هيئة الحكومة الرقمية
Digital Government Authority

الدليل الاسترشادي لمكافحة الاحتيال الرقمي

ديسمبر، 2025
نوع الوثيقة : دليل استرشادي
تصنيف الوثيقة : عام
رقم الإصدار : 1.0
رقم الوثيقة: DGA-1-2-5-232

المحتويات

01. مقدمة

حرصًا من هيئة الحكومة الرقمية على تحقيق أهدافها الإستراتيجية، ودعم تحقيق مستهدفات رؤية السعودية (2030)، ومن أجل تعزيز حماية الجهات الحكومية والمستفيدين من المخاطر الرقمية المتزايدة، ومع التوسع السريع في استخدام التقنيات الرقمية، ظهرت الحاجة إلى وضع دليل استرشادي واضح وشامل لمكافحة الاحتيال الرقمي؛ يهدف إلى تعزيز الثقة بين الأفراد والجهات الحكومية عن طريق توفير تجربة مستخدم آمنة وفعالة، وضمان الحماية الشاملة ضد الاحتيال الرقمي.

تؤدي هيئة الحكومة الرقمية دورًا تنظيميًّا في تعزيز الأمان الرقمي عن طريق وضع الضوابط والمعايير والأدلة الاسترشادية التي تمكّن الجهات الحكومية من بناء القدرات والإجراءات اللازمة لمواجهة الاحتيال الرقمي بصورة فعّالة. وفي هذا السياق، أعدّت الهيئة "الدليل الاسترشادي لمكافحة الاحتيال الرقمي"؛ لدعم جهود الجهات الحكومية في تطوير ممارسات إدارة مخاطر الاحتيال الرقمي وتحسينها ويمكن للجهات الحكومية التنسيق مع هيئة الحكومة الرقمية؛ لتطوير حلول مخصصة لمواجهة التحديات الخاصة بمكافحة الاحتيال الرقمي وذلك لتوحيد جهود الجهات الحكومية.

إنّ مواجهة الاحتيال الرقمي تتطلب تعاونًا شاملًا بين الجهات الحكومية والقطاعات الأخرى المختلفة. وغالبًا ما يحدث الاحتيال على مستويات رقمية متعدّدة، مع تأثيراته متعدّدة الجوانب. ولا يُعدّ الاحتيال الرقمي مسألة مالية فقط، بل له تأثير نفسي واجتماعي على المتضررين. ويقدم هذا الدليل الاسترشادي إلى تقديم أدوات عملية وتوصيات لممارسي إدارة المخاطر وأعضاء الإدارة العليا عن أفضل السبل لتنظيم جهودهم لمكافحة الاحتيال الرقمي، وتقليل آثاره على المجتمع.

02. أهداف الدليل الاسترشادي

يهدف هذا الدليل إلى دعم الجهات الحكومية في تعزيز ثقتها فيما بينها وبين مستفيديها، وتقليل تأثير الاحتيال الرقمي عليها، عن طريق تحقيق الأهداف الآتية:

01 تحسين جودة الخدمات الحكومية الرقمية عن طريق الحدّ من تأثير الاحتيال الرقمي عليها، وضمان تقديم خدمات أكثر أمانًا وكفاءة للمستفيدين.

02 تمكين الجهات الحكومية عبر تزويدها بأُسس واضحة لوضع أطر فعّالة لإدارة مخاطر الاحتيال الرقمي؛ بما يسهم في تحسين استجابتها للتحديات الرقمية.

03 مساعدة الجهات الحكومية على تبني مبادئ مكافحة الاحتيال الرقمي وممارساتها، وفقًا لأفضل المعايير العالمية، وتعزيز قدرتها على مواجهة المخاطر الرقمية بكفاءة.

04 بناء ثقافة راسخة لمكافحة الاحتيال الرقمي، وتعزيز إدارة المخاطر في الخدمات الحكومية؛ لضمان استمرارية الخدمات، وحماية المصلحة العامة.

05 الإسهام في تطبيق منهجية فعّالة لإدارة مخاطر الاحتيال الرقمي في الجهات الحكومية؛ مما يساعد على تحسين إستراتيجيات الوقاية والرصد، والتعامل مع الاحتيال.

06 المشاركة الاستباقية في الجهود الوطنية لمكافحة الاحتيال الرقمي، عن طريق التعاون مع القطاعات المختلفة؛ لتفعيل إستراتيجيات شاملة وموحدة.

07 تعزيز الممارسات والأطر الحالية، والإسهام في تفعيل نهج موحّد لإدارة مخاطر الاحتيال الرقمي؛ بما يسهم في تحسين مستوى الحماية والاستجابة للمخاطر.

08 نشر الوعي في القطاع الحكومي بمفاهيم الاحتيال الرقمي الرئيسة، وتعزيز فهم الجهات لأهمية مكافحة الاحتيال، وحماية مصالح المستفيدين.

03. نطاق الدليل الاسترشادي

يحدّد هذا الدليل الإرشادات والتوصيات العامة التي يجب على الجهات الحكومية اتباعها للحد من الاحتيال الرقمي على منصاتها وتطبيقاتها الرقمية ،وينطبق الدليل على جميع الخدمات والمنتجات الرقمية التي توفرها الجهات الحكومية، مع مراعاة اختلاف احتياجاتها وحجم انشطتها، كما يتيح للجهات الاستفادة من أفضل الممارسات لتطبيق الإجراءات بما يتناسب مع طبيعة عملها، وبطريقة تعزّز استمرارية تقديم الخدمات بكفاءة، ويشتمل الدليل على ثلاثة ركائز رئيسة ،وفقًا للآتي:

- **مخاطر الاحتيال الرقمي:** والمتضمنة تعريف الاحتيال الرقمي، وأنواع مخاطر الاحتيال الرقمي في الجهات الحكومية، إلى جانب تسليط الضوء على أهمية جهود مكافحة الاحتيال الرقمي، وتوضيح سماته.
- **حوكمة مكافحة الاحتيال الرقمي:** والتي تهدف إلى مساعدة الجهات الراغبة في تطوير أو إنشاء وظائف متخصصة في إدارة مخاطر الاحتيال الرقمي.
- **منهجية مكافحة الاحتيال الرقمي:** والتي تتضمن عدد من التوصيات غير المُلزمة تهدف الى تحفيز الجهات الحكومية على استخدام هذه التوصيات لإدارة مخاطر الاحتيال الرقمي لديها بصورة فعالة، بما يتناسب مع احتياجاته.

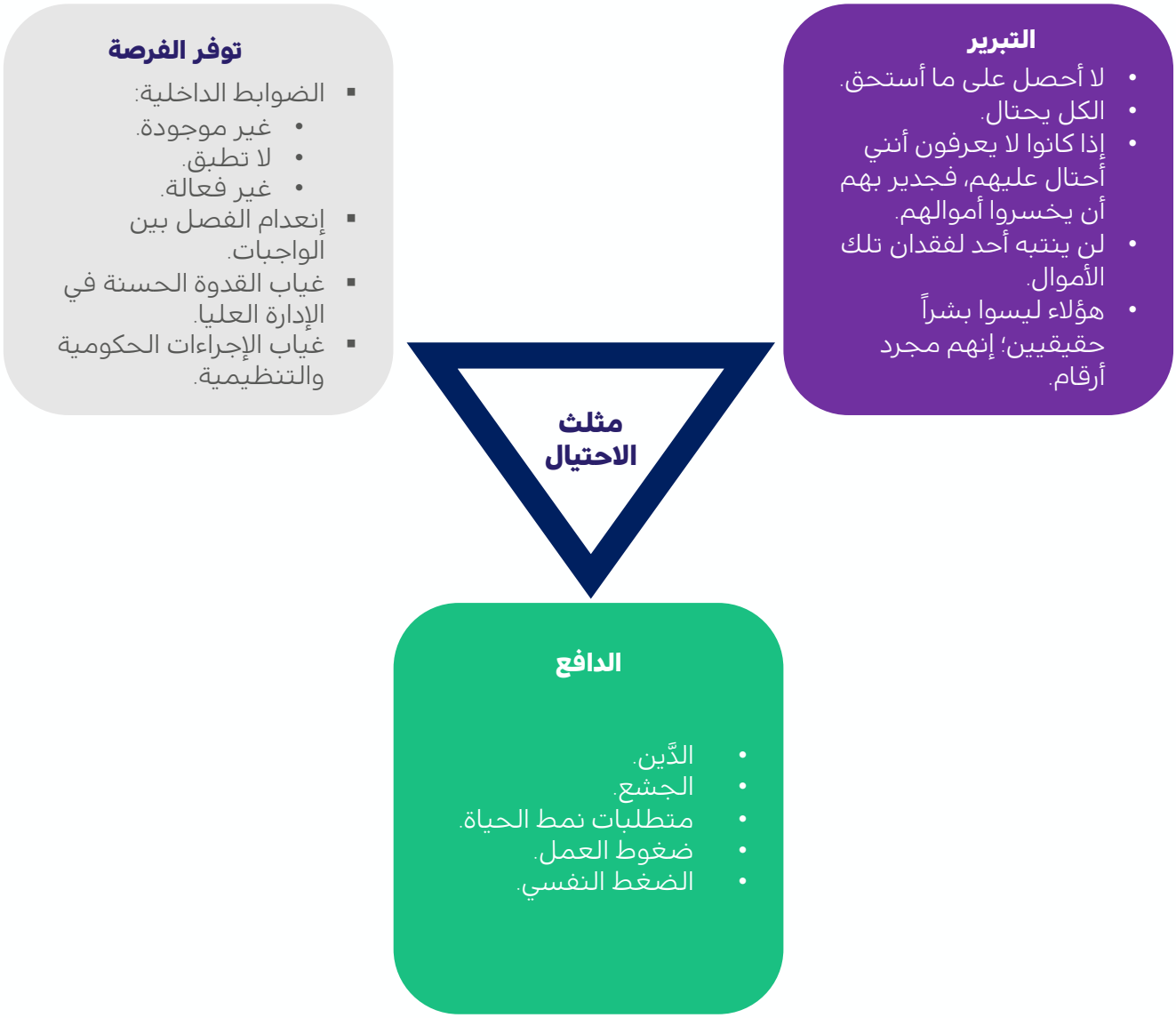
04. الفئات المستهدفة

يستهدف الدليل جميع الجهات الحكومية التي تقدّم خدمات ومنتجات رقمية، بغض النظر عن حجمها أو طبيعة أعمالها، وتختلف مدى قابلية تطبيق الدليل الاسترشادي بناءً على نوع الخدمات المقدمة ومستوى تعرّضها لمخاطر الاحتيال الرقمي، ودعم المختصين في فرق إدارة المخاطر والاحتيال في تصميم خطة فعّالة للمكافحة مخاطر الاحتيال الرقمي وتنفيذها.

05. مخاطر الاحتيال الرقمي

5.1. تعريف الاحتيال

يُعدّ الاحتيال ظاهرة شائعة في التعاملات التجارية، ويتسبب باستمرار في خسائر مالية أو أضرار أخرى للأفراد والمؤسسات. وفي أساسه، هو عملية احتيالية يرتكبها فرد أو جهة؛ بهدف تحقيق مكاسب شخصية.



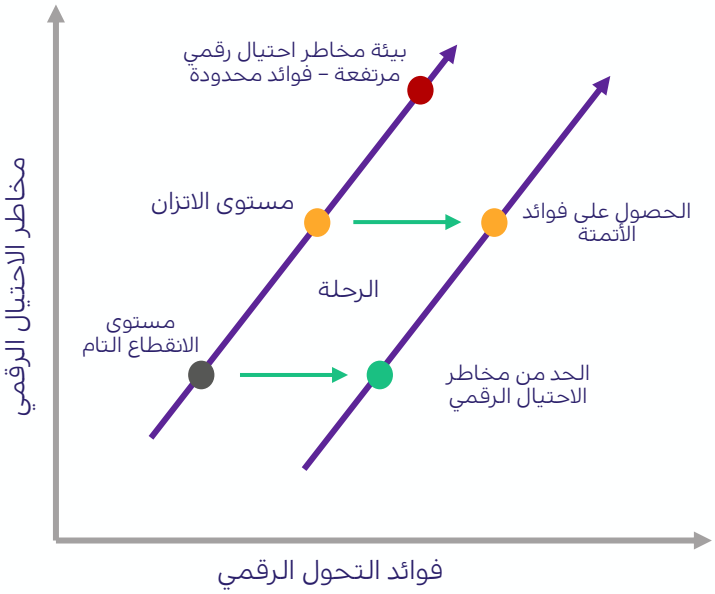
الشكل 1 -مثلث الاحتيال

ويعرف الاحتيال الرقمي بأنّه أي نوع من الأنشطة الاحتيالية التي تُنفَّذ باستخدام التقنية أو المنصات الرقمية،ويشمل هذا النوع من الاحتيال التلاعب التقني أو الخداع، للحصول على قيمة مادية أو معلومات حساسة عن طريق الوسائل الرقمية. يوضّح الشكل رقم (1) "مثلث الاحتيال" العوامل الرئيسة المُسبّبة للاحتيال التي تكمن في (ثلاثة) عوامل رئيسة تتعلق بالسلوك والعواطف الإنسانية، ويوجد الاحتيال في المجتمعات المتطورة وغير المتطورة على حد سواء، لكنه يظهر بطرق مختلفة [1].

[1] ACFE Fraud Definition – Fraud Risk Management Guideline 2nd Edition.

يُعدّ "مثلث الاحتيال"[2] أداة مهمة عند تصميم أطر وأنظمة مكافحة الاحتيال، وهو تذكير بأنّ الاحتيال، رغم جوانبه التقنية، يظل في جوهره تهديدًا نابعًا من الدوافع البشرية. ومع التحول الرقمي الذي شهده المجتمع، تطور الاحتيال أيضًا إلى شكل رقمي؛ فظهر الاحتيال الرقمي، المعروف أحيانًا بالاحتيال الإلكتروني أو الجريمة الإلكترونية، بصفته خطرًا مجتمعيًّا بارزًا له تأثير محتمل يفوق الاحتيال التقليدي. ولاعتماد الاحتيال الرقمي على المنصات التقنية لاستهداف الأفراد أو الجهات؛ فإنه ينتشر بسرعة أكبر مقارنة بالاحتيال التقليدي، الذي غالبًا ما يكون محدودًا بسبب بطء انتشار مخاطره.

مخاطر الاحتيال الرقمي مقابل فوائد التحول الرقمي



الشكل 2 – مخاطر الاحتيال مقابل فوائد التحول الرقمي

على عكس الاحتيال التقليدي، يعمل الاحتيال الرقمي على إخفاء هوية المتضررين، ويعزِّز عناصر "مثلث الاحتيال" (الثلاثة)، حيث يندر أن يكون الجناة قريبين من متضرريهم. كما أنّ احتمالية القبض على الجهات الإجرامية قليلة؛ مما يزيد من دوافع الجناة، نتيجة انخفاض فرص تعرضهم للعقاب. ومع التحول الرقمي للخدمات الحكومية، زادت القدرة على الوصول إلى هذه الخدمات وتحسّنت كفاءتها، لكن هذا التحول أدى أيضًا إلى ارتفاع معدلات الاحتيال الرقمي المرتبط بها، فمع توسع رقمنة الخدمات؛ تزداد فرص المحتالين ومساحة الاستغلال المتاحة لهم. ويسلّط الشكل رقم (2) الضوء على الحالات المختلفة التي تواجهها المجتمعات والجهات من تزايد مخاطر الاحتيال الرقمي مع رقمنة خدماتها يومًا بعد يوم.

Cressey – Other peoples Money: A study in the Social Psychology of Embezzlement 1953[2]
Figure is from BIS Research Paper on Digital Fraud[3]

وقد جرى توثيق العلاقة بين الاعتماد المتزايد على البنية التحتية الرقمية وزيادة الاحتيال الرقمي بصورة جيدة، وإليكم بعض أبرز الأمثلة:

1. **أستراليا**: أفادت لجنة المنافسة والمستهلك الأسترالية بأن الأستراليين فقدوا أكثر من (851) مليون دولار أسترالي؛ بسبب عمليات الاحتيال في عام (2020م)، مما يمثل زيادة قدرها (34%)[4] مقارنةً بعام (2019م). ويرجع هذا الارتفاع بصورة كبيرة إلى زيادة البصمات الرقمية والنشاط الاحتيالي الناجم عن جائحة كورونا. وقد كانت عمليات الاحتيال الاستثمارية، والعاطفية، وإعادة توجيه المدفوعات هي الأكثر ضررًا ماليًّا.

2. **الهند**: شهدت الهند زيادة بمقدار (5)[5] أضعاف في عمليات الاحتيال المتعلقة بالدفع الرقمي؛ نتيجة لتبني واجهة المدفوعات الموحدة بصورة واسعة منذ عام (2016م). وقد أسهم تبني هذا النظام بصفته جزءًا من البنية التحتية الرقمية الأساسية في تغيير مشهد المدفوعات، وفتح مجالات جديدة للمحتالين.

3. **المملكة المتحدة**: تضاعف عدد عمليات الاحتيال المتعلقة بالضرائب، حيث انتحل المحتالون شخصية هيئة الإيرادات والجمارك في عام (2023م)؛ نتيجة لتقديم إقرارات التقييم الذاتي عبر الخدمات الرقمية. وقد أُبلغ عما يصل إلى (800,000)[6] عملية احتيال تستهدف الأفراد، حيث طلب المحتالون الدفع بناءً على تقييمات ذاتية رقمية وهمية. وتتنوع طرق الاحتيال، ويشمل ذلك تقديم خصومات وهمية، ومطالبة العملاء بتحديث بياناتهم الضريبية، أو التهديد بالاعتقال الفوري بتهمة التهرب الضريبي.

ومع استمرار الوتيرة السريعة للتحول الرقمي، سيبقى الاحتيال الرقمي حدثًا اجتماعيًّا متزايد الأهمية؛ مما يستدعي اتباع نهج موثَّق واستباقي ومنسَّق لمواجهة هذا التهديد.

Scammers capitalise on pandemic as Australians lose record $851 million to scams | ACCC[4]
How Fraudsters Exploit the Surge in Digital Payments and Online Banking[5]
Scams warning for 12 million Self Assessment customers | GOV.UK[6]

5.2. أنواع مخاطر الاحتيال الرقمي في الجهات الحكومية

هناك العديد من التصنيفات الدولية المتعلقة بمخاطر الاحتيال وكيفية قياسها ومراقبتها والتخفيف منها. وتؤكد هذه التصنيفات جميعها أنّ الاحتيال يمتد عبر أبعاد وتخصصات متعددة؛ مما يزيد من صعوبة التعامل معه. وتُعدُّ أكثر أطر الاحتيال تطورًا تلك التي توجد في القطاع المالي الدولي، حيث يتسبب هذا النوع من الاحتيال في تأثيرات كبيرة على قطاع الخدمات المالية.

ويعرّف البنك المركزي السعودي "الاحتيال"، وفقًا لإطار عمل مكافحة الاحتيال المالي، على النحو الآتي:

"يتم تعريف الاحتيال على أنه أي فعل مقصود يهدف إلى الحصول على منفعة غير مشروعة أو التسبب في خسارة لطرف آخر. ويمكن أن يكون ذلك بسبب استغلال الوسائل الفنية أو الوثائقية، أو العلاقات أو الوسائل الاجتماعية، أو استخدام القوى الوظيفية، أو الإهمال المتعمد أو استغلال نقاط الضعف في الأنظمة أو المعايير، بشكل مباشر أو غير مباشر."

وإلى جانب تأثير الاحتيال الرقمي على القطاع المالي، تواجه الجهات الحكومية أيضًا مخاطر كبيرة نتيجة الاحتيال، حيث تقدم الجهات الحكومية خدمات متنوعة تشمل: المدفوعات والمشتريات وإدارة الموظفين والخدمات الرقمية؛ مما يجعلها عرضة لمخاطر الاحتيال بصورة مشابهة لمؤسسات القطاع الخاص.

ووفقًا لإطار إدارة مخاطر الاحتيال الصادر عن لجنة المنظمات الراعية (COSO)[7] لإدارة مخاطر الاحتيال والهدر واستغلال المناصب في الجهات الحكومية، تُصنَّف المخاطر الآتية كمخاطر احتيال حرجة:

- **الاحتيال في الائتمان (القروض والضمانات)**
- **الاحتيال في المنح**
- **الاحتيال في الخدمات اللوجستية وسلسلة التوريد.**
- **الاحتيال في بطاقات الشراء والسفر.**
- **الاحتيال في الدفع المُخالِف، (يشمل البائع).**
- **الاحتيال في الإغاثة من الكوارث.**
- **الاحتيال المحاسبي.**
- **الاحتيال في بيانات الهوية.**
- **اختلاس الأصول.**
- **الاحتيال المالي.**
- **الرشوة والفساد.**
- **الاحتيال في المشتريات والعقود.**
- **الاحتيال الرقمي.**
- **الاحتيال في الرعاية الصحية.**
- **الاحتيال في الضمان الاجتماعي.**
- **الاحتيال في برامج المزايا.**

[7] COSO ACFE Fraud Risk Management Guidelines Appendix G

يمكن اعتبار الاحتيال الرقمي جزءًا من الاحتيال بصورة عامة، ولكن عندما تُستخدم التقنية الرقمية لارتكاب الاحتيال، يُعتبر ذلك احتيالًا رقميًّا؛ لأن عدم القدرة على التحكم تكمن في المجال الرقمي. ويمكن تحقيق العديد من مخاطر الاحتيال عبر الوسائل الرقمية؛ مما يجعلها تصنف بصفتها احتيالًا رقميًّا.

