضية، وبعض البيانات الأخرى التي وردت للإدارة مؤخراً من قسم الرواتب والأجور.

في اليوم التالي قدم حسن تقريره لمكتب مدير عام المراجعة، وذكر له بأنه قد وجد أن عدد الحوالات البنكية الشهرية غير مطابق لعدد الموظفين في الشركة، وأن قام بإرسال بريد إلكتروني إلى رئيس قسم الرواتب والأجور الذي يتمتع بخبرة طويلة في أعمال القسم، وأنه أجاب على البريد بأن حالة عدم التطابق طبيعية بسبب عدم ثبات عدد الموظفين خلال السنة، وحالات التعيين والاستقالة والتقاعد والانقطاع عن العمل.

ما هو تقييمك لهذه الحالة، وهل توجد في هذه الحالة شبه فساد مالي؟

كمراجع ما هو الإجراء الواجب اتخاذه في هذه الحالة؟

تعليمات حل التمرين:

التفكير المنفرد ٣ د، العمل ضمن المجموعة ٥ د، المناقشة والحل ١٧ د

مفهوم الفساد وأشكاله

الخلاصة

- يتمثل الفساد في سوء استخدام الأموال العامة و/أو المنصب، والذي في الغالب يكون من أجل تحقيق مكاسب شخصية أو سياسية، ولكون الفساد من أكثر المشكلات التي تعاني منها الدول، فقد تم تواصلت الجهود من أجل الحد منه وسن التشريعات الدولية لمحاربته.
- للفساد صور وأشكال متعددة من الأمثلة الشائعة له (العمولات، والرشوة، والاختلاس والسرقة، والمحسوبية، والابتزاز والتزوير.
- تعتبر الإصلاحات الاقتصادية والتشريعية من أهم العوامل التي تساعد على الحد من الفساد الإداري.

شكراً لكم

الديوان العام للمحاسبة
General Court of Audit

فهم بيئة تقنية المعلومات والأمن السيبراني ودراستها

الديوان العام للمحاسبة

المركز السعودي للمراجعة المالية والرقابة على الأداء

إدارة الأمـن السيبرانـي

مكونات العرض

- تعريف بيئة تقنية المعلومات.
- طرق فهم بيئة تقنية المعلومات.
- أهمية فهم بيئة تقنية المعلومات.
- دراسة بيئة تقنية المعلومات.
- تعريف بيئة الأمن السيبراني.
- مكونات بيئة الأمن السيبراني.
- الموضوعات الرئيسية التي يجب.

دراستها لفهم بيئة الأمن السيبراني.