ويرتبط الاحتيال الرقمي ارتباطًا وثيقًا بحوادث الأمن السيبراني والاحتيال التقليدي، إلا أن هناك بعض الاختلافات الجوهرية. وتسلط ورقة لجنة بازل للرقابة المصرفية BCBS[8] الضوء على هذه الاختلافات، كما هو موضح في الشكل رقم (3). هذه الاختلافات مهمة لأغراض إدارة المخاطر وإعداد التقارير، ولكن في بيئة العمل، قد لا تتضح الخطوط الفاصلة بين الاحتيال الرقمي والأمن السيبراني والاحتيال التقليدي.

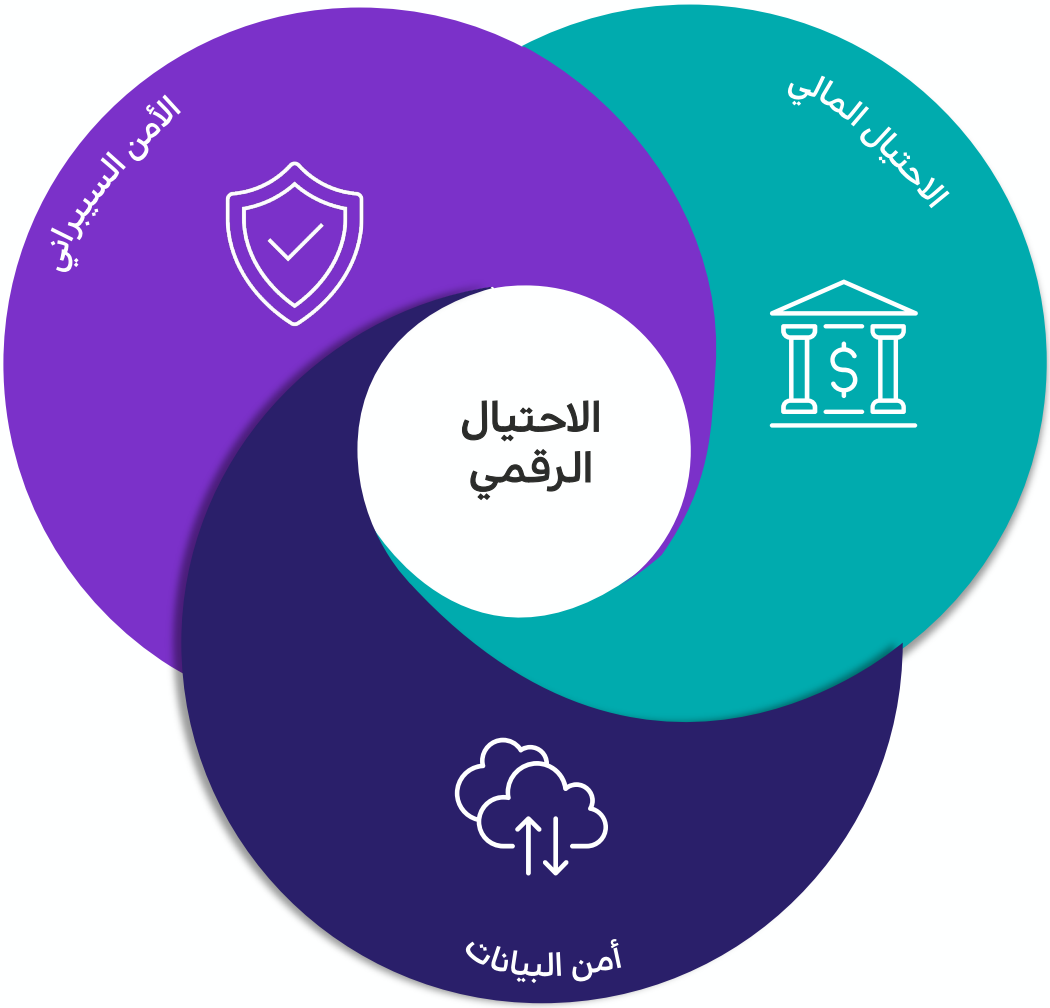
الاختلاف	الوصف
دخول افتراضي/ عن بعد	من طبيعة الاحتيال الرقمي أن يُرتكَب عن بُعد أو افتراضيًا، وهو ما يختلف عن الاحتيال الداخلي الذي يتطلب الوصول الفعلي إلى نظام الجهة.
خداع أو تزوير	يعتمد الاحتيال الرقمي على الخداع أو التزوير لتحقيق نتيجته. وبهذا المعنى فهو يعتمد على عجز الجهة أو المستفيدين منها على التمييز المناسب بين المحتال والعميل.
موجَّه للمستفيد	يستهدف الاحتيال الرقمي الأنظمةَ الموجهةَ نحو العملاء لأن جهات الخطر تعتمد على حملات كبرى لتحقيق نسبة تكلفة أعلى لكل هجوم.
دور الجهة غير المباشر	يمكن للجهات أن تؤدي دورًا غير مباشر وغير طوعي في تسهيل الاحتيال الرقمي من خلال معالجة المعاملات الاحتيالية أو التعامل مع طلبات وصول المستخدم.

الشكل 3 – اختلافات حوادث الأمن السيبراني والاحتيال التقليدي

[8] BCBS -D558 reworded to suit government entity application

5.3. أهمية جهود مكافحة الاحتيال الرقمي

يؤثر الاحتيال الرقمي بصورة ملحوظة على مستخدمي التقنيات في المملكة؛ مما يستدعي تعزيز الجهود لمكافحته. ومع التطور الرقمي المتسارع وفقًا لرؤية السعودية (2030)؛ أصبح من الضروري اتخاذ تدابير فعّالة لحمايته، مع التركيز على الفئات الأكثر عرضة لهذا النوع من الاحتيال.



الشكل 4 -مجالات المخاطر

يأتي الاحتيال الرقمي عند تقاطع مجالات المخاطر الثلاثة الموضحة في الشكل رقم (4)؛ مما يزيد من صعوبة الحد من أضراره. ونظرًا لتداخله مع العديد من تصنيفات المخاطر، يمكن التعامل معه بصفته خطرًا متعدد التصنيفات. وعادةً ما تأتي الضوابط اللازمة لإدارة الاحتيال الرقمي من تنظيم خصوصية البيانات وتنظيم الأمن السيبراني، بينما يجري قياس تأثيره المالي بناءً على معايير قياس محددة. هذا التعقيد يجعل تقييم المخاطر عملية صعبة، خاصةً عند التمييز بين الاحتيال الرقمي وعمليات التضليل الاحتيالي، وعلى الرغم من أن المفهومين مترابطان؛ فإن إجراءات الحد من أضرار كلٍّ منهما تختلف، مما يتطلب تمييزًا دقيقًا بينهما.

5.3.1 الاحتيال الرقمي:

تعريفه: يشير الاحتيال الرقمي إلى أي نوع من الأنشطة الاحتيالية التي تُنفَّذ باستخدام التقنية أو المنصات الرقمية. ويشمل هذا النوع من الاحتيال: التلاعب التقني أو التضليل الاحتيالي؛ للحصول على قيمة مادية أو معلومات حساسة عن طريق الوسائل الرقمية.

- أمثلة عليه: تتضمّن أمثلة الاحتيال الرقمي: هجمات التصيد الاحتيالي، وسرقة بيانات الهوية، وسرقة بيانات بطاقات الائتمان، واختراق الحسابات، والمعاملات الاحتيالية التي تُجرى عبر القنوات الرقمية.
- سِماته: يتسم الاحتيال الرقمي عادةً بالوصول غير المصرح به، والأخطاء البشرية، والتلاعب بالأنظمة الإلكترونية أو البيانات، واستغلال نقاط الضعف في البنية التحتية الرقمية. وغالبًا ما يرتبط الاحتيال الرقمي بوجود أعطال فنية في الضوابط الداخلية.
- كيفية الحدّ من أضراره: يتطلب الحد من أضرار الاحتيال الرقمي تطبيقَ حوكمة قوية وإطار عمل محكم، بجانب تعزيز الضوابط التقنية وبرامج الرصد المتقدمة.
- تأثيراته: تشمل تأثيرات الاحتيال الرقمي: الخسائر المالية، وفقدان البيانات، وتعطل العمليات.

5.3.2 التضليل الاحتيالي:

تعريفه: يشير التضليل الاحتيالي إلى مخططات خادعة أو أنشطة احتيالية؛ تهدف إلى خداع الأفراد أو الجهات للحصول على أموال، أو معلومات حساسة، أو أشياء ثمينة أخرى تحت ذرائع زائفة. ويمكن أن تحدث عمليات التضليل الاحتيالي عبر قنوات اتصال متنوعة؛ ويشمل ذلك المنصات الرقمية، أو عن طريق وسائل تقليدية.

- أمثلة عليه: تشمل أمثلة التضليل الاحتيالي: عمليات الاستثمار الاحتيالية، والأعمال الخيرية المزيفة، والخداع عبر الطرود، والرسائل النصية الاحتيالية.
- سِماته: يعتمد التضليل الاحتيالي غالبًا على تقنيات الهندسة الاجتماعية؛ لاستغلال علم النفس والعواطف البشرية، مثل: الخوف، أو الجشع، أو الشفقة. ويمكن أن تستهدف عمليات التضليل الاحتيالي الأفراد، أو الشركات، إضافةً إلى الجهات الحكومية، وقد تحدث حتى في وجود ضوابط داخلية فعالة.
- كيفية الحد من أضراره يتطلب الحد من أضرار التضليل الاحتيالي؛ زيادة الوعي بين جميع المستخدمين، وتطبيق مشروعات بنية تحتية وطنية، مثل: (مبادرات الاتصالات الفنلندية).
- تأثيراته: تشمل تأثيرات التضليل الاحتيالي: الخسائر المالية للمستفيدين، التأثير بسمعة المملكة العربية السعودية، والألم النفسي للمتضررين.

وعلى الرغم من التسارع الكبير لحوادث الأمن السيبراني بفضل التقنيات الرقمية، إلا أن الاحتيال الرقمي لا يزال مدفوعًا بصورة كبيرة بمثلث الاحتيال كما هو موضح في المقدّمة. ويجب التعامل مع الاحتيال الرقمي باستباقية تُعِين الجهات الحكومية على إدارة المخاطر الرقمية بصورة فعالة ومراقبتها وتقليلها، وذلك عن طريق توفير الإرشادات الضرورية، ورفع الوعي باستمرار؛ لأنه يُشكّل تهديدًا كبيرًا لأمن الجهات الحكومية وسلامتها.

ومن أبرز التهديدات التي يسبّبها الاحتيال الرقمي للجهات الحكومية، ما يأتي:

أولًا، تؤدي عمليات الاحتيال الرقمي إلى انخفاض ثقة العامّة في الجهات الحكومية؛ لإظهارها ضعفًا في حماية البيانات الحساسة، وإدارة الموارد بفاعلية.

يمكن أن يؤدي انعدام الثقة إلى انخفاض مشاركة المواطنين وامتثالهم؛ مما يعوق العمليات الحكومية وتنفيذ السياسات العامة.

ثانيًا، تُعدّ الجهات الحكومية مسؤولة عن كميات ضخمة من البيانات الشخصية للمستفيدين؛ مما يجعلها هدفًا رئيسًا للمنظمات الإجرامية. وتمثّل البيانات التي تحتفظ بها الجهات الحكومية دورًا أساسيًّا في وقوع الاحتيال الرقمي والتضليل الاحتيالي، وقد تؤدي حوادث الاحتيال الرقمي على المنصات الحكومية إلى سرقة بيانات الهوية وانتهاك الخصوصية؛ مما يتسبب في أضرار جسيمة للأفراد والجهات.

وتؤدي الجهات الحكومية دورًا حاسمًا في سلسلة الاحتيال الرقمي، حيث إن انتحال شخصياتها، واستخدام البيانات الشخصية، وإساءة استخدام البنية التحتية الرقمية العامة غالبًا ما يكون أدواتًا للاحتيال الرقمي؛ لذلك يمكن أن تتولى الجهات الحكومية دورًا نشطًا في مواجهة مخاطر الاحتيال الرقمي.

وقد وضعت هيئة الحكومة الرقمية بصفتها الجهة التنظيمية والخط الثاني في نموذج الخطوط (الثلاثة) الموضح في الشكل رقم (7)، "الدليل الاسترشادي لمكافحة الاحتيال الرقمي"؛ الذي يهدف إلى تمكين الجهات الحكومية من إدارة مخاطر الاحتيال الرقمي بفاعلية عبر منصاتها المختلفة، ويقدّم توصيات عملية لمواجهة الاحتيال الرقمي، مع تشجيع الجهات على تطبيقها بما يتناسب مع احتياجاتها وظروفها.

5.4. سمات مكافحة الاحتيال الرقمي

ترتبط المبادئ الأساسية لمكافحة الاحتيال الرقمي ارتباطًا وثيقًا بسمات الاحتيال الرقمي عند وضع نهج أو إطار لمكافحة الاحتيال الرقمي، حيث يُعدّ من الضروري مراعاة المبادئ الآتية:

تبنّي نهج متعدّد التخصصات:

يمكن للجهات الحكومية اعتماد نهج شامل يجمع بين عدّة تخصصات؛ لمكافحة الاحتيال الرقمي بفاعلية، وللتعامل مع المشكلة من الجوانب المختلفة. وبما أن الاحتيال الرقمي ينطوي على أسباب تقنية وتأثيرات مالية وسلبية أخرى، من الممكن أن يشارك مختصون من الجهات المختلفة في تطوير إطار مكافحة الاحتيال الرقمي. ويتضمن ذلك فرق الأمن السيبراني، ومكافحة الاحتيال، والعمليات، والقانون، والموارد البشرية، وفرق تصميم المنتجات الرقمية. وتضمن مشاركة هؤلاء المختصين نهجًا شاملًا للحد من مخاطر الاحتيال الرقمي.

دور إدارة البيانات في مواجهة الاحتيال الرقمي:

تمثّل البيانات دورًا حيويًّا في مكافحة مخاطر الاحتيال الرقمي. ويمكن تشجيع الجهات الحكومية على جمع أكبر قدر ممكن من البيانات وتحليلها؛ لربطها باتجاهات مخاطر الاحتيال الرقمي. ومن الضروري تطبيق نماذج التعلم الآلي والاستفادة من تقنيات النمذجة المتقدّمة للكشف عن حوادث الاحتيال الرقمي والوقاية منها. وتتطلب هذه التقنيات بيانات دقيقة وشاملة؛ لذا يتعين على الجهات الحكومية التفكير الإبداعي في ربط البيانات، مثل: معدلات استخدام المنتجات الرقمية، مع سيناريوهات الاحتيال الرقمي المحتملة.

التركيز على المستفيدين والموظفين:

من الممكن أن تعمل الجهات الحكومية على تدريب موظفيها وتوعية المستفيدين بانتظام بالمخاطر المتعلقة بالاحتيال الرقمي؛ نظرًا لتصاعد تعقيدات هذا النوع من الاحتيال، حيث إن التركيز على التوعية والتدريب للمستفيدين هو أحد المبادئ الأساسية التي يتبناها أي إطار لمكافحة الاحتيال الرقمي.

المرونة والتكيف:

من الضروري أن يكون إطار مكافحة الاحتيال الرقمي قابلًا للتكيف مع التطورات السريعة في مخاطر الاحتيال الرقمي؛ نظرًا لأن هذا المجال يتغير باستمرار، ويُوصى بإجراء مراجعات وتحديثات للسياسات والضوابط دوريًّا، حيث تساعد هذه الآلية في متابعة تطورات الاحتيال الرقمي ومواكبتها بفاعلية.

5.4.1 سمات الاحتيال الرقمي الأساسية

يوضّح الشكل رقم (5) السمات الأساسية للاحتيال الرقمي:

تأثيره على كافة المنصات

نظرًا لأن الاحتيال الرقمي يشكل تمثيلاً عمليًا للمخاطر، فإنه يتقاطع مع عدة فئات من المخاطر، مما يجعل مكافحته أمرًا معقدًا للغاية. وغالبًا ما تؤثر مخاطر الاحتيال الرقمي على عدة مجالات

يتأثر بالبيئة المجتمعية

يتأثر الاحتيال الرقمي بالعوامل الثقافية والاجتماعية، ويرتبط مرتكبو الاحتيال الرقمي أحيانًا بأنماط السلوك والثقة التي تسود في بعض البيئات، والتي قد تساعدهم في بناء الثقة مع المتضررين. يمكن أن يشمل هذا السلوك تقليد عادات محددة أو استغلال أنماط التواصل المعروفة في بعض المجتمعات لزيادة فاعلية الهجوم.

يستهدف الفئات الضعيفة

الاحتيال الرقمي غالبًا ما يستهدف الأفراد أو المجموعات التي تكون أكثر عرضة للإقناع أو التأثر. يشمل ذلك الأشخاص الذين قد يفتقرون إلى المعرفة التقنية أو الذين يعانون من ظروف اجتماعية أو اقتصادية صعبة.

الانتشار السريع

يظهر الاحتيال الرقمي بسرعة ويتطور بشكل متسارع، حيث يستغل مرتكبو الاحتيال الثغرات في الأنظمة أو العمليات لتحقيق مكاسبهم بأقصى سرعة، مما يزيد من تعقيد عملية اكتشافه ومكافحته.

الشكل 5 – السمات الأساسية للاحتيال الرقمي

5.4.2 أبرز التحديات في مكافحة الاحتيال الرقمي

تعتبر مواجهة الاحتيال الرقمي تحديًا كبيرًا؛ لذا يمكن للجهات الحكومية أن تأخذ هذه التحديات بعين الاعتبار عند تنفيذ أطر الحماية لضمان بقاء النظام فعالًا وقادرًا على التكيف مع المتغيرات المستقبلية.

ومن أبرز التحديات في مكافحة الاحتيال الرقمي ما يأتي:

حجم حوادث الاحتيال

إن الحجم الهائل لحوادث الاحتيال الرقمي المكتشفة يمكن أن يَشلّ القدرات التحليلية لفرق مكافحة الاحتيال حيث يعتمد المجرمون على كثرة المحاولات لتحقيق الدخل من جهودهم

رصد الاتجاهات المجتمعية

يمكن لفرق مكافحة الاحتيال الرقمي رصد الاتجاهات المجتمعية الدقيقة التي يمكن أن تمكِّن أو تعزز تأثيرات الاحتيال الرقمي التي غالبًا لا تُرى إلا بعد فوات الأوان.

مخاطر الاحتيال المتقدمة

يستخدم مرتكبو التهديدات الرقمية تقنيات متقدمة مثل الاحتيال تحت قناع الخدمة والتزييف العميق وخدع الهندسة الاجتماعية القائمة على الذكاء الاصطناعي لاستهداف الجهات والمستفيدين بشكل مستمر.

موازنة جهود مكافحة الاحتيال وتجربة المستخدم

تواجه فرق مكافحة الاحتيال الرقمي صعوبةً في إيجاد التوازن المناسب بين ضوابط الحماية الفعالة من الاحتيال ورضا المستخدم، إذ يمكن للقيود المفرطة أن تسبب ضررًا أكبر من الاحتيال نفسه.

5.4.3 مقومات نجاح مكافحة الاحتيال الرقمي

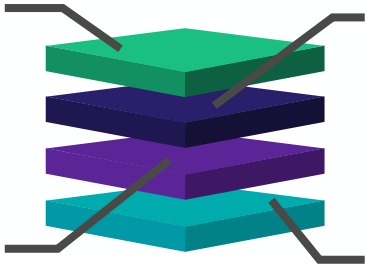
تطوير إطار عمل فعّال لمكافحة الاحتيال الرقمي يمثّل تحديًا كبيرًا، لكنه ليس صعبًا أو مستحيلًا. هناك خطوات رئيسة يمكن اتخاذها مبكرًا لتعزيز فاعلية البرنامج والإطار على المدى الطويل، وضمان تحقيق النجاح في مواجهة هذه التهديدات. يوضّح الشكل رقم (6) مقوّمات نجاح مكافحة الاحتيال الرقمي:

الخطوة 1: مراقبة المخاطر

تتغير تهديدات الاحتيال الرقمي والنصب بسرعة، حيث تتكيف الجهات الفاعلة مع هذه التهديدات. لذلك، من الضروري أن تعتمد الجهات المسؤولة عن إدارة مخاطر الاحتيال الرقمي على المراقبة المستمرة بدلاً من المراقبة الدورية، لضمان متابعة فعالة للتطورات.

الخطوة 2: دليل الرقابة النشطة

نظرًا لأن الاحتيال الرقمي والنصب يشكلان مخاطر متغيرة، يجب تعزيز عمليات التحكم أو تعديلها أو استبدالها بسرعة للتكيف مع التهديدات الجديدة. تضمن الأطر الديناميكية للتحكم التعامل مع التهديدات المتطورة بفاعلية.



الخطوة 3: سرعة الحركة

تسهم الطرق السريعة في تطوير المنتجات في الجهات الحكومية في دفع الابتكارات اللازمة لتقليل مخاطر الاحتيال الرقمي. يجب أن تشارك وظيفة إدارة الاحتيال الرقمي في تطوير المنتجات لضمان سد الثغرات وتعزيز الضوابط ضمن العملية.

الخطوة 4: الذكاء

يمكن أن توفر وظيفة البيانات الاستباقية التي تركز على الاحتيال الرقمي ميزة استراتيجية للجهات الحكومية في مواجهة هذه التهديدات.

الشكل 6 – مقومات نجاح مكافحة الاحتيال الرقمي

06. حوكمة مكافحة الاحتيال الرقمي

6.1. إنشاء الإطار

في هذا القسم، يعرض الدليل الاسترشادي العناصر الأساسية التي يمكن للجهات الحكومية استخدامها لتطوير إطار شامل لإدارة مخاطر الاحتيال الرقمي. ويمكن التعامل مع هذه العناصر بصفتها أجزاءً مستقلة أو تنفيذها تدريجيًّا وفقًا لخطوات محدّدة. وعند إعداد إطار لمكافحة الاحتيال الرقمي، يُنصح بأن تستعين الجهات الحكومية بالأطر الوطنية؛ لفهم أعمق لمخاطرها المُحتملة، ودورها في سلسلة الاحتيال الرقمي.

6.1.1 السياسة

لضمان إدارة فعالة لمخاطر الاحتيال الرقمي؛ يمكن للجهات الحكومية وضع سياسة واضحة لمكافحة الاحتيال الرقمي، التي تُعد وثيقة حوكمة أساسية في هذا المجال. وبحسب السياق التنظيمي للجهة، يمكن أن تكون هذه السياسة مستقلة أو جزءًا من سياسة مكافحة الاحتيال العامة، أو ملحقًا بسياسة إدارة المخاطر. كما يجري تحديد نطاق تنفيذ السياسة داخليًّا على مستوى الجهة ومنسوبيها، أو مع الأطراف الخارجية للجهة. ويمكن أن توفر السياسة إطارًا عامًّا وتصنيفًا يساعد أصحاب المصلحة على إدارة الاحتيال الرقمي بكفاءة دون التأثير على سير العمل.

وعند وضع سياسة لمكافحة الاحتيال الرقمي[9] ، من الممكن للإدارة العليا التأكد من أنّ السياسة:

1. مناسبة لغرض الجهة الحكومية: يمكن للجهة الحكومية تقييم منتجاتها، ومراجعة الحوادث الفعلية المرتبطة بالاحتيال الرقمي؛ لتحديد نطاق السياسة. وبناءً على ذلك يتعيّن تحديد هدف الوثيقة، وضمان تحقيقه بفاعلية.

2. تُحَدِّد صاحب الشأن في الجهة الحكومية: يمكن تحديد موقع مخاطر الاحتيال الرقمي داخل المؤسسة، وتوضيح المسؤولين المعنيّين باتخاذ القرارات المتعلقة بها.

3. تتضمّن التزامًا بتلبية التوصيات المعمول بها: يمكن تحديد الجداول الزمنية والدورات ونقاط التفتيش؛ لضمان الامتثال لنقاط الضوابط ذات الصلة.

4. توفر إطارًا لتحديد أهداف مكافحة الاحتيال: بناءً على الغرض من السياسة؛ من الممكن وضع ضوابط الخط الأول من الخطوط (الثلاثة)، وضمان إنشاء خطط فعالة.

5. تحدِّد مبادئ جمع المعلومات عن حوادث الاحتيال الرقمي: يمكن تحديد تعريف واضح لحوادث الاحتيال الرقمي، ووضع إجراءات لجمع المعلومات؛ ويشمل ذلك تحديد مدى تأثير الحوادث. [10]

6. تتضمّن التزامًا بالتحسين المستمر: تحتوي السياسة على آلية للاستفادة من الدروس المستفادة من تقارير الحوادث وفشل الضوابط، وتضمين النتائج في تطوير إجراءات جديدة.

7.تحدّد العواقب المُترتبة على عدم الالتزام بمتطلبات السياسة: يمكن أن تتضمّن السياسة موقفًا حازمًا تجاه مخاطر الاحتيال الرقمي، مع توضيح واضح للعقوبات التي ستُطبق في حالة عدم الالتزام بالسياسة.

---

[9] ISO37003 Reference for basic policy principles that have been enhanced and adapted
[10] Potentially utilize impact matrix of Risk Management Guidelines

8. أن تتوفر على هيئة معلومات موثقة: يمكن أن يجري توثيق السياسة وتسجيلها رسميًّا، وفقًا لتصنيف الجهة في قسم المخاطر المادية.

9. أن تُعَمَّم داخل الجهة: يمكن أن يجري إدخال المدخلات من (فرق الأمن السيبراني وإدارة المخاطر والتدقيق ومكافحة الاحتيال)؛ لضمان تغطية الجوانب الفنية والإجرائية جميعها.

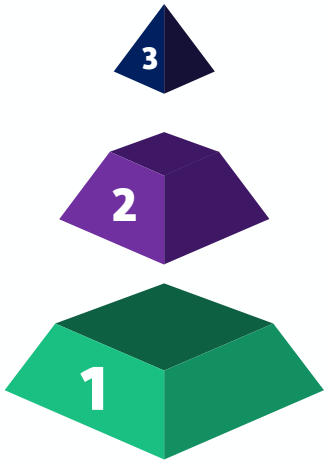
10. أن تُتاح للأطراف المهتمة جميعها بحسب الاقتضاء: يمكن أن تكون السياسة متاحة لجميع الموظفين بحسب الحاجة، مع تسليط الضوء على أهمية إدارة مخاطر الاحتيال الرقمي.

11. أن تُعمَّم بنبرة ولغة مناسبتين للجهة الحكومية: يمكن أن تتّسق السياسة في أسلوبها وصياغتها اللغوية مع السياسات الأخرى المُعتمدة في الجهة الحكومية.

ويمكن للجهات الحكومية، عند أخذ عمليات الاحتيال الرقمية بعين الاعتبار، اختيار تطبيق واحد أو أكثر من هذه الإرشادات، ويظل المبدأ الرئيس: أن تعكس سياسة إدارة مخاطر الاحتيال الرقمي احتياجات الجهة بصورة شاملة.

6.1.2 الأدوار والمسؤوليات

تتطلب إدارة مخاطر الاحتيال الرقمي[11] توفير موارد كافية، وبناء قدرات وإجراءات لتطوير ممارسات مكافحة الاحتيال الرقمي وتحسينها بما يتناسب مع الهيكل التنظيمي للجهة، مع الأخذ بعين الاعتبار المخاطر التي تواجهها الجهة والمستفيدون منها. كما يمكن للجهات الحكومية أن تتبع نهجًا يتماشى مع التهديدات الرقمية، وذلك عن طريق توزيع المسؤوليات في نموذج الخطوط (الثلاثة)، بحيث تتبنى الجهات الحكومية نموذجًا مكونًا من (ثلاثة) خطوط دفاع؛ لتسهيل إدارة المخاطر المرتبطة بالاحتيال الرقمي والإشراف عليها. ويمكن أن يتوافق هذا الهيكل مع متطلبات الجهة الحكومية، وأن يكون ميثاق الأدوار والمسؤوليات مبنيًّا على نموذج الخطوط (الثلاثة)، الموضح في الشكل رقم (7):



- يمكن أن تُشرف وظيفة التدقيق في الخط الثالث على العملية بالكامل، وتجري تحقيقات بعد وقوع الحوادث الكبيرة، ولها الصلاحية الكاملة للتحقيق في أي مسألة في أي وقت.

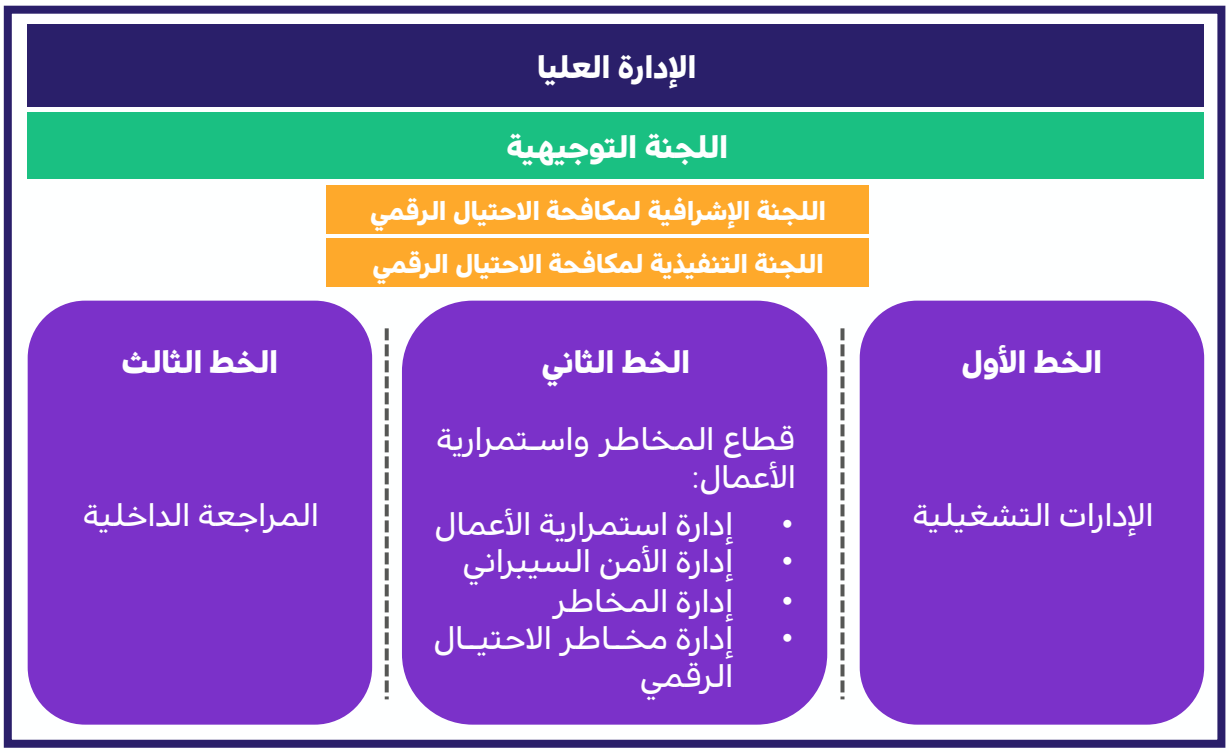
- تُكلَّف فرق إدارة المخاطر في الخط الثاني بمراجعة وتحدي واختبار خطط التحكم في الخط الأول للتأكد من أنها تتماشى مع التنظيمات الصادرة عن الهيئة.
- تُعد فرق إدارة المخاطر في الخط الثاني تقارير إدارية تتعلق بالاحتيال الرقمي.
- تدعم فرق إدارة المخاطر في الخط الثاني الخط الأول عند الحاجة.

- يتولى مسؤولية الخط الأول أصحاب المنتجات ومديرو وحدات الأعمال، الذين يكونون مسؤولين عن إدارة مخاطر الاحتيال الرقمي أو النصب.
- يمكن لأصحاب المنتجات ومديري وحدات الأعمال تنفيذ أطر التحكم في الخط الأول وتدابير الأمن المحددة لمكافحة الاحتيال الرقمي أو النصب.
- يمكن لأصحاب المنتجات ومديري وحدات الأعمال تسجيل حوادث الاحتيال الرقمي أو النصب في مستودع إدارة الحوادث المركزي.

الشكل 7 – نموذج الخطوط الثلاثة

[11] قد يختلف مسمى (إدارة مخاطر الاحتيال الرقمي) من جهة إلى أخرى بحسب طبيعة الجهة وأعمالها والهيكل التنظيمي الخاص بها.

تقع إدارة مخاطر الاحتيال الرقمي ضمن الخط (الثاني) في نموذج الخطوط (الثلاثة) في الجهة، وذلك بالتزامن مع إدارات عديدة، مثل: (إدارة المخاطر المؤسسية، وإدارة استمرارية الأعمال، وإدارة الأمن السيبراني)، وعلى الرغم من فاعلية نموذج الخطوط (الثلاثة)؛ فإن الواقع يشير إلى أن مخاطر الاحتيال الرقمي قد تتجاوز الخطوط الأخرى. لذا يمكن أن تكون الأدوار والمسؤوليات مرنة بما يكفي للتكيف مع مشهد التهديدات المُتغير. ومن الضروري أن تحافظ وظيفة مكافحة الاحتيال الرقمي على علاقات عمل وثيقة مع وظائف إدارة المخاطر الأخرى؛ نظرًا لترابط حوادث مخاطر الاحتيال الرقمي بها، وذلك عن طريق الفحص الدقيق وآلية جمع الحوادث الرقمية، إضافةً إلى هيكلية لجان فعّالة. ويوضّح الشكل التالي موقع إدارة مخاطر الاحتيال الرقمي ضمن الخطوط (الثلاثة):



الشكل 8 – مكافحة الاحتيال الرقمي ضمن الخطوط الثلاثة

كما توضّح الجداول رقم (1,2,3) تفاصيل المهام والمسؤوليات المُحتملة لكل من الخط (الأول، والثاني، والثالث)، مبنيًا على منهجية الاحتيال الرقمي ومراحله ودورة حياته. وتعتبر هذه المهام والمسؤوليات إرشادية، ويمكن لكل جهة حكومية تطوير إطار عمل وظيفي يتناسب مع حوكمة الجهة، ومدى تعرضها للمخاطر.

مراحل الاحتيال الرقمي					
الدور الوظيفي	1-الوقاية	2-الرصد	3-الاستجابة	4-الإبلاغ	5-التحسين المستمر
الخط الأول	1. وضع ضوابط على مستوى المنتج؛ لضمان الحد من مخاطر الاحتيال الرقمي على المستفيدين.	1. هو المسؤول عن اكتشاف الاحتيال على المستفيدين والمنتجات ووحدات الأعمال ذات الصلة.	1. هو المسؤول عن تنسيق جهود الاستجابة لحوادث الاحتيال الرقمي على محيط الخدمة/ الجهة الحكومية.	1. إعداد تقارير منتظمة عن حوادث الاحتيال الرقمي واتجاهاتها وتعرّضها للمخاطر؛ لمراجعتها من لجان إدارة المخاطر والإدارة العليا.	1. وضع ضوابط جديدة أو محسّنة، واستخدامها بناءً على الدروس المستفادة من حوادث الاحتيال السابقة.
	2. تنفيذ ضوابط على مستوى المؤسسة؛ لمنع حوادث الاحتيال الرقمي.	2. تسجيل عمليات الاحتيال الرقمية، وفقًا لإجراءات جمع الحوادث وتسجيلها داخل نظام جمع الحوادث.	2. مكلف بالانتقال من التحقيق إلى الحادث.	2. التأكد من الإبلاغ عن حوادث الاحتيال الرقمي والأنشطة ذات الصلة جميعها.	2. التأكد من فهم الموظفين لأدوارهم في منع الاحتيال الرقمي.
	3. تزويد المستفيدين بالتدريب والتعليم المناسبين؛ لرفع الوعي بالاحتيال الرقمي.	3. تشغيل مجموعة أدوات التقنية الخاصة به ومعايرتها؛ للكشف عن الاحتيال على المستفيدين والأنظمة الداخلية.	3. مكلف بتحديث إجراءات الاستجابة للحوادث، والحفاظ عليها، والامتثال لها.		3. تحديث هذه الضوابط وتحسينها بانتظام؛ لمعالجة التهديدات والثغرات الأمنية المتطوّرة.
	4. إجراء تقييمات المخاطر؛ من أجل إدارة مخاطر الاحتيال الرقمي ومراقبتها.		4. توكّل إليه المسؤولية التنظيمية عن كل حادث، ويمكن أن يكون الذي يتولى مسؤولية الحادث من حيث المبدأ دومًا في الخط الأول.		
			5. مكلّف بتحليل ما بعد الحادث، وأداء أنشطة إدخال البيانات جميعها.		

الجدول 1 – مراحل الاحتيال الرقمي (الخط الأول)

مراحل الاحتيال الرقمي					
الدور الوظيفي	1-الوقاية	2-الرصد	3-الاستجابة	4-الإبلاغ	5-التحسين المستمر
الخط الثاني	1. زيادة المراقبة للكشف عن أي مخاطر متبقية أو تهديدات ناشئة بعد الحادث.	1. تحديد معايير تصنيف الحوادث.	1. إجراء تقييم شامل لحادث الاحتيال؛ لفهم نطاقه وتأثيره.	1. التأكد من توافق متطلبات إعداد التقارير بصورة واضحة مع متطلبات العمل.	1. زيادة المراقبة للكشف عن أي مخاطر متبقية أو تهديدات ناشئة بعد الحادث.
	2. تعزيز ثقافة التحسين المستمر عن طريق دمج الدروس المستفادة من حادث الاحتيال الرقمي.	2. تحديد مستويات التحقّق عند رصد الحوادث الخطيرة المُحتملة.	2. إجراء تحليل للعلة الأساس؛ لتحديد كيفية حدوث الاحتيال.	2. تقديم التقارير بحسب المُقتضى إلى الإدارة العليا، فيما يتعلق بحالة مخاطر الاحتيال الرقمي.	2. تعزيز ثقافة التحسين المستمر عن طريق دمج الدروس المستفادة من حادث الاحتيال الرقمي.
		3. إثراء تدفق المعلومات الاستخبارية الأولية بمزيد من الأفكار.	3. تقديم دعم إضافي لجهات الخط الأول في أثناء حوادث مخاطر الاحتيال الرقمي ذات المستوى أو التأثير العالي.		3. الإشراف على حلقة الاستخبارات، والتأكّد من اتباع الدروس المستفادة على الفور.
		4. الإبلاغ الفوري عن الحوادث الخطِرة.	4. تنسيق الاتصالات مع الإدارة العليا، وجميع وأصحاب المصلحة المعنيّين.		
			5. توفير الإشراف السلبي على إجراءات إدارة الحوادث.		

الجدول 2 – مراحل الاحتيال الرقمي (الخط الثاني)

مراحل الاحتيال الرقمي					
الدور الوظيفي	1-الوقاية	2-الرصد	3-الاستجابة	4-الإبلاغ	5-التحسين المستمر
الخط الثالث	الإشراف على جوانب العملية جميعها باتباع نهج قائم على المخاطر.				

الجدول 3– مراحل الاحتيال الرقمي (الخط الثالث)

6.1.3 اللجان

اللجنة الإشرافية المسؤولة عن مكافحة الاحتيال الرقمي:

لتنفيذ إطار عمل فعّال لمكافحة الاحتيال الرقمي؛ يمكن للجهات الحكومية إنشاء اللجان الإشرافية القائمة لديها أو الاستفادة منها وتكليفها بالمهام الرئيسة؛ لضمان وجود ضوابط لمكافحة الاحتيال الرقمي. وبصورة مبدئية، يمكن أن تكون هذه اللجنة لجنة إدارية عليا تضمّ كبار مسؤولي المعلومات، وكبار مسؤولي أمن المعلومات أو الأمن السيبراني، ومسؤول التدقيق الداخلي، ومسؤول المخاطر (أو مسؤولين على مستوى مكافئ)؛ لمناقشة مخاطر الاحتيال الرقمي، واتخاذ القرارات بشأنها. ويمكن أن تعقد هذه اللجنة اجتماعات تقريبية (مرتين) في السنة[12].

المهام الرئيسة للجنة الإشرافية المسؤولة عن مكافحة الاحتيال الرقمي:

اعتماد السياسات اعتماد السياسات والإجراءات ذات الصلة.	**اعتماد الضوابط والارشادات** إعتماد الضوابط والإرشادات لإدارة إطار فعال لمكافحة الاحتيال الرقمي، وتقييم نتائج تطبيق السياسة (6.1.1).
توفير الرقابة الإشراف على إطار عمل مكافحة الاحتيال الرقمي في الجهة.	**تأكيد الموارد** التأكد من أنّ الفرق التشغيلية تمتلك التمويل والموارد الكافية؛ لتحقيق أهداف الإطار.
تقديم آراء تقديم مشورة بشأن قرارات المخاطر، ويشمل ذلك: قبول المخاطر، أو التخفيف منها، أو نقلها.	

من الممكن أن تتحمل اللجنة الإشرافية المسؤولية الكاملة عن تنفيذ جوانب إطار مكافحة الاحتيال الرقمي جميعها والامتثال لها.

اللجنة التنفيذية لمكافحة الاحتيال الرقمي:

يمكن لكل جهة حكومية تشكيل لجنة فرعية من اللجنة الإشرافية لتكون مسؤولة عن إدارة العمليات المتعلقة بمكافحة الاحتيال الرقمي، بحيث تعقد هذه اللجنة اجتماعات دورية، عادةً (مرة) شهريًّا، وتكون مسؤولة عن الجوانب التشغيلية والفنية لمكافحة الاحتيال الرقمي. ويمكن أن تضمّ اللجنة متخصصين في مجالات (الأمن السيبراني، وإدارة المخاطر، ومكافحة الاحتيال، وتحليل البيانات، والقانون، والامتثال)؛ لضمان نهج شامل ومرن في الحد من مخاطر الاحتيال الرقمي. كما يمكن أن تكون للجنة صلاحيات مفوّضة من اللجنة الإشرافية؛ لمتابعة الجوانب التشغيلية لمخاطر الاحتيال الرقمي وإدارتها.