بيئة تقنية المعلومات

تعريف بيئة تقنية المعلومات

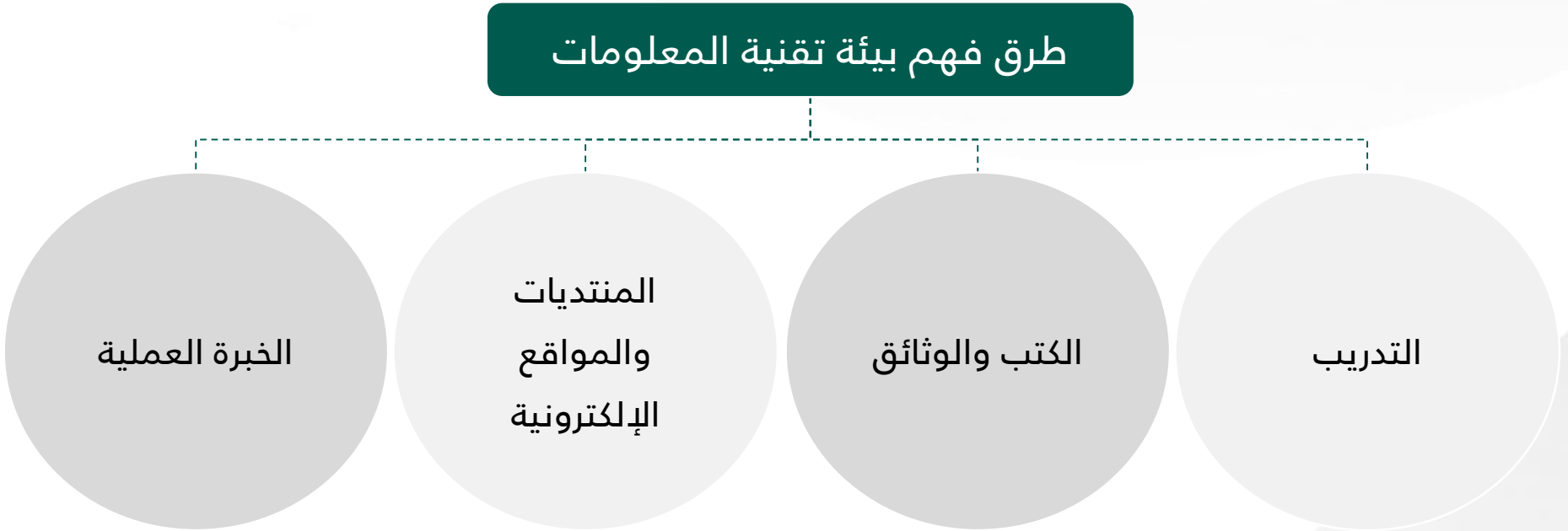
- **تعريف بيئة تقنية المعلومات:**

وهي مجموعة الأنظمة والشبكات والأجهزة التي تستخدمها المؤسسة لمعالجة البيانات وإنشاءها ونقلها، ويمكن أن تتكون بيئة تقنية المعلومات من مجموعة متنوعة من المكونات، بما في ذلك:

- أجهزة الكمبيوتر
- الخوادم
- شبكات الحاسوب
- تطبيقات الحاسوب
- بيانات الحاسوب

فهم بيئة تقنية المعلومات

يساعد فهم بيئة تقنية المعلومات في معرفة كيفية عمل أنظمة تقنية المعلومات وكيفية حماية البيانات من التهديدات بالإضافة الى المساعدة في اتخاذ قرارات مستنيرة حول أمن المعلومات والمخاطر.



فهم بيئة تقنية المعلومات

- **التدريب:**

يمكن أن يساعد التدريب في تطوير فهم أساسي لتقنية المعلومات، ويمكن أن يقدم المهارات والمعارف الأساسية المهمة لفهم كيفية عمل أنظمة تقنية المعلومات.

- **الكتب والوثائق:**

تساعد الكتب والوثائق في التعمق في الموضوعات المحددة، فيمكنها أن توفر معلومات حول مكونات تقنية المعلومات المختلفة والتقنيات المستخدمة لحماية البيانات.

فهم بيئة تقنية المعلومات

- **المنتديات والمواقع الإلكترونية:**

تساعد المنتديات في التواصل مع الخبراء الآخرين والحصول على المساعدة، ويمكن أن توفر منتدى للمناقشة وتبادل المعلومات حول تقنية المعلومات والأمن السيبراني.

- **الخبرة العملية:**

تساعد الخبرة العملية في تطبيق ما تعلمته في العالم الحقيقي، بحيث يمكن أن تمنح الخبرة العملية فهمًا أفضل لكيفية عمل أنظمة تقنية المعلومات في بيئة حقيقية.