[12] ISO 37003 Roles Responsibilities and authorities

مسؤوليات اللجنة التنفيذية لمكافحة الاحتيال الرقمي:

الإشراف على التنفيذ

متابعة وتوجيه تنفيذ خطط مكافحة الاحتيال الرقمي.

تطبيق المبادئ

ضمان دمج مبادئ مكافحة الاحتيال الرقمي في تصميم وتدفقات المنتجات وتدفقاتها.

إدارة التقييمات

إجراء تقييمات دورية لمخاطر الاحتيال الرقمي.

مراجعة التقارير

مراجعة تقارير مخاطر الاحتيال الرقمي، ومؤشرات المخاطر الرئيسة، ومؤشرات الأداء الرئيسة؛ لتوجيه إدارة المخاطر.

التدريب والتوعية

قيادة جهود التدريب والتوعية للمستفيدين والموظفين.

إدارة الحوادث

التعامل مع حوادث الاحتيال الرقمي ذات التأثير العالي.

الرفع بالتوصية على السياسات

الرفع إلى اللجنة الاشرافية بالتوصية على سياسات إدارة مخاطر الاحتيال الرقمي.

تنسيق الأنشطة

تنسيق وتنظيم الأنشطة التشغيلية لمكافحة الاحتيال الرقمي، وتنظيمها عبر مختلف الأقسام المختلفة.

تُعتبر هذه المهام إرشادية وليست شاملة لكل الأنشطة المُمكِنة، وعند الاحتياج يمكن لكل جهة حكومية تصميم هيكل اللجنة التنفيذية لمكافحة الاحتيال الرقمي؛ بما يتناسب مع إجراءات الحوكمة وممارسات إدارة المخاطر المتبعة لديها. وفي بعض الحالات، خاصة في الجهات ذات التعرض المنخفض لمخاطر الاحتيال الرقمي، قد تكون هذه اللجان غير ضرورية أو قد تُشكّل عبئًا تشغيليًّا.

6.1.4 العمليات والإجراءات

من وجهة نظر تنظيمية، يمكن أن تشمل سياسة مكافحة الاحتيال الرقمي مجموعة من العمليات والإجراءات المتكاملة التي تدعم الإطار العام، ويمكن دمج هذه العمليات والإجراءات ضمن الأطر الحالية، أو يمكن تطويرها في إجراءات مستقلة ووثائق خاصة بالسياسة، وتعتمد الطريقة المناسبة للتنفيذ على الهيكل التنظيمي للجهات الحكومية.

يوضّح الجدول رقم (4) الطرق المُمكِنة لتحديث الأطر، إضافةً إلى المستندات التي يمكن للجهات الحكومية إنشاؤها أو تحديثها لإدارة مخاطر الاحتيال الرقمي.

الإجراء (غير شامل)	الوصف	وثيقة مستقلة	الدمج في الإطار الحالي
إجراءات تقييم المخاطر	يحدّد تقييم مخاطر الاحتيال الرقمي نقاط الضعف والتهديدات والمخاطر المُحتملة المُتعلّقة بالاحتيال في البيئات الرقمية. ويساعد الجهات الحكومية على فهم تعرضها للمخاطر، وإعطاء الأولوية للتدابير الوقائية، ووضع إستراتيجيات فعّالة للتخفيف من مخاطر الاحتيال.	إذا نُفِّذ إجراء تقييم المخاطر بوصفه مستنداً مستقلاً، فلا بد أن يحتوي على العناوين الآتية على الأقل: 1. تقييم الأثر. 2. تقييم الاحتمالية. 3. مصفوفة المخاطر. 4. رسم خرائط الضوابط. 5. تحليل الثغرات والتوصيات 6. في خطة العمل.	يمكن إضافة موضوع الاحتيال الرقمي إلى تقييمات المخاطر الحالية عن طريق إدراج قسم محدد أو مجموعة أسئلة تركز على مخاطر الاحتيال الرقمي. ويمكن القيام بذلك إذا كان لدى الجهة الحكومية عملية تقييم مخاطر ناضجة، بحيث يمكن إضافة موضوع إضافي.
التحقيق	تحدّد سياسةُ التحقيق في الاحتيال الرقمي الإجراءاتِ اللازمةَ للكشف عن الأنشطة الاحتيالية، والتحقيق فيها، والحد من أضرارها في السياقات الرقمية.	إذا نُفِّذ إجراء التحقيق في الاحتيال الرقمي بوصفه مستنداً مستقلاً، فلا بد أن يحتوي على العناوين الآتية على الأقل: 1. تكوين فريق التحقيق. 2. مصادر بيانات التحقيق. 3. تصنيف التحقيق. 4. تحويل التحقيق إلى حادث. 5. متابعة ما بعد التحقيق.	من حيث المبدأ، تتطلب تحقيقات الاحتيال الرقمي موظفين متخصصين للغاية، لكنها يمكن أن تتبع إجراءات تحقيق داخلية محدّدة سلفًا.

الجدول 4 – الطرق الممكنة لتحديث الأطر (2-1)

الإجراء (غير شامل)	الوصف	وثيقة مستقلة	الدمج في الإطار الحالي
جمع الحوادث	تتضمّن إجراءات جمع الحوادث بروتوكولات لجمع حوادث الاحتيال الرقمي. ويمكن أن تحدّد كيفية جمع الحوادث، وكيفية تحديد تأثيرها وتصنيفها. ويمكن لها أيضاً تحديد حدود الخطورة التي تبيّن إن كان الحادث يمثّل أزمة أم لا.	إذا نُفِّذ إجراء جمع حوادث الاحتيال الرقمي بوصفه مستنداً مستقلاً، فلا بد أن يحتوي على العناوين الآتية على الأقل: 1. مصادر البيانات لجمع حوادث الاحتيال الرقمي. 2. ربط الحادث بإجراءات العمل. 3. تصنيف فرعي لحوادث الاحتيال الرقمي. 4. سبب الحادث. 5. تأثير الحادث. 6. تحليل البيانات.	إذا كانت أنظمة رصد الاحتيال الرقمي ومراقبته محدّدة تحديداً جيداً، وكان هناك تصنيف قائم؛ فيمكن التعامل مع الاحتيال الرقمي (يشمل ذلك الفئات الفرعية ذات الصلة) عن طريق إجراءات جمع الحوادث الحالية، إذا كانت على مستوىً عالٍ من الأتمتة والنضج.
إدارة الحوادث	تتضمّن إجراءات إدارة الحوادث الخاصة بالاحتيال الرقمي التحقق من حوادث الاحتيال الرقمي المحتملة، واحتواء الخطر، والقضاء على مصدره، واستعادة الأنظمة المتأثرة، وإجراء مراجعات ما بعد الحادث؛ لضبط تدابير الوقاية.	إذا نُفِّذت إدارة الحوادث بوصفها مستندًا مستقلاً، فلا بد أن تحتوي على العناوين الآتية على الأقل: 1. تكوين فريق إدارة الحوادث. 2. مصفوفة تصنيف الحوادث. 3. تدفق إدارة الحوادث العادية. 4. تدفق إدارة حوادث الأزمات. 5. العلاج. 6. الدروس المستفادة. 7. تحليل السبب الجذري.	يمكن أن يتبع الاحتيال الرقمي، إذا كان معرَّفًا تعريفًا جيدًا (يشمل ذلك الفئات الفرعية ذات الصلة)، عمليات إدارة الحوادث المُحدّدة سابقاً إذا كانت في حالة عالية من النضج. (على سبيل المثال، وُضِعت أنظمة Archer وServiceNow لإدارة الحوادث).
الإبلاغ	يمكن أن تحدّد إجراءات الإبلاغ مؤشرات المخاطر الرئيسة، وتحدّد البيانات التي تعتمد عليها، وهي وثيقة الصلة بسياسة إدارة الحوادث. ويمكن أن تحدّد حدود الإبلاغ عن المخاطر، وتوضّح التغييرات التنظيمية التي تحدث في حالة انتهاك الحدود.	إذا نُفِّذ الإبلاغ عن مخاطر الاحتيال الرقمي بوصفه مستنداً مستقلاً، فلا بد أن يحتوي على العناوين التالية على الأقل: 1. متطلبات إعداد التقارير. 2. مؤشرات المخاطر الرئيسة. 3. منهجية القياس. 4. فترات إعداد التقارير. 5. ربط إعداد التقارير بمستويات تحمّل المخاطر. 6. بروتوكولات إعداد التقارير المتابعة.	يمكن أن يكون إجراء الإبلاغ عن الاحتيال الرقمي إجراءً مستقلاً أو مجموعة فرعية من إجراءات المخاطر القائمة.

الجدول 4 – الطرق الممكنة لتحديث الأطر (2-2)

6.1.5 الضوابط

يمكن تقسيم ضوابط مكافحة الاحتيال الرقمي، وفقًا لنموذج الخطوط (الثلاثة) الشكل رقم (7) :

الضوابط في الخط (الأول):

الضوابط التقنية: تتضمّن ضوابط تقنية مُصمّمة من أصحاب المنتجات، وتغطي مجالات، مثل: ضوابط الوصول، ومراقبة النشاط، وفصل الواجبات.

أمثلة:

عند تسجيل العميل في خدمة حكومية رقمية جديدة، يتعيّن على الجهات الحكومية التأكد من جمع عدة مؤشرات حيوية.

إجراء مسح يومي لمنصات التواصل الاجتماعي عن طريق خدمات حماية العلامة التجارية الآلية؛ لضمان عدم وجود منصات حكومية وهمية تستهدف المستفيدين.

الضوابط في الخط (الثاني) و(الثالث):

الضوابط الإشرافية: تضمن تنفيذ ممارسات مكافحة الاحتيال الرقمي بصورة مناسبة عن طريق الجهة.

أمثلة:

يمكن أن يكون لدى الجهة الحكومية تصنيف محدّد لمخاطر الاحتيال الرقمي، بما يتماشى مع استراتيجية الجهة.

يمكن أن تكون لدى الجهة الحكومية خطة مُعتمدة للاستجابة لحوادث الاحتيال الرقمي.

عند التنفيذ، من الممكن التأكد من أن الإطار موثق بصورة جيدة، ويُحدَّث بانتظام، ويكون مفهومًا من جميع الموظفين المعنيّين. ويمكن دمج إطار الرقابة الرقمية ضمن إطار الرقابة التنظيمية الشامل. عند تصميم أي نوع من أطر الرقابة، يمكن مراعاة المبادئ الموضّحة في معيار ISO 37003 [13] بشأن ضوابط مكافحة الاحتيال.

وتتطلب هذه المبادئ وضع ما يأتي:

01

ضوابط قائمة على المخاطر

بعد تحديد المخاطر وتقييمها؛ يجري وضع ضوابط للحدّ منها.

02

عملية تحسين مستمر

ضمان مراجعة الضوابط وتحديثها بانتظام.

03

تعميم الضوابط

إتاحتها لجميع الموظفين، بما يتناسب مع مسؤولياتهم ووظائفهم.

04

سهولة الوصول إلى الضوابط

ضمان إمكانية الوصول إلى أحدث إصدار من نظام الرقابة الداخلية بسرعة وكفاءة.

05

برنامج تدقيق داخلي

يتضمّن مراجعة الالتزام بالرقابة الداخلية.

06

قدوة القيادة

أن يكون مجلس الإدارة والإدارة العليا قدوة في الالتزام بالرقابة.

07

تعزيز الثقافة

توعية الموظفين بأهمية اتباع الضوابط، وقد يشمل ذلك ربط الالتزام بالضوابط ببرنامج مراجعة الأداء المنتظم.

إنّ عمليات الرقابة أساسية لمنع مخاطر الاحتيال الرقمي، ويمكن تطويرها واستخدامها وفقًا لمتطلبات الأعمال بناءً على المخاطر المحدّدة. ولا يوجد إطار واحد يناسب الجميع، ويمكن لقادة إدارة المخاطر في الجهات الحكومية تحديدُ أفضل السبل لإدارة مخاطر الاحتيال الرقمي بصورة مناسبة لجهاتهم.

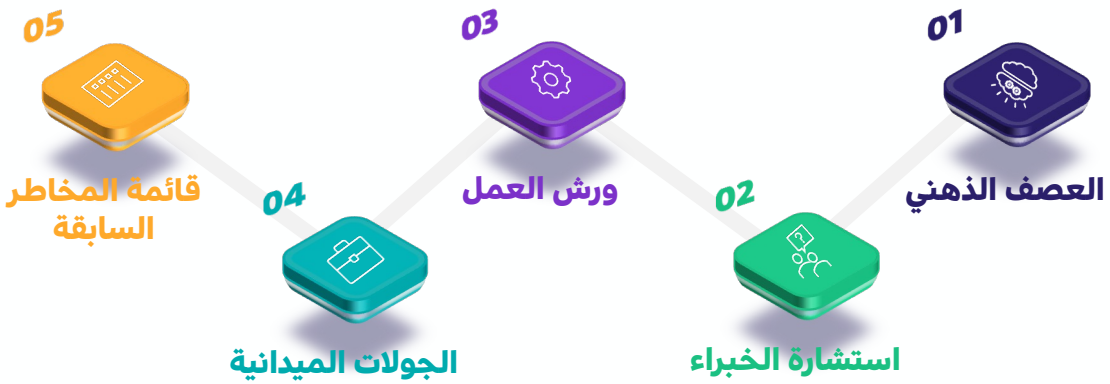
---

[13] ISO 37003 Fraud Management Control Systems – Page 20

6.1.6 تحديد المخاطر المحتملة للاحتيال الرقمي

يقع خطر الاحتيال الرقمي في منطقة بين (المخاطر القانونية، ومخاطر الامتثال، والمخاطر التشغيلية، ومخاطر الأمن السيبراني)؛ مما يجعله صعب التعريف. وعادةً ما تكون أسباب الاحتيال الرقمي مُصنّفة ضمن فئة الأمن السيبراني، بينما التأثير ينتمي إلى فئات المخاطر التشغيلية والقانونية ومخاطر الامتثال. ولتحديد مخاطر الاحتيال الرقمي وتقييمها بصورة دقيقة؛ يُوصى بأن تتبع الجهات الحكومية منهجية تحديد المخاطر التالية، وفقًا للدليل الاسترشادي لإدارة المخاطر واستمرارية الأعمال للحكومة الرقمية.[14]

طرق تحديد المخاطر



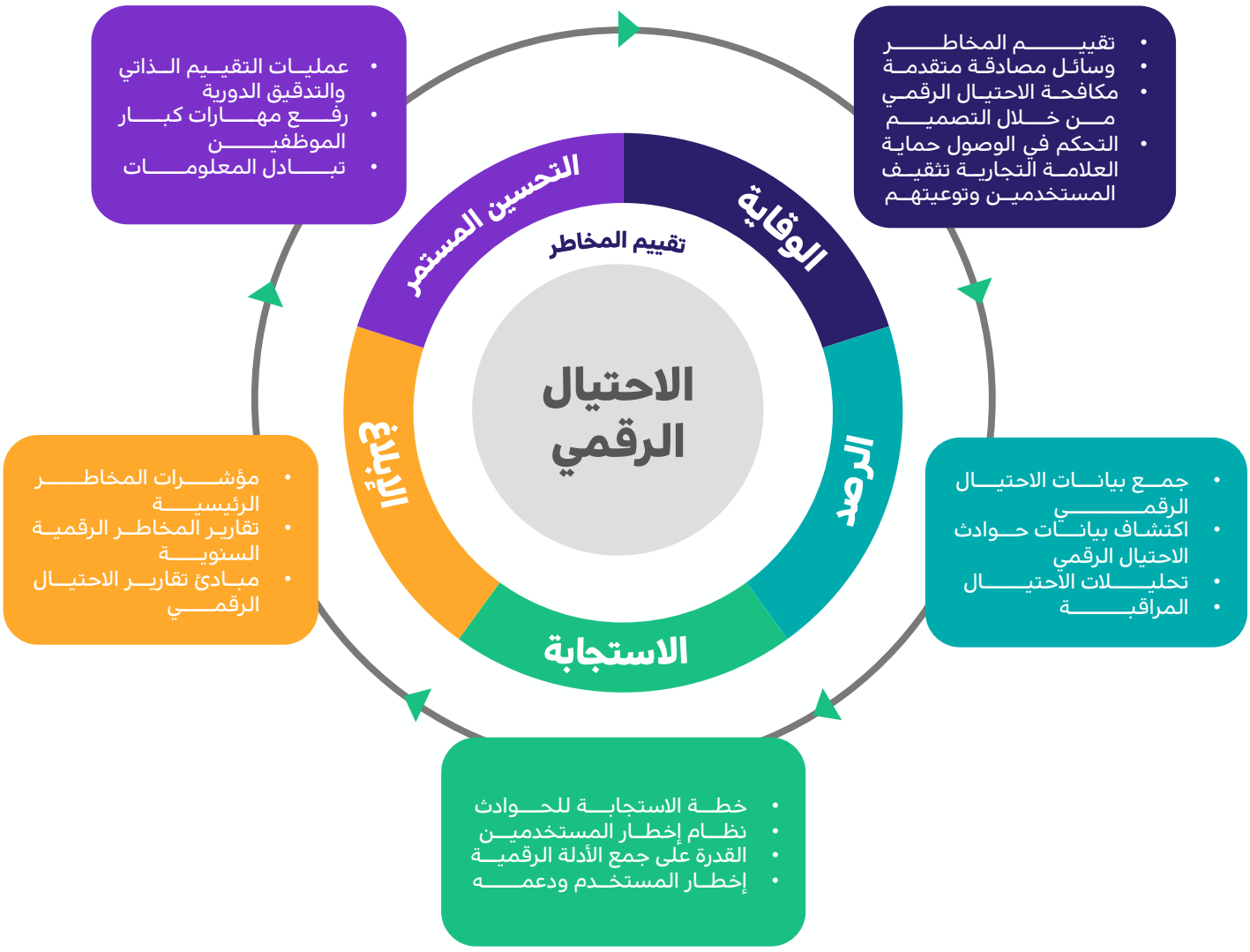
الشكل 9 – طرق تحدد المخاطر

يمكن أن تكون جهود تحديد المخاطر دوريةً، وبما يتماشى مع تصنيف المخاطر الرئيسة المُعتمد من الجهات الحكومية، أو تصنيف مخاطر الاحتيال الذي تفرضه الحكومة. ويمكن لجهود تحديد المخاطر أن تأخذ في الحسبان أيضًا الأهداف التشغيلية للقطاعات والإدارات التابعة للجهات الحكومية. وكما هو موضّح في الشكل رقم (9)، فإن إحدى مراحل تحديد المخاطر الرئيسة هي المخاطر المحدّدة سابقًا؛ لذلك من الممكن أن يكون منطلق جهود إدارة مخاطر الاحتيال الرقمي جميعها من الحوادث والتحقيقات السابقة.

14 الدليل الاسترشادي لإدارة المخاطر واستمرارية الأعمال للحكومة الرقمية الصادر عن هيئة الحكومة الرقمية

07. منهجية مكافحة الاحتيال الرقمي

جرى وضع المنهجية في هذا القسم للجهات الحكومية؛ بهدف الجمع بين جوانب الاحتيال السيبراني وإدارة المخاطر المتعلقة بالاحتيال الرقمي، وتوفير إطار عمل شامل يركز على الاحتيال الرقمي. وتعتمد هذه المنهجية إلى حد بعيد على عناصر من التخصصات الأخرى جميعها، ويمكن ألا تُعتبر بمعزل عن غيرها، بل وثيقة تكميلية لإطار وطني أوسع لإدارة المخاطر. ويوضّح الشكل رقم (10) منهجية مقترحة لمكافحة الاحتيال الرقمي [15]



الشكل 10 – منهجية مكافحة الاحتيال الرقمي

تُعتبر المراحل والتوصيات المذكورة في هذه المنهجية مجرد اقتراحات، ولا تُعدّ إلزامية. ويمكن أن تتبع كل جهة حكومية التوصيات المحدّدة بناءً على تعرضها لمخاطر الاحتيال الرقمي، ومتطلبات الخدمة الشاملة.

وتُشجع الجهات الحكومية على استخدام هذه التوصيات لإدارة مخاطر الاحتيال الرقمي بصورة فعالة، بما يتناسب مع احتياجاتها الخاصة، وما يتماشى مع تعرضها لمخاطر الاحتيال الرقمي ومتطلبات الخدمة الشاملة.

[15] ISO 37003 Fraud Management Control Systems

7.1 التقييم الذاتي الأولي للاحتيال الرقمي

يمكن للجهات الحكومية الاستفادة من نموذج التقييم الذاتي الأولي الموجود في (الملحق (أ))؛ للحصول على رؤية أفضل حول مدى نضجها الحالي والمستقبلي في مجال الاحتيال الرقمي؛ ويهدف النموذج إلى تقديم مؤشر للتعرض المحتمل للمخاطر عن طريق تقييم نضج عناصر إطار مكافحة الاحتيال الرقمي، مما يوفر نقطة انطلاق غنية بالمعلومات بشأن بيانات تقبل المخاطر المحتملة. وبناءً على النتائج المستخلصة، تُنصح الجهات الحكومية بإجراء تقييم شامل لمخاطر الاحتيال الرقمي باستخدام المنهجية الموضّحة في "الدليل الاسترشادي لإدارة المخاطر واستمرارية الأعمال للحكومة الرقمية" الصادر عن هيئة الحكومة الرقمية. كما يمكن الاستعانة بمصفوفة مخاطر انقطاع خدمات وأعمال الحكومة الرقمية لتصنيف الخدمات الرقمية المقدّمة؛ لمعرفة مستوى أهمية الخدمات، بجانب نتيجة التقييم الذاتي الأولي للجهة.

7.1.1 تعريف النطاق والأهداف

يمكن للجهات الحكومية تحديد نطاق بيئتها، استنادًا إلى ممارسات إدارة المخاطر الحالية، وإجراء تحديد أولي لمتطلبات التقييم الذاتي الأولي للاحتيال الرقمي. وعند تحديد النطاق، يمكن للجهة الأخذ بعين الاعتبار ما يأتي:

طبيعة الخدمات المقدمة

هل لدى الجهة خدمات التحقق من هوية العميل أو خدمات تستخدم كمية كبيرة من البيانات الشخصية أو بيانات الدفع؟

الحجم

هل تخدم الجهة العديد من المستفيدين؟

تحقُّق الخطر

هل اكتشفت الجهة حوادث احتيال رقمية أو هل أسهم فشل أنظمتها الخاصة في حدوث الاحتيال الرقمي في جهة أخرى؟

الاحتمالية والتأثير

هل هناك احتمال حدوث حالات احتيال رقمي وما هو التأثير المادي الذي خلَّفته أو ستخلفه هذه الحوادث؟

الشكل 11 – اعتبارات تحديد النطاق

ويهدف التقييم الذاتي الأولي للاحتيال الرقمي إلى تمكين قادة الجهات الحكومية من الحصول على فهم سريع لمخاطر الاحتيال الرقمي المُحتملة، وتقييم مستوى استعداد الجهة لمواجهة هذه المخاطر.

يمكن العثور على نموذج التقييم الذاتي الأولي للاحتيال الرقمي في (الملحق (أ)).

7.2 الوقاية

إنّ الوقاية من الاحتيال الرقمي ليست مجرد تحدٍ تقنيٍ، بل هي ضرورة إستراتيجية تتطلب جهود بيئة العمل في الجهة برمتها، وتتضمّن تنفيذ تدابير أمنية قوية، وتعزيز ثقافة اليقظة والوعي، واستباق التهديدات الناشئة عن طريق المراقبة المستمرة والتحسين.

ولتنفيذ إستراتيجيات فعّالة للوقاية من الاحتيال، تحتاج الجهات الحكومية إلى التأكّد من أنّ نهجها يشمل:

تقييم المخاطر	وسائل مصادقة متقدّمة
مكافحة الاحتيال الرقمي بواسطة التصميم	ضوابط الوصول
حماية الهوية المؤسسية	تثقيف المستخدمين وتوعيتهم

تندرج العناصر المذكورة جميعها في إطار منع الاحتيال الرقمي ضمن مجالات موضوعية متنوعة؛ ممّا يعكس الطبيعة المُعقدة للاحتيال الرقمي وحاجة مكافحة هذا الخطر إلى تضافر جهود الجهة بالكامل. ويسعى هذا الدليل إلى تحديد المجالات التي تتضمن عناصر محدّدة من جهود مكافحة الاحتيال الرقمي، وسيُشير إلى الأطر ذات الصلة التي يمكن أن تساعد في قياس مخاطر الاحتيال الرقمي ومراقبتها، ويُفضّل للجهات الحكومية طلب التوجيه من أطر المجال ذات الصلة، وتطبيق ضوابط الوقاية الفنية وفقًا لمتطلباتها.

كما أنّه من المستحسن أن تُجري فرق إدارة المخاطر في الجهات الحكومية تقييمات للمخاطر بالتعاون مع الأطراف المعنية، مثل: ممثلي المخاطر، وفرق العمليات المسؤولة عن المخاطر، وغيرهم، وتُعدّ تقييمات المخاطر أدوات أساسية للوقاية من مخاطر الاحتيال الرقمي؛ لأنها تساعد في تحديد الأماكن التي تتركّز فيها المخاطر المتبقّية على المستوى المؤسسي، التي قد لا تتوافق مع بيانات تقبّل المخاطر.

7.2.1 تقييم المخاطر

يُفضّل أن تُجري فِرَق إدارة المخاطر في الجهات الحكومية تقييمات المخاطر بالتعاون مع الأطراف ذات الصلة، مثل: ممثلي المخاطر وفِرَق العمليات التي تتولى مسؤولية المخاطر وغيرهم. وتُعدّ تقييماتُ المخاطرِ الأدواتِ الأساسيةَ للوقاية من مخاطر الاحتيال الرقمي؛ لأنها تشير إلى الأماكن التي تتركّز فيها المخاطر المتبقّية على المستوى المؤسسي، التي قد لا تتوافق مع مستويات تقبّل المخاطر.

توصيات بشأن تقييم المخاطر	
1 تقييم المخاطر	يمكن للجهات الحكومية إجراء تقييمات سنوية لمخاطر الاحتيال الرقمي للحفاظ على مستوى عالٍ من الوعي بالمخاطر. يُوصى باستخدام المنهجية الموصوفة في القسم 6.1.2 من إرشادات إدارة المخاطر التابعة لهيئة الحكومة الرقمية لتقييم مخاطر الاحتيال الرقمي.

كما هو مذكور في القسم (6.1.2) بشأن الأدوار والمسؤوليات، يمكن أن تكون تقييمات المخاطر بمثابة الخط الأول ضمن الخطوط (الثلاثة) مع إشراف مناسب من المُتخصصين في إدارة المخاطر في الخط الثاني. كما يمكن أن تكون نتائج تقييم المخاطر موثّقة بالكامل، وتوفر بيئة عمل متكاملة لإدارة مكافحة الاحتيال الرقمي، مع تحديد المخاطر والضوابط اللازمة لتكثيف جهود الوقاية من مخاطر الاحتيال الرقمي.[16]

[16] NCA Essential Cybersecurity Controls Document

7.2.2 تدابير المصادقة المتقدمة

تمثّل وسائل المصادقة المتقدّمة دورًا حيويًّا في مكافحة الاحتيال الرقمي عن طريق تعزيز الأمان، والتحقق من هوية المستخدم أو العملية أو الجهاز؛ مما يجعل ذلك شرطًا أساسيًّا للوصول إلى الموارد في النظام. ويُعتبر هذا الجانب الفني أساسيًّا لجميع المستفيدين الذين يتعاملون مع المنتجات التي تعزّز منع الاحتيال الرقمي بفاعلية. ويمكن للجهات الحكومية استخدام تقنية واحدة أو أكثر من التقنيات في الشكل رقم (12)، بناءً على أهمية خدمات الحكومة الرقمية التي تقدّمها:

يمكن للجهات الحكومية اتباع إجراءات المصادقة المتقدّمة استناداً الى التنظيمات الصادرة عن الجهات ذات العلاقة؛ لضمان الالتزام بمبادئ تصميم مكافحة الاحتيال الرقمي، ويشمل ذلك التنظيمات الصادرة من الهيئة الوطنية للأمن السيبراني، على سبيل المثال:

- الضوابط الأساسية للأمن السيبراني.
- الدليل الارسترشادي لتطبيق الضوابط الأساسية للأمن السيبراني.

كما يمكن للجهات الحكومية الرجوع إلى التنظيمات الصادرة عن هيئة الحكومة الرقمية؛ لتحديد أهمية خدمات الحكومة الرقمية، وتحديد مستويات المصادقة المناسبة بناءً على ذلك.

نوع المصادقة المتقدم	الوصف
التحقق المتعدد	يتطلب استخدام مستويات متعددة من التحقق لتوفير الأمان المطلوب للتصدي للاحتيال الرقمي، حيث يضيف كل مستوى حاجزاً إضافيًا من الحماية. في حال تم اختراق أحد مستويات المصادقة، تكون هناك حواجز أخرى تردع التهديدات الإجرامية.
التحليلات السلوكية	تعتمد على سلوك المستخدم لتحديد الوصول إلى الأنظمة، مثل أنماط التحميل المعتادة، سرعة حركة الفأرة، طريقة الكتابة على لوحة المفاتيح، أو أي بيانات أخرى تسهم في كشف النشاطات الاحتيالية.
المصادقة البيومترية	تقنية تحقق تستخدم الصفات الجسدية الفريدة، مثل بصمة الوجه وبصمة الإصبع وبصمة العين، لضمان دقة التعرف على الهوية.
المصادقة القائمة على الرموز	تستخدم رموزاً مؤقتة، سواء من أجهزة مادية أو برامج رقمية، للتحقق من هوية المستخدم عند دمجها مع تفاصيل تسجيل الدخول الأخرى.
المصادقة القائمة على المخاطر	تعتمد على تحليل وتقييم المخاطر السياقية لكل محاولة تسجيل دخول، حيث يُستخدم تقييم المخاطر الرئيسية لتحديد مستوى الأمان المطلوب، ويمكن إدخال إجراءات إضافية مثل عبارات الإقرار بالمسؤولية ضمن تدفقات المنتجات لتعزيز الحماية.

الشكل 12 – أنواع المصادقة المتقدمة

أصبحت وسائل المُصادقة المتقدّمة أكثر أهمية مع تطور محركات البحث ومنصات الذكاء الاصطناعي. وبما أن عمليات انتحال شخصيات كبار المسؤولين التنفيذيين أصبحت واقعًا ملموسًا؛ فإن التقنيات الحديثة تتطلب وجود بروتوكولات إضافية، مثل: بروتوكول الأسئلة والأجوبة، خاصة مع تزايد الحوادث التي تستهدف كبار أصحاب المصلحة عن طريق تقنيات انتحال الشخصية.[17]

توصيات بشأن تدابير المصادقة المتقدمة	
2 واحد أو أكثر من تدابير المصادقة المتقدمة	من الممكن للجهات الحكومية تقييم وتحديد مستوى حساسية خدماتها الرقمية، وعلى أساس هذا التقييم، يتم تطبيق واحد أو أكثر من تدابير المصادقة المتقدمة واختيار المستوى المناسب للتحقق من هوية المستخدمين وتقنيات التحقق المرتبطة بتلك المستويات، كما هو موضح في ضوابط تصنيف الخدمات الحكومية الرقمية الحساسة ومستويات التحقق الصادرة من الهيئة.

مع تزايد استخدام تقنيات التزييف العميق، وعمليات التضليل الاحتيالي المُعقدّة المُعتمدة على الهوية؛ تبرز الحاجة إلى تبني مبادئ مصادقة متقدّمة؛ لضمان سلامة العمليات الرقمية وقوتها.

ومن مبادئ المصادقة المتقدمة ما يأتي:

المبدأ	الوصف
مرحلة التصميم	يمكن إشراك فرق مكافحة الاحتيال الرقمي في مرحلة تصميم المنتجات وبناء الأنظمة، مع التنسيق الوثيق بين فرق التصميم وفرق الأمن السيبراني في لجان تصميم المنتجات لضمان توفير الحماية الكافية في الأنظمة والتطبيقات.
استخدام سيناريو المخاطر	يمكن للجهات الحكومية التأكد من وجود مجموعة من سيناريوهات مخاطر الاحتيال الرقمي لاختبار وتقييم أنظمتها وتطبيقاتها على مدار دورة حياة المشروع. يمكن أن تكون هذه السيناريوهات عامة أو مصممة خصيصا للجهة الحكومية، ويجب اختبار الخدمات ضد جميع هذه السيناريوهات لضمان فاعلية الأداء.
اختبار الدورة السريعة	يمكن للجهات الحكومية إجراء اختبارات مستمرة على خدمات وتطبيقات الأنظمة الحالية للتأكد من فاعلية تدابير مكافحة الاحتيال الرقمي في مواجهة التهديدات المستجدة. ويجب استخدام حلقة تغذية راجعة سريعة لتكييف تدابير الحماية بمرونة وباستمرار.
إطار الرقابة النشطة	يمكن تصميم أنظمة المنتجات والخدمات بحيث تسمح بتحسين بيئة التحكم استنادًا إلى تقارير الحوادث أو معلومات المخاطر، وينبغي أن تكون هذه التحسينات فورية وقابلة للتطبيق بسرعة لتعديل التدابير بناءً على مستوى المخاطر.

الشكل 13 – مبادئ تصميم مكافحة الاحتيال الرقمي

[17] الاطلاع على الملحق ب دراسات حالة الحوادث – رقم 1 حادثة التزييف العميق (حادثة فيراري)

7.2.3 مكافحة الاحتيال الرقمي بواسطة التصميم

إنّ تبني مبادئ تصميم مكافحة الاحتيال الرقمي يُعدّ أمرًا بالغ الأهمية لبناء أنظمة داخلية قوية ومقاومة للاحتيال في الجهات الحكومية، مع تقديم منتجات آمنة للمستفيدين. ورغم أنّ هذه المبادئ ومنهجيات العمل لا يمكنها القضاء على جميع أشكال الاحتيال الرقمي، إلا أنها تسهم في تحسين المنتجات لتكون أكثر مرونة وأمانًا؛ مما يجعل تجربة المستخدمين أكثر أمانًا.

وقد تتعارض مبادئ مكافحة الاحتيال الرقمي في بعض الأحيان مع تجربة المستفيدين الرقمية، حيث تتطلب إضافة خطوات إضافية للتحقق من شرعية الاستخدام؛ لذا يُفضّل أن تحدّد الجهات الحكومية مستوى أهمية أنظمة التعامل مع المستفيدين قبل تحديد مستوى ضوابط مكافحة الاحتيال الرقمي المطلوب تنفيذها على منتج أو نظام معيّن.

ويمكن أن تُصمّم هذه المبادئ لتتناسب مع حالة استخدام الخدمة أو المنتج، ويُفضّل تطبيقها وفقًا لنهج قائم على المخاطر. ورغم أن هذه المبادئ ليست شاملة أو نهائية، إلا أنها أداة فعالة لتصميم خدمات مرنة وقادرة على مواجهة الاحتيال الرقمي وتشغيلها. ويمكن استخدام الاستبانة الواردة في (الملحق (ج)؛ لتقييم مدى تطبيق مبادئ مكافحة الاحتيال الرقمي في الجهة الحكومية، إضافةً إلى تحديد خريطة طريق لاعتماد هذه المبادئ بصورة منهجية:

توصيات بشأن تصميم مكافحة الاحتيال الرقمي	
3 **التبني المبكر**	يمكن للجهات الحكومية أخذ سيناريوهات الاحتيال الرقمي في الاعتبار خلال مراحل تصميم وتطوير المنتجات الجديدة، سواء كانت منتجات داخلية أو موجهة للمستفيدين.
4 **مرونة الضوابط**	يمكن تصميم المنتجات والخدمات الحكومية بمرونة كافية بحيث يمكن إضافة ضوابط إضافية عند الحاجة من منظور مخاطر النصب أو الاحتيال الرقمي.
5 **التفاعل عن طريق التصميم**	يمكن تصميم المنتجات والخدمات الحكومية لتوفير قنوات تواصل مباشرة مع المستفيدين، مما يمكنهم من تلقي إشعارات عن أي عمليات نصب أو احتيال محتملة، وكذلك الإبلاغ عن الاحتيال الرقمي عند الضرورة.

7.2.4 ضوابط الوصول

تُعدّ ضوابط الوصول عنصرًا حاسمًا في تعزيز قدرة الجهات الحكومية على مواجهة الاحتيال الرقمي؛ إذ تمثّل إدارة وصول المستفيدين والموظفين الداخليين إلى الأنظمة وتطبيقاتها إجراءً أساسيًّا للوقاية من الاحتيال الرقمي.

وغالبًا ما يعتمد المجرمون على الوصول إلى البيانات السرية واستغلالها؛ لتحقيق مكاسب مالية أو غيرها، ويُعدّ ذلك أحد الأسباب الرئيسة وراء العديد من حوادث الاحتيال الرقمي. لذا يمكن للجهات الحكومية ضمان تطبيق مستويات كافية من ضوابط الوصول؛ لمنع وقوع مثل هذه الحوادث.

توصيات للتحكم في الوصول	
6 **تطبيق منهجيات التحكم في الوصول**	يمكن للجهات الحكومية الرجوع إلى التنظيمات ذات الصلة والمتعلقة بإدارة هويات الدخول والصلاحيات والصادرة من الهيئة الوطنية للأمن السيبراني.
7 **إدارة الوصول المميز**	يمكن للجهات الحكومية التأكد من إعادة اعتماد صلاحيات المستخدمين ذوي الامتياز بانتظام، خاصة فيما يتعلق بقواعد البيانات التي تحتوي على بيانات المستفيدين التي قد تُستخدم في ارتكاب الاحتيال الرقمي.
8 **فصل الواجبات**	يمكن للجهات الحكومية التأكد من فصل الأدوار والواجبات بين الوظائف ذات الصلة لمنع التداخل الذي قد يؤدي إلى استغلال غير مشروع للبيانات.

عند تحديد ضوابط الوصول المناسبة التي يمكن تنفيذها، يمكن للجهات الحكومية الرجوع إلى ضوابط تصنيف الخدمات الحكومية الرقمية الحساسة ومستويات التحقق الصادر عن هيئة الحكومة الرقمية. وفي تحديد مستوى تطبيق هذه الضوابط[18].

[18] البند 5.15 ضوابط تحكم الوصول من معيار ISO/IEC 27002:2022

يُعدّ وجود ضوابط الوصول إجراءً وقائيًّا، فهو ضروري لمنع الاحتيال الرقمي؛ إذ يضع بروتوكولات للتحقق من صلاحية وصول المستخدم وتفويضه، مما يقلل من النشاط غير المشروع، ويحد من مخاطر الاحتيال. وتضمن المؤسسات الحكومية -عبر تنفيذ تدابير ضوابط الوصول- أنّ الوصول إلى البيانات الحساسة والأنظمة الحيوية مقصور على الموظفين المُصرّح لهم فقط؛ مما يعزّز الحماية ضد الاختراقات التي قد تؤدي إلى حوادث الاحتيال الرقمي.

ومن منظور منع الاحتيال الرقمي، يمكن التركيز بصورة خاصة على القيود المفروضة على الوصول المميز وفصل الواجبات؛ فالقصور في هذين المجالين قد يسمح باستغلال النظام من الموظفين الداخليين أو الحسابات المخترقة. ويفضّل أن تتبنى الجهات الحكومية مبادئ إدارة حقوق الوصول الشاملة الآتية؛ لضمان الوقاية الفعالة من الاحتيال الرقمي.[19]

أكثرُ ثلاثةِ مبادئ استخدامًا عند تصميم ضوابط الوصول لأنظمة المنتجات والتطبيقات هي:

- **الحاجة إلى المعرفة**: لا يُسمَح للمستفيدين أو المؤسسات أو الأفراد بالوصول إلى المعلومات إلا إذا كانوا في حاجة إليها لأداء مهامهم.
- **الحاجة إلى الاستخدام**: لا تُمنح حقوق الوصول إلى البنية التحتية لتقنية المعلومات إلا عند وجود حاجة واضحة.
- **مبدأ الأقل امتيازًا**: كل شيء يُعتبر ممنوعًا عمومًا ما لم يُسمَح به صراحةً.

علاوة على ذلك، يسهم تطبيق ضوابط الوصول في تعزيز قدرات جمع الأدلة الرقمية ومراقبة الأنشطة، مما يُعَدّ مصدرًا هامًّا لبناء مؤشرات الإنذار المبكر، ورصد أنماط سلوك المستخدمين. وأثبتت الدراسات أن المؤسسات التي تطبق إستراتيجيات فعالة للتحكم في الوصول أقل عرضة لمخاطر الاحتيال الرقمي. لذا، تعَدّ ضوابط الوصول ركيزة أساسية للأمن السيبراني في تقليل أضرار الاحتيال الرقمي، وتعزيز الثقة، وسلامة عمليات المنتجات الرقمية.

[19] البند 5.15 ضوابط تحكم الوصول من معيار ISO/IEC 27002:2022

7.2.5 حماية الهوية المؤسسية

تُعدّ حماية الهوية المؤسسية من الممارسات الأساسية لحماية الموظفين والمستفيدين من عمليات التضليل الاحتيالي. ووفقًا للتعريفات الواردة في القسم (5)، تعتمد عمليات التضليل الاحتيالي على خداع المتضرر وتعاونها، حيث يرتبط هذا التضليل الاحتيالي ارتباطًا وثيقًا بانتحال الهوية المؤسسية. وغالبًا ما يحاول مرتكبو التهديدات الإجرامية انتحال هوية المؤسسات الحكومية المعروفة؛ لبناء جسر من الثقة بين المتضرر والمحتال.[20]

تتمثّل حماية الهوية المؤسسية في تحسين الموارد وتعزيز الضمانات؛ لجعل استغلال هوية معينة مكلفًا وغير جذاب للمحتالين. وبما أن الجهات الفاعلة الإجرامية تسعى لتحقيق الربح؛ فإن ارتفاع تكلفة جهودهم قد يدفعهم إلى تجنب انتحال هويات مؤسسية أو حكومية معينة.