إرشادات لفهم بيئة تقنية المعلومات

ابدأ بالأساسيات

- من المهم أن تفهم الأساسيات قيل التقدم في المفاهيم المتقدمة، ويمكن أن تساعد الكتب والوثائق والتدريب في ذلك

ابحث عن الخبراء

- يوجد العديد من الخبراء المتاحين للمساعدة، ويمكن أن تساعد المنتديات والمواقع الإلكترونية وخبرات العمل في العثور على الخبراء المناسبين

مارس ما تعلمته

- أفضل طريقة لتعلم شيء جديد هي ممارسته، العمل على تطبيق ما تم تعلمه في العالم الحقيقي

دراسة البيئة

- بعد فهم البيئة يمكن دراسة المكونات والتقنيات المحددة التي تتكون منها بيئة تقنية المعلومات الخاصة بك، وقد تساعد الدراسة في تحديد المخاطر المحتملة وكيفية تجنبها

خطوات دراسة بيئة تقنية المعلومات

جمع معلومات حول مكونات تقنية المعلومات:

هذا يشمل أجهزة الكمبيوتر والخوادم، والشبكات، والتطبيقات، والبيانات.

فهم كيفية عمل هذه المكونات معًا:

سيساعد على فهم كيفية حماية بياناتك.

البحث عن التهديدات المحتملة:

التهديدات خارجية أو داخلية.

ضع خطة للحماية من التهديدات:

تنفيذ تدابير أمنية مثل التحكم في الوصول والتشفير والنسخ الاحتياطي.

بيئة الأمن السيبراني

تعريف بيئة الأمن السيبراني

فهم بيئة الأمن السيبراني ودراستها أمر مهم للمؤسسات والأفراد على حد سواء، بحيث تساعد في معرفة كيفية عمل أنظمة الأمن السيبراني وكيفية حماية البيانات من التهديدات في اتخاذ قرارات مستنيرة حول أمن المعلومات ومخاطر الأمن السيبراني.

تعريف بيئة الأمن السيبراني:-

وهي مجموعة الأنظمة والتقنيات والإجراءات التي تستخدمها المؤسسات لحماية بياناتها من التهديدات والمخاطر السيبرانية.

مكونات بيئة الأمن السيبراني

تتكون بيئة الأمن السيبراني من مجموعة متنوعة من المكونات، بما في ذلك:

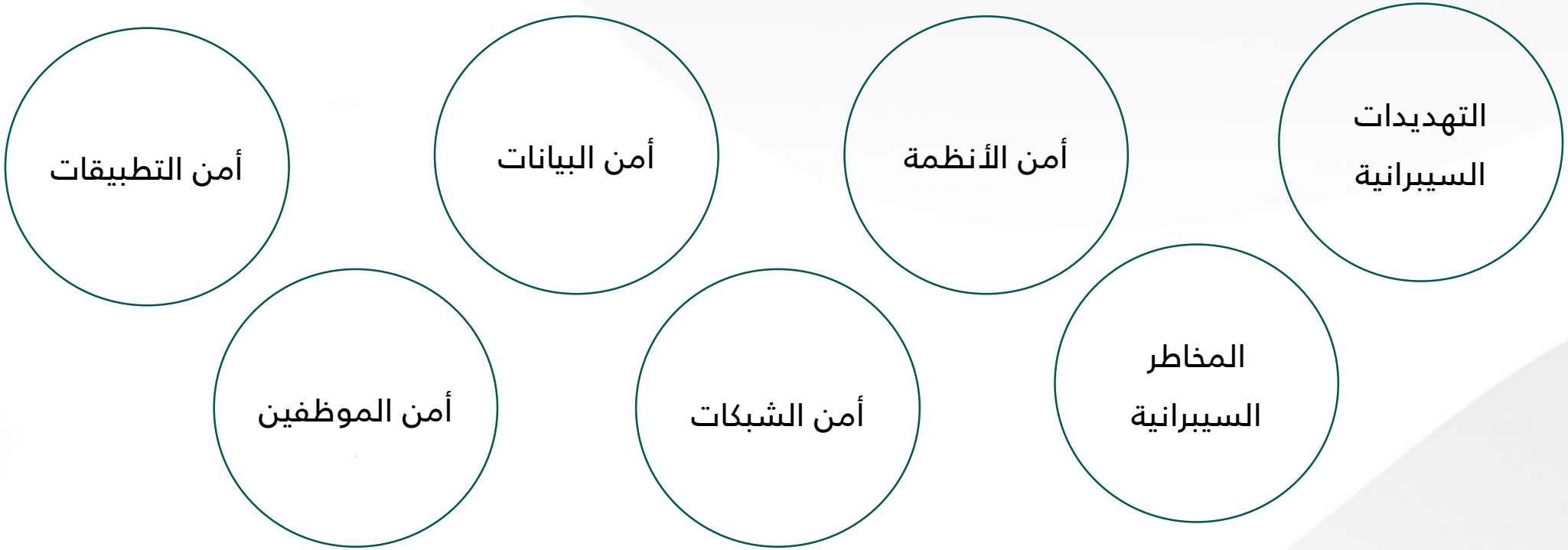
الأنظمة الأمنية، مثل جدار الحماية وبرامج مكافحة الفيروسات.

التقنيات الأمنية، مثل التشفير والتعرف على الوجه.

الإجراءات الأمنية، مثل سياسة الوصول والتحكم في الوصول.

فهم بيئة الأمن السيبراني

مواضيع رئيسية يجب دراستها لفهم بيئة الأمن السيبراني:



مواضيع الأمن السيبراني

- **التهديدات السيبرانية:**

هي أي شيء قد يضر بأنظمة تقنية المعلومات أو البيانات، يمكن أن تكون التهديدات السيبرانية خارجية أو داخلية. وتشمل التهديدات الخارجية الهجمات الإلكترونية مثل الاختراق وبرامج الفدية، أما التهديدات الداخلية فهي الأخطاء البشرية أو سوء التصرف.

- **المخاطر السيبرانية:**

هي احتمال وقوع ضرر من تهديد سيبراني، ويمكن تقييم المخاطر السيبرانية من خلال تقييم احتمالية وقوع التهديد وتأثيره المحتمل.

- **أمن الأنظمة:**

هو حماية الأنظمة المادية والبرمجية من التهديدات، وقد يساعد أمن الأنظمة في حماية البيانات من الوصول غير المصرح به أو التغيير أو التلف.

مواضيع الأمن السيبراني

- **أمن الشبكات:**

هو حماية الشبكات من التهديدات ويساعد في حماية البيانات من الوصول غير المصرح به أو التغيير أو التلف أثناء النقل.

- **أمن البيانات:**

هو حماية البيانات من التهديدات ويهدف لحماية البيانات من الوصول غير المصرح به أو التغيير أو التلف أثناء التخزين أو المعالجة.

- **أمن التطبيقات:**

هو حماية التطبيقات من التهديدات ويهدف في حماية البيانات من الوصول غير المصرح به أو التغيير أو التلف أثناء الاستخدام.

- **أمن الموظفين:**

هو حماية الموظفين من التهديدات وقد يساعد أمن الموظفين في حماية البيانات من الوصول غير المصرح به أو التغيير أو التلف من قبل الموظفين.

شكراً لكم

الديوان العام للمحاسبة

المركز السعودي للمراجعة المالية والرقابة على الأداء

إدارة الأمـن السيبرانـي

التوصيات المقترحة :

السلام عليكم ورحمة الله وبركاته

في البداية أود أن أقدم شكري والشكر نيابة عن قيادة الجهاز المركزي للرقابة والمحاسبة – الجمهورية اليمنية لإتاحة الفرصة لنا بالمشاركة والاستفادة من المعلومات المقدمة في اللقاء التدريبي والشكر موصول لقيادة ديوان المحاسبة السعودي والمنظمة العربية للأجهزة العليا للرقابة (الأرابوساي) وكل من ساهم أو شارك في التنظيم أو الإشراف أو التدريب لكل فعاليات اللقاء التدريبي ولما قُدِّم فيه من المعلومات الغنية بالفائدة والمتعلقة بالأشكال المختلفة للمخاطر المصاحبة لتشغيل البيانات الالكترونية والأساليب الحديثة لاكتشاف تلك المخاطر وكيفية تحديد مواطن الفساد والاحتيال.