توصيات لحماية الهوية المؤسسية	
9 **دليل حماية الهوية المؤسسية**	يمكن للجهات الحكومية اعتماد عناصر دليل حماية الهوية المؤسسية بما يتناسب مع تعرضها للمخاطر ومتطلبات العمل.
10 **المراقبة الخارجية**	يمكن للجهات الحكومية الاستفادة من إمكانيات المراقبة الخارجية المتعلقة بهويتها المؤسسية.
11 **تقييم مخاطر الهوية المؤسسية**	يمكن للجهات الحكومية إجراء تقييم لمخاطر الهوية المؤسسية على الأقل مرة واحدة سنويًا لتحديد المخاطر المحتملة وحماية سمعتها من الأضرار.

حماية الهوية المؤسسية: هي نظام مراقبة يركّز أساسًا على الجوانب الخارجية، ويعتمد بصورة كبيرة على تقنيات الطرف الثالث، وآليات الرصد؛ لاكتشاف المحتوى الاحتيالي الذي يُستخدم في التضليل الاحتيالي على المستفيدين. وتعود صعوبة حماية الهوية المؤسسية إلى أنها تحدث غالبًا خارج نطاق الجهة الحكومية المباشر؛ مما يتطلب مسحًا نشطًا وشاملًا لتقليل مخاطر إساءة الاستخدام.

ومن منظور التضليل الاحتيالي، تشمل إساءة استخدام الهوية المؤسسية للجهات الحكومية ما يأتي:

- قرصنة حقوق الطبع والنشر: نسخ الصور والشعارات الحكومية دون إذن.
- مواقع التقليد: استخدام مجال آخر للهوية المؤسسية الرسمية للحكومة.
- انتحال شخصية وسائل التواصل الاجتماعي: إنشاء حسابات تتطابق مع الهوية الحكومية أو الفردية.

[20] الاطلاع على الملحق ب دراسات حالة الحوادث – رقم 3 انتحال شخصية الحكومة (الولايات المتحدة)

- سرقة الإعلان: نسخ اسم الهوية المؤسسية، أو نص الإعلان في الحملات الإعلانية.
- تقديم عروض على هويتك المؤسسية: تقديم عروض باستخدام الكلمات الرئيسة التي تحمل هوية حكومية.
- محاكاة أسماء النطاقات: إنشاء ملفات تعريف ضارة على الإنترنت تحاكي نطاقات المنصات الحكومية، مع تحريف طفيف في الأحرف.

لتنفيذ إطار فعال لحماية الهوية المؤسسية والحد من الاحتيال الرقمي؛ يُفضّل أن تعتمد الجهات الحكومية العناصر المُدرجة أدناه.

إدارة النطاق

- السيطرة المستمرة على أسماء النطاقات المرتبطة بالجهة الحكومية لضمان عدم تسجيلها أو استخدامها بطرق غير مصرح بها، والتقيد بما تصدره الجهات الحكومية ذات الصلة بهذا الخصوص.
- منع محاكاة أسماء النطاقات واختطافها من خلال مراقبة مستمرة لتسجيلات النطاقات.
- استخدام بروتوكولات نقل البيانات الآمن عبر الإنترنت مثل HTTPS لحماية المستخدمين الذين يزورون مواقع الجهة الحكومية.

إدارة المحتوى

- تنفيذ عملية الموافقة على المحتوى لضمان الاتساق والدقة في التمثيل الرقمي، والتقيد بما تصدره الجهات الحكومية ذات الصلة بهذا الخصوص.
- مراجعة واعتماد المحتوى الرقمي، بما في ذلك المواقع الإلكترونية والمدونات والبيانات الصحفية، قبل النشر.
- معالجة أي محتوى غير مصرح به قد يُضر بالجهات الحكومية أو بسمعة المملكة العربية السعودية بشكل عام.

مراقبة الهوية المؤسسية

- تطوير سياسات وإرشادات واضحة تحدد كيفية تمثيل هوية الجهات الحكومية عبر الإنترنت.
- تحديد قواعد استخدام الشعار والطباعة وأنظمة الألوان والعناصر المرئية لضمان الاتساق.
- ضمان التناسق في الهوية المؤسسية عبر جميع مواقع الويب ووسائل التواصل الاجتماعي والمنصات الرقمية الأخرى.

العمل على الجهات كافةً

- التعاون مع الجهات الحكومية الأخرى لتبادل أفضل الممارسات ومعالجة التحديات المتعلقة بالهوية المؤسسية.
- مكافحة المنتجات أو الخدمات التي تسيء استغلال اسم الجهة الحكومية.

توحيد مسمى الهوية المؤسسية

- وضع إرشادات واضحة لملفات تعريف وسائل التواصل الاجتماعي وصور الغلاف وصور الملف الشخصي لضمان الاتساق.
- مراقبة حسابات الجهات الحكومية الرسمية بانتظام ومعالجة أي حالات انتحال أو إساءة استخدام بشكل سريع.
- توعية الموظفين بتقنيات بناء العلامات التجارية على وسائل التواصل الاجتماعي لتعزيز الحماية.

الأمن السِّبراني

- الحماية من هجمات التصيد التي تستغل هوية الجهات الحكومية من خلال تدابير وقائية فعالة.
- توعية الموظفين بالمخاطر الأمنية المتعلقة برسائل البريد الإلكتروني والروابط التي قد تؤثر على الهوية المؤسسية.
- التعاون مع الهيئة الوطنية للأمن السيبراني لتأمين مواقع الجهات الحكومية ومنع الاختراقات.

7.2.6 إدارة النطاق

تُعدّ إدارة النطاق جانبًا مهمًّا في الوقاية من الاحتيال الرقمي، حيث يُعتبر استخدام النطاق الخاص بالجهات الحكومية من الأساليب الشائعة التي يستخدمها المحتالون لكسب ثقة المستفيدين؛ بهدف الاحتيال عليهم.

تستغل الجهات الاحتيالية المُمنهجة أنواع الثغرات جميعها المتعلقة بالنطاق؛ لخداع الأفراد والجهات بهدف الحصول على وصول غير مصرح به إلى البيانات الحساسة والبيانات الشخصية. وتُعدّ المواقع الإلكترونية الرسمية TLD's من بين الأهداف الرئيسة للمحتالين الذين يسعون لاستغلال النطاق الرسمي للجهات الحكومية للاحتيال على المستخدمين؛ بهدف الحصول على بياناتهم الشخصية، وتنفيذ هجمات الاحتيال المبنيّة على المصداقية.

بعض من أبرز التهديدات المُتعلقة بدورات حياة إدارة المحتوى، هي:

التقليد الاحتيالي للنطاق: نطاق احتيالي يشبه بصورة كبيرة المواقع الإلكترونية الرسمية للجهات الحكومية؛ مما يمنح المستخدمين الثقة لإدخال معلومات سرية.

احتيال الأخطاء الإملائية: تسجيل نطاق باستخدام أخطاء إملائية أو استخدام لغات أجنبية، (مثل: الأبجدية السيريلية).

اختراق النطاقات الفرعية: يمكن استغلال النطاقات الفرعية المُدارة بصورة سيئة أو المهملة؛ لاستضافة محتوى خادع أو احتيالي، أو لنشر محتوى ضار أو برمجيات ضاره لسرقة البيانات.

استغلال النطاقات المُنتهية الصلاحية: يمكن أن يجري الاستحواذ على النطاقات التي لم تُجدّد من الجهات الاحتيالية، واستخدامها للأنشطة الاحتيالية.

إعادة التوجيه المفتوح: يحدث عندما تسمح تطبيقات الويب عن غير قصد بإدخال مستخدم (محتال) للتحكم في توجيه المستخدم (المتضرر) إلى موقع خارجي. يتيح هذا للمحتال إعادة توجيه المتضررين غير المُدركين من مواقع sa الرسمية إلى صفحات احتيالية.

وتعدّ إدارة النطاقات عنصرًا أساسيًّا في جهود مكافحة الاحتيال الرقمي الوطنية حيث يتعيّن على الجهات الحكومية الالتزام بما يصدر عن الهيئة من تنظيمات بهذا الخصوص بهدف تأمين النطاقات الرسمية، ومراقبة الأنشطة الاحتيالية بصورة استباقية، وتوعية الجمهور بكيفية التعرف على المواقع المشبوهة، أنْ تقلّل بصورة كبيرة من مخاطر الاحتيال الرقمي المُتعلقة بالنطاقات.

كما يعزز تنفيذ الإجراءات الأمنية القوية للنطاقات، وتوعية المستفيدين، الثقةَ في التعاملات الرقمية، ويحمي هذان الإجراءان المستفيدين من الاحتيال الرقمي.

توصيات لإدارة النطاق	
12 تأمين تسجيل النطاقات وتجديدها	يمكن للجهات الحكومية اعتماد عناصر إطار حماية الهوية وفقاً لمدى تعرضها للمخاطر ومتطلبات أعمالها.
13 إدارة النطاقات الداخلية والارتباطات	يمكن للجهات الحكومية ربط جميع النطاقات الداخلية والخارجية والتحكم بها ومراجعتها بشكل دوري للتأكد من التوجيه الصحيح لحركة المرور على الويب Web traffic
14 توعية المستفيدين	يمكن للجهات الحكومية إقامة حملات توعوية بشكل دوري لتوعية المستفيدين وفرق العمل فيما يخص مخاطر الاحتيال الرقمي المتعلقة بالنطاقات.

الجدير بالذكر الجانب المتعلق بالأمن السيبراني في إدارة النطاقات، حيث يمكن للجهات الحكومية الالتزام بما تصدره الجهات ذات الاختصاص.

إضافة إلى ذلك، تُنصح الجهات الحكومية بعدم استخدام الروابط ضمن الرسائل النصية أو البريدية الموجهة للمستفيدين، والاكتفاء بإشعارات التطبيقات والمنصات الرسمية التابعة للجهة، وذلك بهدف رفع مستوى حماية مستفيدي الخدمات الحكومية الرقمية من مخاطر الاحتيال عن طريق الروابط المشبوهة أو المزيفة.

7.2.7 تثقيف المستخدم وتوعيته

تُعتبر جهود تثقيف المستخدمين وتوعيتهم عناصر حيوية في مكافحة الاحتيال والتضليل الاحتيالي الرقميين على المنصات الحكومية. وتوفر هذه المبادرات للموظفين الحكوميين والمستفيدين المعرفة والمهارات اللازمة لاكتشاف التهديدات المحتملة، والإبلاغ عنها، والاستجابة لها بفاعلية؛ نظرًا لأن الاحتيال الرقمي يرتبط بطبيعة الإنسان، فإنّ تعزيز قدرة الأفراد على التعرف على الاحتيال الرقمي يُعدّ أمرًا أساسيًّا. ويوضح الشكل رقم (14) منهجية مقترحة للتدريب على مكافحة الاحتيال الرقمي:

الشكل (14)– التدريب على مكافحة الاحتيال الرقمي

تعمل برامج التدريب الشاملة على تعليم الموظفين أحدث تكتيكات التصيّد الاحتيالي وهجمات الهندسة الاجتماعية، وغيرها من الأنشطة الاحتيالية عن طريق فهم أساليب المحتالين الرقميين، حيث يمكن للموظفين التعرف على الأنشطة المشبوهة واتخاذ الإجراءات المناسبة لمنع الاحتيال الرقمي بفاعلية أكبر. ويضمن التدريب المنتظم أن يظل جميع الموظفون على اطلاع دائم بالتهديدات الجديدة والناشئة، مما يُعزّز النهج الاستباقي بدلًا من النهج التفاعلي في التعامل مع الاحتيال الرقمي. كما أنّ التدريب المستمر ضروري للحفاظ على دفاع قوي ضد المخططات الاحتيالية المتزايدة التعقيد يومًا بعد يوم.

توصيات للتوعية الداخلية	
12 **التدريب السنوي**	يمكن للجهات الحكومية تنظيم دورة واحدة على الأقل سنويًا عبر الإنترنت لمكافحة الاحتيال الرقمي، تعرض خلالها الاتجاهات الرئيسية في هذا المجال.
13 **التدريب القائم على الدور**	يمكن للجهات الحكومية تطوير محتوى تدريبي قائم على الأدوار، يتناسب مع مستوى المسؤولية والدور داخل المؤسسة، لضمان تلقي الأفراد التدريب المناسب لمكافحة الاحتيال الرقمي.
14 **التدريب القائم على المخاطرة**	من الضروري أن تنبه الجهات الحكومية الموظفين بشأن احتمال زيادة حالات الاحتيال الرقمي خلال أوقات الذروة.

تعتبر حملات التوعية العامة من الأدوات الحيوية لمنع الاحتيال الرقمي، إذ تُعزّز هذه الحملات أمان المنصات الحكومية عن طريق توعية المستفيدين بكيفية حماية أنفسهم من عمليات التضليل الاحتيالي الرقمية. يمكن أن تشمل هذه الحملات موارد إعلامية، وورش عمل، ومحتوى وسائط متعددة؛ لتعليم الأفراد كيفية اكتشاف المواقع الاحتيالية، والتعرّف على رسائل البريد الإلكتروني الاحتيالية، والحفاظ على اتصال آمن بالإنترنت.

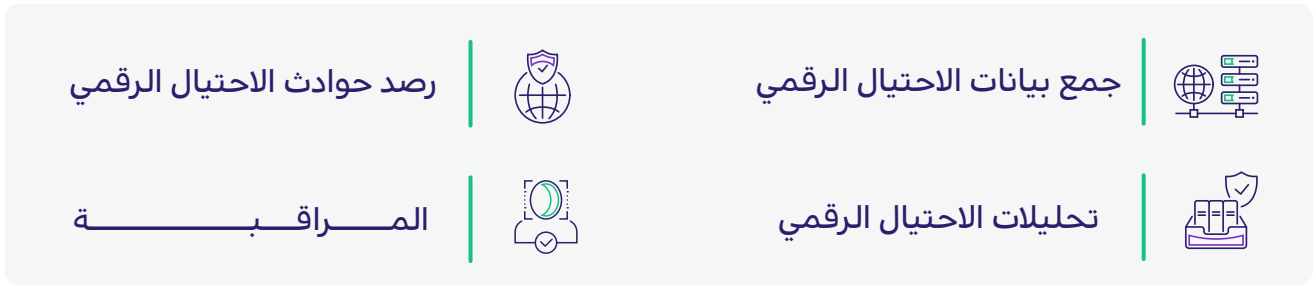
توصيات للتوعية العامة	
15 **منهجية الاستهداف**	يمكن للجهات الحكومية وضع منهجية استهداف لضمان تدريب المستفيدين وفقًا للتقسيمات السكانية المناسبة.
16 **التوعية العامة ربع السنوية**	يمكن للجهات الحكومية إطلاق أربع حملات توعية عامة على الأقل، تتناول موضوعات مكافحة الاحتيال.
17 **ربط حماية الهوية المؤسسية**	يمكن للجهات الحكومية ربط جهود حماية الهوية المؤسسية بحملات التوعية العامة. وفي حال زيادة حالات الاستيلاء على الهوية المؤسسية، ينبغي إطلاق حملات لإعلام المستفيدين بالتطورات الكبرى.

وعن طريق رفع مستوى الوعي، يمكن للجهات الحكومية تقليل قابلية منصاتها والمستفيدين منها للتعرض للاحتيال والتضليل الاحتيالي الرقمي. فالمواطن المُطَّلِع يكون أقل عرضة للوقوع ضحيةً للاحتيال.

7.3 الرصد

يمكن للجهات الحكومية، بغض النظر عن حجمها أو أهميتها، تبني آليات استباقية للكشف عن الاحتيال الرقمي، ويمكن أن تستند هذه الآليات إلى التقييمات الذاتية للمخاطر الأولية وممارسات التحقق من الاحتيال الرقمي عامة.

تشمل جهود الرصد الأساسية:



يُعدّ رصد الاحتيال الرقمي عنصرًا رئيسًا في تطوير نماذج المخاطر التنبؤية، فهو أداة أساسية لإدارة مخاطر الاحتيال، وتمكين تصميم ضوابط أكثر فاعلية، حيث يعتمد رصد الاحتيال الرقمي بصورة كبيرة على البيانات، وتكون فاعليته مرتبطة بنضج أنشطة معالجة بيانات الاحتيال.

بجانب كونه ممارسة تعتمد على البيانات، يهدف رصد الاحتيال إلى تحسين عملية اتخاذ القرار عن طريق توفير معلومات موجزة حول الاحتيال. تبني نهج يركز على جمع البيانات في الوقت المناسب والقابلة للتنفيذ، ويمكن أن يمكّن صناع القرار من تطبيق مبادئ الرصد بفاعلية، وتعزيز أُطر الوقاية.

في المراحل الأولية من عملية الرصد، تعمل الجهات الحكومية على تطوير قدراتها لاكتشاف الحوادث بعد وقوعها. ومع تقدّم التحليلات، تتطور القدرة على اكتشاف الحوادث قبل وقوعها.

تشمل أنشطة الرقابة الكشفية عمليات وإجراءات مصممة خصيصا لتحديد محاولات الاحتيال الرقمي أو العمليات التي تحدث فعليًّا، في الوقت المناسب، والحد من تأثير أي احتيال رقمي يتجاوز الرقابة الوقائية.

7.3.1 جمع بيانات الاحتيال الرقمي

من منظور رصد الاحتيال الرقمي، تعتبر البيانات أساس قدرة الجهات الحكومية على اكتشاف عمليات الاحتيال الرقمية. تشمل هذه العملية جمع بيانات الحوادث والبيانات الوصفية التي قد تشير إلى حوادث وشيكة، مما يُعزّز تطبيق تقنيات القياس المتقدمة والمعالجة في الوقت الفعلي، ويؤدي إلى اكتشاف حوادث الاحتيال الرقمي بشكل أكثر كفاءة. يتضمن جمع البيانات مصادر داخلية وخارجية، ويشمل ذلك المنصات الآلية الداخلية والخارجية، وتقارير المستفيدين أو الموظفين.

تُعدّ البيانات حجر الزاوية في إدارة مخاطر الاحتيال الرقمي، ولا يمكن لإطار إدارة مخاطر الاحتيال الرقمي أن يكون فعّالًا دون جمع مستمر للبيانات من مصادر متعددة. بناءً على أنشطة الجهة الحكومية وحجمها، قد تكون هناك مجموعات بيانات متنوعة تُسهم في تحسين فهم الاحتيال الرقمي عامة.

يمكن أن تشمل المصادر المحتملة للبيانات ما يأتي:

1. الجهة الحكومية وأنظمتها الداخلية
2. المستخدمون والمستفيدون
3. مقدمو خدمات مكافحة الاحتيال المتخصصون من طرف ثالث
4. عامة المستفيدين
5. مؤسسات أخرى
6. الجهات الرقابية

أنواع البيانات التي يمكن جمعها تشمل:

- بيانات المستخدم.
- بيانات النظام والشبكة.
- بيانات الحوادث.
- بيانات الموارد البشرية.
- معلومات حماية الهوية المؤسسية.
- بيانات مركز الشكاوى.
- البيانات الجغرافية المكانية.
- بيانات جهات إنفاذ القانون.
- تنبيهات رصد الاحتيال.
- تقارير المعلومات الخارج.
- بيانات المعاملات: (معاملات الدفع أو الخدمات الحكومية).

يعتمد مدى البيانات التي تُجمع وطريقة استخدامها على حالات استخدام الاحتيال الرقمي التي تواجهها المؤسسة. ويوضح الشكل رقم (15) رحلة جمع بيانات الاحتيال الرقمي: [21]

[21] ISO 37003 Roles Responsibilities and authorities.

الشكل (15) – رحلة جمع بيانات الاحتيال الرقمي

عن طريق جمع البيانات وإجراء تحليلات هادفة لها، يمكن للجهات الحكومية تحسين كفاءتها في جميع مراحل إدارة مخاطر الاحتيال الرقمي، وتسهيل عمليات الإبلاغ عن الاحتيال الرقمي. بناءً على البيانات وقدرات تحليلها، يمكن تطوير معلومات الاحتيال التي تدعم أنشطة التحكم الاستباقية عند الحاجة.

سيُوفّر هذا لكبار صناع القرار رؤية واضحة حول كيفية استجابة المؤسسة، وكيفية تعزيز مواردها، وتحديد أولويات حلول إدارة المخاطر الأكثر صلة. كما يمكن للجهات الحكومية وضع إطار لجمع الحوادث ليكون الأساس لجهود رصد الاحتيال.

إنشاء قاعدة بيانات قوية لحوادث الاحتيال الرقمي يُسهم في تسهيل أنشطة التحكم والمراقبة، فمن الضروري تحديث قاعدة البيانات هذه، وصيانتها بانتظام؛ لضمان توافقها مع الأحداث المستجدة حيث إن الهدف هو بناء أساس قوي يمكن الاعتماد عليه لإنشاء قاعدة بيانات فعّالة تتعلق بالحوادث والتحقيقات عن طريق جمع البيانات ذات الصلة. بعد توحيد مجموعات البيانات، يمكن تطبيق أدوات معلومات الاحتيال والمراقبة في الوقت الفعلي؛ لجعل عملية الرصد ذات طبيعة تنبؤية.

توصيات لجمع بيانات الاحتيال الرقمي	
18 **جمع البيانات المبني على المخاطر**	يجب أن تحدد الجهات الحكومية بناءاً على تقييم المخاطر الرقمية الحد الأدنى للبيانات التي يجب جمعها وإدارة مخاطر الاحتيال الرقمي الخاصة بها.
19 **توحيد العمليات**	ينبغي على الجهات الحكومية أن تسعى إلى توحيد البيانات التي يتم جمعها في تنسيق يمكن استخدامه على المستوى الوطني.

7.3.2 رصد حوادث الاحتيال الرقمي

تُعدّ عملية رصد حوادث الاحتيال الرقمي أمرًا حيويًّا، حيث إنّ العديد من هذه الحوادث لا يجري الإبلاغ عنها أو اكتشافها. وفقًا لمركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي الأمريكي (IC3) ،جرى تقديم (791,790) شكوى بشأن جرائم الإنترنت في عام (2020م)، والتي أسفرت عن خسائر تجاوزت (4.2) مليارات دولار. ومع ذلك، فإنّ الحوادث الرقمية غالبًا ما لا تُبَلَّغ بصورة كافية بسبب عوامل، مثل: شعور المتضرر بالحرج، أو نقص الوعي، أو الاعتقاد بأنّ الإبلاغ غير مجدٍ. تُشير بعض التقديرات إلى أنّ (10%-12%) فقط من للمتضررين الاحتيال الرقمي يبلّغون عن تجاربهم، مما يعني أنّ غالبية الحوادث تظلّ غير مكتشفة أو غير مُبَلَّغ عنها.

لمعالجة هذه المشكلة، يمكن للجهات الحكومية التأكد من أنّ جميع الموظفين والمستفيدين لديهم القدرة على الإبلاغ عن حوادث الاحتيال الرقمي عن طريق القنوات الرسمية. كما يمكن تعزيز الوعي، وتشجيع الإبلاغ الفعّال عن حالات الاحتيال الرقمي.

توصيات للتوعية العامة	
20 **صندوق بريد داخلي**	يجب أن توفر الجهات الحكومية صندوق بريد داخلي متاح للموظفين للإبلاغ عن الاحتيال الرقمي.
21 **الإبلاغ المباشر**	ينبغي على الجهات الحكومية تمكين المستفيدين من الإبلاغ مباشرةً عن عمليات النصب المشبّه بها أو الاحتيال الرقمي إلى الجهة المالكة للخدمة.
22 **الإبلاغ الإلزامي**	يجب إلزام الموظفين بالإبلاغ عن عمليات الاحتيال أو النصب الرقمي المشبّه بها حتى إذا اكتُشفت في المجال العام.
23 **التحفيز**	ينبغي إنشاء برنامج حوافز لتشجيع الإبلاغ عن حوادث الاحتيال الرقمي.

نظرًا إلى أنّ المتضررين قد يميلون إلى عدم الإبلاغ، فمن الضروري أن يكون موظفو الجهات الحكومية والمستفيدون على دراية كاملة بطرق الإبلاغ الواضحة؛ لتسهيل الإبلاغ عن الحوادث بصورة مناسبة، مما يُسهم في قياس مخاطر الاحتيال الرقمي بدقة أكبر.

يُعدّ الموظفون والمستفيدون مصادر أساسية لرصد الاحتيال الرقمي، ولكن العديد من الحوادث تُكتشف أيضًا عبر أدوات مراقبة الأمن السيبراني في الجهات الحكومية، أو عن طريق منصات مكافحة الاحتيال الرقمي المتخصصة.

عندما يُبلَّغ عن حادث، من الممكن أن يجري التحقيق وفقًا للإجراءات والمعايير المعمول بها، مع وجود مؤشرات واضحة لتحديد متى يكون التحقيق قد أثبت وقوع حادثة احتيال رقمي.

توصيات لتحليلات الاحتيال الرقمي	
24 **عملية التحقيق**	يمكن أن تتبع الجهات الحكومية عملية تحقيق محددة في حالات الاحتيال أو الخداع الرقمي، تتماشى مع متطلبات إدارة المخاطر وبروتوكولات التعامل مع الحوادث.
25 **تسجيل الحوادث**	يمكن للجهات الحكومية تسجيل جميع حوادث الاحتيال أو الخداع الرقمية في مستودع مركزي، وتصنيفها على أنها حوادث احتيال أو خداع رقمية.

إضافة إلى الإبلاغ المطلوب من الموظفين والمستفيدين، يمكن للجهات الحكومية وضع واستخدام آليات للكشف عن الاحتيال الرقمي، سواءً داخل المؤسسة أو عبر طرف ثالث. يمكن توجيه هذه الآليات لتغطي البيانات جميعها التي جُمِعت في إطار جهود جمع البيانات، والتركيز على المنتجات الحرجة لتعزيز فاعلية رصد الاحتيال الرقمي.

7.3.3 تحليلات الاحتيال الرقمي

تحليل مكافحة الاحتيال الرقمي يستفيد من علم البيانات والتعلم الآلي (Machine learning) والذكاء الاصطناعي لتحديد الأنماط والانحرافات والتوجهات التي قد تُشير إلى نشاط مشبوه محتمل. عن طريق تحليل كميات كبيرة من البيانات وسلوك المستخدم في الوقت الفعلي أو القريب من الوقت الفعلي، تستطيع هذه الأدوات رصد محاولات الاحتيال قبل أن تتسبب في ضرر كبير. ويمكن استخدام أدوات تحليل البيانات، ويشمل ذلك اختبار تحليل بيانات التصميم، لالتقاط المؤشرات ذات الصلة التي تدل على التعرض للاحتيال الرقمي.[22]

[22] ISO37003 – 8.3.5 Data Analytics

عندما تتوفر البيانات الأساسية وإجراءات جمع البيانات، يمكن للجهات الحكومية تطبيق تحليلات البيانات للكشف عن الاحتيال، مما يوفر مؤشرات تحذيرية مبكرة تُسهم في تعزيز دورة المعلومات الشاملة. بناءً على هذه المؤشرات، يمكن للجهات الحكومية تطوير أنظمة كشف دقيقة تلبي احتياجات عملها وأنشطتها، بهدف الرصد الفعال للاحتيال الرقمي مع الأخذ بعين الاعتبار تطبيقات وأنظمة الذكاء الاصطناعي.

توصيات لتحليلات الاحتيال الرقمي	
26 **تجميع البيانات التحليلية**	يمكن للجهات الحكومية التأكد من أن جهود جمع البيانات تتماشى مع القدرات المتاحة على المستوى الوطني.
27 **اختبارات إثبات المفهوم التقنية**	يمكن للجهات الحكومية التي تواجه مخاطر عالية من الاحتيال الرقمي إجراء اختبارات إثبات المفهوم لتحديد التقنيات ومقدمي الخدمات الخارجيين القادرين على المساعدة في تقليل مخاطر الاحتيال الرقمي.

يمكن أن تشمل تحليلات بيانات الاحتيال المتقدمة (ثلاث) منهجيات بديلة: [23]

1. الوقت الحقيقي: يشمل تحليل البيانات الحيَّة داخل الأنظمة. يُستخدم هذا النهج في أنظمة المعاملات المصرفية والمدفوعات، حيث يعمل نظام تسجيل المخاطر على إيقاف المعاملات والحسابات المشبوهة فورًا، كما تُستخدم تقنيات مماثلة لمكافحة غسيل الأموال.

2. الوقت شبه الحقيقي: يعتمد هذا النهج على تطبيق حلول ترصد النشاط الاحتيالي بصورة شبه فورية، مما يسمح للجهة بالتحقق السريع من التهديدات الأمنية المحتملة.

3. الأثر الرجعي: تُحلّل البيانات المجمعة سابقًا لتحديد اتجاهات الاحتيال، ودفع عملية تقييم المخاطر، وتعديل بيئة الضوابط وفقًا لذلك.

يمكن أن تستند نتائج تحليل البيانات إلى مبادئ معلومات الاحتيال لتقديم تحليلات في الوقت المناسب، قابلة للتنفيذ، وذات صلة بجهود الرصد والمعالجة التنبؤية.

على الجهات الحكومية أن تستفيد من الأدوات والتقنيات الحالية، وتدمج متطلبات تحليل البيانات مع الموارد الوطنية المتاحة. واعتمادًا على الإستراتيجية المختارة، قد يتطلب الأمر التعاون مع مزودي خدمات من طرف ثالث لتحقيق المستوى المطلوب من تحليل البيانات. لذلك، من الضروري تحديد متطلبات التحليل بفاعلية بما يتماشى مع الأهداف المرجوّة من نتائج العمل.

[23] ISO 37001 Benchmark

7.3.4 المراقبة

عند إنشاء إطار مراقبة ناجح في سياق جهود رصد الاحتيال الرقمي، يمكن للجهات الحكومية اتّباع عملية مراقبة تعتمد على الضوابط والحوادث. من منظور إطار المراقبة، يُعتبر استخدام الضوابط الموضحة في إطار عمل المعهد الوطني للمعايير والتقنيةNIST[24] وسيلة فعّالة للمراقبة المستمرة لحوادث الاحتيال الرقمي. ونظرًا لأنّ عمليات الاحتيال والتضليل الاحتيالي الرقمية غالبًا ما تكون مدفوعة بأنشطة المجال الإلكتروني، فإنّ هذه الضوابط تشكّل لبِنات بناء قوية لإنشاء إطار مراقبة متسق. يُفضّل دمج هذه الضوابط في أطر رصد الاحتيال الرقمي الخاصة بالجهات الحكومية.

يمكن أن تخضع الضوابط الأمنية للمراجعة المستمرة مع مقارنة أدائها بحوادث الاحتيال الرقمي التي تجمعت. هذه العملية تُتيح للجهات الحكومية تقييم فاعلية الضوابط، وتحديد ما إذا كانت هناك حاجة إلى إجراء أي تعديلات في إطار الرقابة الشامل

لبنات بناء قوية لإنشاء إطار مراقبة متسق. يُفضّل دمج هذه الضوابط في أُطر رصد الاحتيال الرقمي الخاصة بالجهات الحكومية.

الرصد المستمر:

- الرصد المستمر (1): مراقبة الشبكات وخدمات الشبكة لرصد الأحداث الضارة المحتملة.
- الرصد المستمر (2): مراقبة البيئة المادية لرصد الأحداث الضارة المحتملة.
- الرصد المستمر (3): مراقبة أنشطة الموظفين واستخدام التقنية لرصد الأحداث الضارة المحتملة.
- الرصد المستمر (6): مراقبة أنشطة وخدمات مقدمي الخدمات الخارجيين لرصد الأحداث الضارة المحتملة.
- الرصد المستمر (9): مراقبة بيئات تشغيل الأجهزة والبرامج الحاسوبية وبياناتها لرصد الأحداث الضارة المحتملة.

توصيات لرصد الاحتيال الرقمي

28 التوافق مع أطر الرصد الوطنية	يمكن أن تتماشى جهود الرصد لدى الجهات الحكومية مع الأطر الوطنية أو المعايير الدولية ذات الصلة.

إجراء تقييمات دورية للضوابط استنادًا إلى بيانات الحوادث، يمكن أن يكون مؤشرًا مهمًّا على فاعلية هذه الضوابط. كما أن هذه التقييمات تُسهم في تحديد ثغرات مخاطر الاحتيال الرقمي بصورة أكثر دقة وكفاءة.[25]

[24] NIST – Continuous Monitoring Framework Controls
[25] ISO 37001 Framework On Monitoring and Measurement Activities

7.4 الاستجابة

عند الاستجابة لحادثة احتيال رقمي أو حملة احتيالية، يجب التصرف فورًا واتّباع عمليات راسخة ومدعومة بخطوط اتصال واضحة، مع تحديد الأدوار والمسؤوليات بصورة دقيقة. في مرحلة الاستجابة، تكون الأولوية لتوفير أسلوب منظم للتعامل مع الحوادث، مما يقلّل من التأثير الكلي على الجهات الحكومية والمستفيدين.

ومن منظور الاحتيال الرقمي، تشمل العناصر الأساسية التي يمكن أن تتوفر لدى الجهة الحكومية لضمان استجابة فعّالة:

- خطة الاستجابة للحوادث: تضمن وجود خطوات واضحة للتعامل مع الحادث.
- نظام إخطار المستخدمين: لإبلاغ المستفيدين والمستخدمين المتأثرين بالحادث.
- القدرة على جمع الأدلة الرقمية: لضمان توثيق الحادث بصورة مناسبة.

يمكن أن تتّبع عمليات الاستجابة للاحتيال الرقمي والتعافي منه الخطوط الأساسية لخطط استجابة حوادث المخاطر المعمول بها سابقًا. ويمكن للجهات الحكومية إيلاء اهتمام خاص بالجوانب الفريدة للاحتيال الرقمي، نظرًا للتأثير الكبير للحادث وسرعة انتشاره. كما يمكن الحرص على توثيق أكبر قدر ممكن من البيانات، خصوصًا في حالات الاحتيال الرقمي ذات التأثير الكبير.

7.4.1 خطة الاستجابة للحوادث

عند إعداد خطة الاستجابة لحوادث الاحتيال الرقمي، يمكن تحديد الغرض والنطاق بدقة، مع تحديد المهام التي تغطيها الخطة لعزل الأنشطة المتعلقة بالتعامل مع الحوادث المحددة بدلًا من إدارة المخاطر بصورة أوسع.

توصيات بشأن الاستجابة للحوادث	
29 خطة الاستجابة للحوادث	يمكن للجهات الحكومية دمج الاحتيال الرقمي ضمن خطط الاستجابة للحوادث العامة أو إنشاء خطط مستقلة بناءً على متطلبات العمل.

يمكن أن تتبع خطط الاستجابة لحوادث الاحتيال الرقمي نهجًا تدريجيًّا يشمل الخطوات الآتية:

01 **الإعداد:** التأكيد على أهمية الإعداد المسبق، ويشمل ذلك التدريب المنتظم للموظفين، وإجراء محاكاة للحوادث، وتحديث خطة الاستجابة دوريًّا.

02 **التعريف:** وضع إجراءات واضحة لتحديد وقوع حادثة احتيال رقمي، وتأكيدها، مع وضع خطوات لجمع المعلومات الأولية، وتقييم الوضع بدقة.

03 **الاحتواء:** تقديم إرشادات واضحة لاحتواء الحادث؛ بهدف منع المزيد من الأضرار. ويمكن وضع إستراتيجيات احتواء قصيرة الأمد وطويلة الأمد.

04 **الاستئصال:** تحديد الخطوات اللازمة لإزالة سبب الحادث، مثل: إلغاء وصول المستخدمين المشتبه بهم، وإيقاف الخدمة المتأثرة، أو وقف استخدام البيانات والخدمات المعنية.

05 **الاسترداد:** تقديم تفاصيل حول كيفية استعادة الخدمات المتضررة، مع تطبيق ضوابط إضافية لمنع تكرار حوادث الاحتيال.

عند تطوير خطة الاستجابة للحوادث، من الضروري أن تستفيد الجهات الحكومية بصورة كبيرة من المبادئ الواردة في الأدلة الاسترشادية الخاصة بتحديد خطوط إبلاغ واضحة للأدوار والمسؤوليات، كما هو موضح في القسم (6.1.2) في هذا الدليل الاسترشادي. وضوح الأدوار في الاستجابة للحوادث أمر بالغ الأهمية لضمان إدارة فعالة لإطار عمل الاستجابة، خاصةً الوقت الحساس للاستجابة، والتأثير الكبير المحتمل لحوادث الاحتيال الرقمي على الجهات الحكومية أو المستفيدين.

إضافة إلى وجود خطة واضحة للاستجابة، يمكن للجهات الحكومية التأكد من أنّ منسوبي الجهة المختصين المعنيين بحوادث الاحتيال الرقمي قد تلقّوا التدريب المناسب، ويمكن أن يكون هذا التدريب مرتبطًا بالأدوار والمسؤوليات الموكّلة إلى الموظفين لضمان تغطية جميع الجوانب المناسبة ومستوى التفاصيل المطلوبة.

7.4.2 القدرة على جمع الأدلة الرقمية

يُعدّ التحليل الجنائي خطوة أساسية لفهم أصل وأساليب ونطاق حوادث الاحتيال الرقمي عن طريق فحص الأدلة الرقمية، مثل: السجلات، ورسائل البريد الإلكتروني، وسجلات المعاملات، حيث يمكن لخبراء الاحتيال الرقمي إعادة بناء تسلسل الأحداث التي أدّت إلى الحادث، وتحديد المخاطر المتبقية المحتملة بدقة أكبر. ويمكن أن يكون جمع الأدلة الرقمية جزءًا من إجراءات التحقيق، على أن تتوافق هذه الإجراءات مع إطار إدارة الحوادث الشامل الخاص بالجهة الحكومية.

توصيات بشأن جمع الأدلة الرقمية	
30 **تمكين جمع الأدلة الرقمية**	يمكن أن تمتلك الجهات الحكومية القدرة على تسجيل وجمع الأدلة الرقمية المتعلقة بحوادث الاحتيال أو النصب الرقمي.

يُسهم هذا التحليل في فهم تكتيكات وأساليب المهاجمين، مما يمكّن الجهات الحكومية من معالجة الثغرات الأمنية، والحدّ من احتمالية تكرار الحوادث في المستقبل. كما يمثّل التحليل الجنائي دورًا جوهريًّا في تقييم حجم الضرر الناتج عن الاحتيال، ويشمل ذلك تحديد الأنظمة والبيانات المتأثرة، كما أنّه عنصر أساسي في استجابة الحوادث الشاملة، ووضع إستراتيجية فعّالة للتعافي.

7.4.3 إبلاغ المستخدم ودعمه

يُعدّ إبلاغ المستخدمين ودعمهم أحد أهم العوامل لإنجاح إطار الاستجابة لمكافحة الاحتيال الرقمي، كما يساعد إبلاغ المستفيدين في الوقت المناسب على اتخاذ الإجراءات اللازمة، مثل: تأمين حساباتهم، ومراقبة الأنشطة المشبوهة، وطلب الدعم من الجهات المختصة، مما يُسهم في تقليل الأضرار المحتملة الناجمة عن الاحتيال الرقمي.[26] لذلك، يُعدّ الوصول السريع والآمن إلى المستفيدين أمرًا حاسمًا عند التعامل مع حوادث الاحتيال الرقمي، أو الحد من تأثيرها.[27]

توصيات بشأن إبلاغ المستخدم ودعمه	
31 **دمج الإبلاغات**	يمكن للجهات الحكومية دمج آليات استجابة المستخدم ضمن استراتيجية شاملة لمكافحة الاحتيال الرقمي، مع التركيز على التدابير الاستباقية والتفاعلية.
32 **المعلومات الدقيقة**	من الممكن أن تقدم الجهات الحكومية معلومات مفصلة عبر الإخطارات عن حوادث الاحتيال المحتملة، بما في ذلك طبيعة البيانات المخترقة، والمخاطر المحتملة، والإجراءات الموصى بها للمستفيدين.
33 **الاتصال الثنائي الاتجاه**	يمكن للجهات الحكومية إنشاء قنوات إبلاغ يمكن للمواطنين استخدامها للإبلاغ عن الاحتيال المشتبه به، وتطوير نظام اتصال ثنائي الاتجاه يعزز من مرونة البنية التحتية الرقمية الوطنية.
34 **الوظيفة المُضَمَّنة**	يمكن تضمين عمليات إخطار المستفيد والاستجابة ضمن الرحلة الرقمية لعروض المنتجات الخاصة بالجهات الحكومية.
35 **دعم متضرري الاحتيال**	يمكن أن تكون الجهات الحكومية قادرة على تقديم الدعم اللازم للمستفيدين والموظفين الذين تعرضوا للاحتيال.
36 **تبادل المعلومات**	يمكن للجهات الحكومية تجنب إرسال البيانات السرية أو مراجع المنصات الرقمية عبر الرسائل النصية أو وسائل الاتصال غير المشفرة.

عن طريق دمج عمليات إبلاغ المستخدمين والاستجابة ضمن إطار شامل لمكافحة الاحتيال الرقمي، يمكن للجهات الحكومية تقليل التأثيرات المباشرة للاحتيال، وتعزيز ثقة الجمهور في الخدمات الرقمية.

[26] الاطلاع على الملحق أ – التقييم الذاتي الأولي لمخاطر الاحتيال الرقمي
[27] GDPR mandates that citizens need to be notified of an incident regarding their data without undue delay

7.5 الإبلاغ

من أجل فاعلية الإبلاغ، يمكن للجهات الحكومية التأكد من وجود قنوات إبلاغ معروفة، وأن تكون فرق الخط الأول قادرة على إرسال تقارير الحوادث إلى مستودع مركزي، مثل: (خدمة البلاغ الرقمي). ستوفر بنية البيانات القوية القدرة على إنشاء تقارير إدارية تساعد في اتخاذ قرارات إستراتيجية بشأن تخصيص الموارد لمكافحة الاحتيال الرقمي.

عند تصميم هيكل التقارير، يمكن اتباع المبادئ الأساسية الآتية:

1. تسجيل حوادث الاحتيال الرقمي جميعها بصورة مناسبة في جميع الوحدات التنظيمية.

2. التحقيق في جميع الحوادث المشتبه بها باعتبارها احتياليًا، واستخدام نتائج التحقيق كأساس للتعامل معها.