بالنسبة للتوصيات التي نقترح أخذها في الاعتبار هي كالتالي:

1- لماذا لا تتبنى المنظمة العربية مشروع بناء برنامج معلوماتي موحد يتم استخدامه من قبل كافة الأجهزة العليا للرقابة في نطاق المنظمة في الأتي :
   - لتوثيق كل إجراءات التدقيق بدءً من أعمال التخطيط وانتهاء بإعداد التقرير الرقابي.
   - لتسهيل أعمال التدقيق من خلال التوقعات بحسب تصنيف مواضيع المراجعة والبيانات المخزنة سابقاً، ويمكن الاستفادة في ذلك من تقنيات الذكاء الاصطناعي.

   وذلك على غرار ما قامت به المنظمة من توحيد منهجية العمل في جانب التدريب الالكتروني المتمثل بمنصة الارابوساي للتعلم الالكتروني كتجربة سابقة ناجحة قامت بهاالمنظمة .

2- نوصي بالاهتمام بشكل أكبر على فهم الجانب التقني المتعلق بالسجلات الرقابية الالكترونية، ما هي ؟ وكيف يمكن تكوينها؟ وما نوع البيانات التي لابد أن تتضمنها؟ ومتى تكون هذه الملفات محل شك ، وما الإجراءات التي ينبغي على المراجع القيام بها عند الشك في صحة هذه الملفات ؟

   لأنها عنصر رئيسي من عناصر التحكم لا استغناء عنه في اكتشاف التحريف في البيانات والتلاعب بها واكتشاف المنفذون، وبدونها يكون غالباً من الصعب جداً اكتشاف التحريف والتلاعب بالبيانات حتى لوكان التحليل باستخدام التطبيقات الحديثة مثل IDEA ,ACL or EXCEL.

خالص تحياتي لكم،،،

فيصل أحمد الربيعي

الجهاز المركزي للرقابة والمحاسبة

توصيات اللقاء التدريبي حول مخاطر التشغيل الإلكتروني للبيانات وكيفية اكتشاف

1) من خلال الجوانب النظرية والحالات الدراسية التي تم استعراضها وتجارب الأجهزة الأعضاء، توجد جوانب عديدة تحتاج لمزيد من الحالات العملية، في الأمن السيبراني مثلاً، واستعراض لحالات عملية حول مظاهر الفساد والتعدي على الأموال العامة وخطوات التدقيق التي تم اتباعها لاكتشافها.
2) قدم البرنامج معلومات مفيدة وتم استعراض ومشاركة التجارب حول موضوع اللقاء، ونوصي بتكرار تقديمه خلال الفترة القادمة.
3) الوقت لم يكن كافٍ لاستعراض الموضوعات باستفاضة، وقد يكون من المناسب تنفيذه خلال مدة أطول، كما تم اقتراح أن يكون هناك مجموعات من المشاركين يتم تدريبها على مراحل لتأهيلهم كأخصائيين في موضوع محدد، ويتم تنفيذ البرامج التدريبية الخاصة بهم من قبل جهاز واحد أو أكثر.
4) نوصي بتقديم دورات مستقلة في الأمن السيبراني.
5) نوصي بتقديم دورات مستقلة في تحليل البيانات باستخدام الوسائل الرقمية.
6) أن يكون هناك فرصة لتقديم البرنامج من خلال مدربين من أكثر من جهاز، بما يثري الموضوع ويعزز من فرص التعاون وتبادل الخبرات.
7) يقترح المشاركون أن يكون مقر الإقامة في مقر إقامة (واحد) لمزيد من التواصل والتعارف بين المشاركين خلال فترة ما بعد انتهاء التدريب.