3. تحديد نقاط الضعف في الرقابة الداخلية.

4. اتخاذ الإجراءات التصحيحية اللازمة لمعالجة نقاط الضعف في الرقابة الداخلية.

جمع هذه البيانات يمكّن الإدارة العليا من إدارة مخاطر الاحتيال الرقمي بصورة أكثر فاعلية. كما يمكن أن تُسهم هذه المبادئ في بناء مجموعة من مؤشرات المخاطر الرئيسة التي يمكن استخدامها بصفتها أدوات تنبؤية لتفادي التعرض للمخاطر. ويمكن مراقبة هذه المؤشرات بانتظام للتأكد من أن الإدارة العليا تتّخذ التدابير الوقائية المناسبة، وتحدّ من الأضرار بصورة فعالة.

7.5.1 مؤشرات المخاطر الرئيسة

مؤشرات المخاطر الرئيسة تُعدّ أدوات مهمة تعمل بعدّها أنظمة إنذار مبكر تنبّه المستخدمين إلى العواقب السلبية المحتملة للمخاطر، وتؤدي هذه المؤشرات دورًا حيويًّا في إدارة المخاطر، إذ تساعد في تقييم فاعلية الضوابط القائمة، وتقدير احتمالية المخاطر، وتتميز مؤشرات المخاطر الرئيسة بقدرتها على القياس والتنبؤ والمقارنة، ويتعيّن الإبلاغ عن أيّ تغييرات فيها بانتظام، وتحليلها، ومراقبتها؛ لضمان استجابة فعالة وملائمة.

أمثلة على مؤشرات المخاطر الرئيسة للاحتيال الرقمي المحتمل:

مؤشرات المخاطر الرئيسة	الوصف
مراقبة الفترات الحرجة لحوادث الاحتيال الرقمي	من الضروري فهم أعداد حوادث الاحتيال الرقمي ومراقبتها في الفترات ذات التفاعل العالي، وذلك لتفعيل الضوابط النشطة بفاعلية.
طلبات الوصول الخاطئة إلى الخدمات الحكومية الرقمية	الزيادة في عدد طلبات الوصول الخاطئة قد تُشير إلى تعرض النظام للاختراق، مما يمكن أن يؤدي إلى حوادث احتيال رقمي.
رصد الاتجاهات العالمية	تتبع اتجاهات الاحتيال الرقمي على المستوى العالمي، فغالبًا ما تكون هذه التهديدات إجرامية خارجية تستهدف الجهات الحكومية والمستفيدين.
عدد حوادث الاحتيال الرقمي	يُعَدُّ العدد الإجمالي لحوادث الاحتيال الرقمي مؤشرًا حيويًّا على المخاطر المحتملة، بناءً على بيانات جمع الحوادث.
عدد حوادث التضليل الاحتيالي	تسجيل عدد حوادث التضليل الاحتيالي في فترة زمنية محددة، مثل: ربع سنة، لتقييم مدى انتشارها.
نسبة حوادث حماية الهوية المؤسسية الناجحة/ الفاشلة	تعكس هذه النسبة فاعلية جهود حماية الهوية المؤسسية للجهة الحكومية.
عدد متضررين الاحتيال	تحديد عدد الأفراد المتأثرين بحوادث الاحتيال.
كمية الأموال المسلوبة بالاحتيال	تقدير المبالغ المالية التي سُلبت من المستفيدين.
عدد حوادث الأمن السيبراني المهمة	مراقبة الحوادث الكبيرة في الأمن السيبراني، مثل: خروقات البيانات، التي قد تؤدي إلى الاحتيال الرقمي.

الجدول (5)– مؤشرات المخاطر الرئيسة

7.6 التحسين المستمر

التحسين المستمر في إدارة مخاطر الاحتيال الرقمي أمر حيوي، إذ يمكّن الجهات الحكومية من استباق التهديدات المتطورة وتكييف إستراتيجياتها وفقًا لذلك. تتغير اتجاهات وأنماط الاحتيال الرقمي بسرعة، ومواكبة هذا التغيير تشكّل تحديًا كبيرًا للجهات جميعها. ولأن تأثير مخاطر الاحتيال الرقمي قد يكون كبيرًا، فإنّ اعتماد نهج ثابت في إدارة المخاطر لا يكفي، ويمكن أن يكون التحسين المستمر نقطة تركيز أساسية تحفز جهود إدارة المخاطر.

7.6.1 عمليات التقييم الذاتي والتدقيق الدورية

يمكن للجهات الحكومية أن تضمن إجراء تقييمات ذاتية وتدقيقات منتظمة لمخاطر الاحتيال الرقمي، لضمان مراقبة فعالة وتكييف تدابير مكافحة الاحتيال الرقمي عبر جميع جوانب المؤسسة. تؤدي المراجعة الداخلية دورًا حاسمًا ضمن إطار إدارة المخاطر الشامل، ويُعدّ دمج مخاطر الاحتيال الرقمي ضمن تقييماتها ضرورة إستراتيجية للجهات الحكومية المعرضة لمستويات عالية من هذه المخاطر.

توصيات بشأن عمليات التقييم الذاتي والتدقيق		
37	**سجل التقييم المنتظم**	يمكن للجهات الحكومية تحديد جدول زمني وتكرار دورات التقييم الذاتي والتدقيق في إطار تقييم مخاطر الاحتيال الرقمي.
38	**دمج الاحتيال الرقمي مع التدقيق**	يمكن للجهات الحكومية الاستفادة من أطر التدقيق الحالية وتوسيع نطاقها لتشمل تقييم تأثيرات الاحتيال الرقمي.
39	**دمج الاحتيال الرقمي مع التخطيط**	يمكن للجهات الحكومية دمج نتائج تقييم الاحتيال الرقمي في التخطيط الاستراتيجي لأنشطة إدارة المخاطر وتطوير خطط عمل مناسبة لمعالجة هذه المخاطر.
40	**ثقافة التقييم والمساءلة**	يمكن للجهات الحكومية تعزيز ثقافة الشفافية والمساءلة من خلال ضمان وضوح نتائج التدقيق لجميع أصحاب المصلحة ومتابعة تنفيذ التوصيات بفاعلية.
41	**حلقة التغذية الراجعة المتكاملة**	يمكن للجهات الحكومية تنفيذ حلقات تغذية راجعة من عمليات التدقيق واستجابات الحوادث وبرامج تدريب الموظفين، بهدف تحسين إطار إدارة مخاطر الاحتيال الرقمي بشكل مستمر.

في العديد من الجهات الحكومية، تُعدّ عمليات التدقيق الداخلي من بين الأكثر تطورًا من منظور إدارة المخاطر، ودمج مخاطر الاحتيال الرقمي ضمن هذا السياق يُعدّ ممارسة فعّالة من حيث تخصيص الموارد. علاوة على ذلك، قد يكون من الضروري زيادة وتيرة التقييمات من منظور التقييم الذاتي نظرًا للطبيعة الدينامية لمخاطر الاحتيال الرقمي. وإذا لم تكن لدى الجهات الحكومية وظيفة تقييم ذاتي ناضجة لمخاطر الاحتيال الرقمي، يمكن استخدام التقييم المقترح في الملحق (أ) بِعدّه نموذجًا أوّليًّا للتقييم الذاتي.

7.6.2 رفع مهارات منسوبي الجهة المختصين بمكافحة الاحتيال الرقمي

يمكن للجهات الحكومية أن تضمن حصول موظفيها على تعليم مستمر يُسهم في تطوير مهاراتهم، حيث يُعدّ التطوير المهني المستمر أمرًا أساسيًّا في مواجهة الاحتيال الرقمي. فهو يعزّز قدرة الموظفين على التعامل مع التحديات المتطورة، ويزيد من وعيهم بالأمور المتعلقة بالاحتيال الرقمي، مما يُعدّ من الأسس الرئيسة للوقاية الفعالة.

توصيات بشأن رفع مهارات كبار الموظفين	
42 **برنامج التعلم المستمر**	يمكن تخصيص جهود التدريب لرفع المهارات بناءً على أدوار ومسؤوليات كبار الموظفين.
43 **التدريب القائم على الأدوار**	يمكن تخصيص جهود التدريب لرفع المهارات بناءً على أدوار ومسؤوليات كبار الموظفين.
44 **الشهادات والاعتمادات**	يمكن تشجيع كبار الموظفين على الحصول على الشهادات والاعتمادات المتخصصة ذات الصلة.
45 **تعزيز النهج المشترك بين الإدارات**	يفضل تسهيل تبادل المعرفة والتعلم التعاوني بين الإدارات المختلفة.
46 **قياس فاعلية التدريب**	يمكن تقييم فاعلية التدريب بشكل منتظم من خلال التقييم والتغذية الراجعة، لضمان تحسين مستمر في المهارات.

بجانب تحسين القدرات الفنية، يُسهم رفع مهارات منسوبي الجهة المختصين في مكافحة الاحتيال الرقمي في بناء قوة عمل متخصصة تلبي احتياجات المؤسسات الحكومية بما يتماشى مع أهداف رؤية السعودية (2030). إضافة إلى ذلك، يعزّز رفع المهارات ثقافة الوعي وإدارة المخاطر الاستباقية داخل المؤسسة.

عندما يتلقى الموظفون تدريبًا منتظمًا على أحدث اتجاهات الاحتيال الرقمي وأفضل الممارسات، يصبحون أكثر يقظة، ويكتسبون معرفة متعمقة. كما أن هذا التدريب يعزّز من قدرتهم على كشف التهديدات، ويجعلهم قادرين على نقل هذه المعرفة داخل دوائرهم الاجتماعية المباشرة. وبذلك، يجري تعميم الوعي، وتوسيع تأثير ثقافة الأمان الرقمي داخل المؤسسة أو الجهة بفاعلية.

7.6.3 تبادل المعلومات

بالنظر إلى حوادث الاحتيال الرقمي التي تنشأ في مجال معين، وتؤثر في مجالات أخرى، فإنّ تبادل المعلومات بين الجهات الحكومية يصبح أمرًا بالغ الأهمية للحصول على صورة كاملة حول بيئة الاحتيال الرقمي، ويُعدّ تبادل المعلومات عنصرًا أساسيًّا في مكافحة الاحتيال الرقمي داخل الجهات الحكومية، حيث يتيح تبادل معلومات التهديد، ومشاركة أفضل الممارسات بفاعلية، وفي الوقت المناسب، بين الجهات المختلفة. يمكن للجهات الحكومية، على الأقل، أن تسعى إلى إنشاء:

توصيات بشأن تبادل المعلومات	
47 **بروتوكولات تبادل المعلومات**	يمكن للجهات الحكومية وضع بروتوكولات واضحة ومحددة لمشاركة بيانات الاحتيال الرقمي، سواء داخل الجهات الحكومية أو بينها.
48 **الشراكة بين القطاعين العام والخاص**	يمكن للجهات الحكومية التعاون مع شركاء القطاع الخاص لتبادل معلومات التهديدات والاستفادة من خبراتهم ومواردهم، مما يعزز الوضع الأمني العام.
49 **مجتمعات تبادل المعلومات**	يمكن للجهات الحكومية التعاون مع شركاء القطاع الخاص لتبادل معلومات التهديدات والاستفادة من خبراتهم ومواردهم، مما يعزز الوضع الأمني العام.
50 **تبادل المعلومات الآمن**	يمكن للجهات الحكومية اعتماد تقنيات قوية للتشفير وقنوات اتصال آمنة لضمان حماية المعلومات المشتركة وسريتها.

اعتماد هذه المتطلبات يمكّن الجهات الحكومية من التعاون مع مجموعة أوسع من الشركاء للتصدي لمشكلة الاحتيال الرقمي بشكل مشترك. كما يعزّز الوعي بالمشكلة ويحسن إجراءات الرصد والاستجابة، ويساعد تبادل المعلومات أيضًا على تخصيص الموارد بصورة أكثر فاعلية. عندما تتبادل الجهات الحكومية الأفكار حول خروقات الأمن ومخاطر الاحتيال الرقمي، فإنها توسع نطاق المعرفة التي تفيد الأطراف المعنية جميعها.

تعزّز هذه المشاركة الفعّالة من جوانب الوقاية والرصد والاستجابة ضمن إطار إدارة مخاطر الاحتيال الرقمي الأوسع. إضافةً إلى ذلك، فإن ترسيخ ثقافة تبادل المعلومات داخل المؤسسات وبين بعضها بعضًا يعزّز الشفافية، ويعزز توليد معلومات قيمة حول الاحتيال عن طريق تبادل المعلومات علنًا بشأن الاحتيال الرقمي والتدابير المتخذة لمكافحته، حيث تظهر المؤسسات التزامها بحماية الموارد العامة واستعدادها لتحمل المسؤولية.

08. الاستنتاج النهائي

مكافحة الاحتيال الرقمي تُعدّ من المهام المعقدة التي قد تؤثر سلبًا على تقديم الخدمات الحكومية الرقمية وتجربة المستخدمين. إذ يمكن أن يكون للاحتياطات الرقمية تأثيرات مالية وتشغيلية ونفسية عميقة، مما يتطلب إدارة فعّالة لمخاطر الاحتيال الرقمي لمراقبتها والحد من أضرارها؛ لتحقيق ذلك، يُفضل أن تضع الجهات الحكومية أُطرًا مستقلة لإدارة مخاطر الاحتيال الرقمي أو تعزيز الأطر الحالية لتتناسب مع إدارة مخاطر الاحتيال الرقمي.

عند اتخاذ القرارات حول النهج المناسب، يمكن للجهات الحكومية:

• بناء نهج قائم على تقييم المخاطر وتقبُّلها: من المهم تجنب تطبيق ضوابط إدارة المخاطر التي قد تتعارض مع أهداف العمل العامة، ويمكن التركيز على العناصر التي تتماشى مع التعرض لمخاطر الاحتيال الرقمي، وتقبُّل المخاطر، والأهداف الإستراتيجية للجهة.

• زيادة وتيرة التقييمات: يتعين على الجهات الحكومية إجراء تقييمات دورية معززة لمخاطر الاحتيال الرقمي مع جمع المعلومات من المصادر الوطنية والمحلية؛ لضمان التعامل الفعال مع اتجاهات الاحتيال المتغيرة بسرعة.

• تعزيز ثقافة الشفافية والتثقيف: من الممكن أن تسعى الجهات الحكومية إلى نشر ثقافة الشفافية حول الاحتيال الرقمي، ومناقشة المخاطر علانية، وتوفير فرص التدريب والتطوير المستمر للموظفين لمواكبة أحدث الاتجاهات.

• دعم الضوابط النشطة: يمكن تطوير الخدمات والتطبيقات، مع مراعاة سيناريوهات الاحتيال الرقمي، وضمان القدرة على إدخال عناصر تحكم جديدة، أو إيقاف الخدمات عند الضرورة.

• التعاون مع الجهات الأخرى: من الضروري التعاون مع الجهات الأخرى، واستخدام القدرات والأطر الوطنية لتعزيز فعالية مكافحة الاحتيال، والحصول على فهم أعمق لتأثيراته الإجمالية.

في الختام، لا يوجد حل موحد يناسب الحالات جميعها في إدارة مخاطر الاحتيال الرقمي. تُمكّن التوصيات والمنهجيات الواردة في هذا الدليل الاسترشادي الجهات الحكومية من إدارة مخاطر الاحتيال الرقمي بفاعلية. ويمكن للجهات الاستفادة من هذه المبادئ لتطوير أُطر ملائمة تتناسب مع متطلبات أعمالها ومخاطر الاحتيال الرقمي التي تواجهها.

09. جدول المصطلحات

يُقصد بالألفاظ والعبارات الآتية -أينما وردت في هذه الوثيقة- المعاني المبينة أمام كلٍّ منها، ما لم يقتض السياق خلاف ذلك:

المصطلح	تعريفه
الهيئة	هيئة الحكومة الرقمية.
الحكومة الرقمية	دعم العمليات الإدارية والتنظيمية والتشغيلية داخل القطاعات الحكومية -وفيما بينها- لتحقيق التحول الرقمي، وتطوير وتحسين وتمكين الوصول بسهولة وفاعلية للمعلومات والخدمات الحكومية.
الجهات الحكومية	الوزارات والهيئات والمؤسسات العامة والمجالس والمراكز الوطنية، وما في حكمها.
الضابط الرقابي (الضوابط)	سياسة أو إجراء أو ممارسة أو عملية أو تقنية أو غير ذلك من التدابير التي من شأنها تخفيف احتمالية أو/ وأثر المخاطر.
التحول الرقمي	تحويل نماذج الأعمال وتطويرها إستراتيجيًّا، لتكون نماذج رقمية مستندة على بيانات وتقنيات وحلول الأعمال.
المخاطر	حوادث محتملة الحدوث قد تؤثر على أهداف الجهة.
تقييم المخاطر	نهج كمي أو نوعي لتحديد الأحداث الخطرة المحتملة، وتحليلها، وتقدير احتمالية حدوثها وآثارها، مع مراعاة عوامل التعرض لها، ومواطن الضعف، وقابلية التضرر منها.
التحسين المستمر	نشاط متكرر لتعزيز أداء عمليات إدارة مخاطر الاحتيال الرقمي.
الإدارة العليا	جميع المسؤولون عن اتخاذ القرارات الأساسية داخل الجهة.
التدريب	بناء المهارات والكفاءات للرفع من أداء المعنيين فيما يتعلق بأدوار أو مسؤوليات محددة.
أصحاب المصلحة	الأطراف والجهات التي تؤثر وتتأثر بقرارات وتوجهات وإجراءات وأهداف وسياسات ومبادرات الحكومة الرقمية، وتشاركها بعضًا من اهتماماتها ومخرجاتها، وتتأثر بأي تغير يحدث بها.
التقييم الذاتي	خطة مفصلة لتوجيه وتوضيح التقدم في تحقيق المبادرات والأهداف.
التوعية	تطوير فهم المخاطر والتهديدات الرئيسة التي من الممكن أن تؤثر سلبًا على تحقيق أهداف الجهة.
الإجراءات	خطوات محددة ومقننة ومفصلة، تنفَّذ عن طريقها الأعمال أو العمليات أو الأنشطة ذات الصلة بالمخاطر واستمرارية الأعمال، استناداً إلى السياسات والمعايير ذات العلاقة.
العمليات	أنشطة مترابطة ومتداخلة ومتفاعلة فيما بينها لتحقيق نتائج محددة في مجال إدارة المخاطر واستمرارية الأعمال، وتكون بناء على السياسات والإجراءات المتعمدة.
ورشة العمل	تمرين قائم على المناقشة، يوجه المشاركين، أو يقدم نظرة عامة على الخطط، والسياسات، والتشريعات، والموارد، والإمكانيات، والقدرات.

المصطلح	تعريفه
التدريبات	تمرين عملياتي يجري توظيفه لاختبار أو ممارسة إجراء أو دور أو آلية عمل محددة، ضمن فريق عمل معني ومحدد.
استمرارية الأعمال	الموارد والإمكانات والقدرات والإجراءات والأعمال اللازمة للاستمرار في تقديم الخدمات الأساسية والمنتجات الضرورية بمستويات محددة مسبقًا، وبإطار زمني مقبول، في حال التعرض للتعطل أو حدوث انقطاع.
المؤشرات الحيوية	الخصائص الجسدية الفريدة للأفراد، مثل: بصمات الأصابع.
لجنة المنظمات الراعية	هي منظمة تقدم الأطر والتوجيهات بشأن إدارة المخاطر في الشركات والرقابة الداخلية، وردع الاحتيال.
الاحتيال الرقمي	استخدام وسائل رقمية لتنفيذ خداع مقصود؛ بغرض تحقيق مكاسب غير مشروعة، سواء أكانت مالية، أو سرقة بيانات، أو تحقيق أهداف ضارة أخرى.
الاحتيال	خداع شخص بصورة متعمّدة للحصول على مكاسب غير مشروعة، أو حرمان المتضرر من حق قانوني.
سرقة الهوية	جريمة يجري فيها الحصول على معلومات شخصية لشخص آخر، مثل: أرقام الهوية، أو بيانات بطاقات الائتمان، واستخدامها لأغراض احتيالية.
المنظمة الدولية للمعايير (ISO)	منظمة دولية مستقلة غير حكومية تعمل على تطوير المعايير ونشرها لمجموعة واسعة من القطاعات والممارسات.
التضليل الاحتيالي	مخطط أو خدعة غير شريفة، تهدف إلى خداع شخص ما، وسرقة شيء ثمين منه؛ كالمال، أو المعلومات الشخصية غالبًا.
الهندسة الاجتماعية	التلاعب النفسي بالأشخاص لحملهم على القيام بأفعال، أو الكشف عن معلومات سرية، ويستخدم غالبًا في أنواع مختلفة من الاحتيال الإلكتروني وغير الإلكتروني.

المصطلح	تعريفه
جمعية مُحقّقي الاحتيال المعتمدين (ACFE)	أكبر منظمة عالمية لمكافحة الاحتيال، تركز على رصد الاحتيال، والتحقيق فيه، ومنعه عن طريق التدريب والشهادات والأبحاث.
لجنة بازل للرقابة المصرفية (BCBS)	لجنة دولية جرى تشكيلها لتطوير معايير عالمية للأنظمة والرقابة المصرفية، وتهدف إلى تعزيز جودة الرقابة المصرفية على مستوى العالم.
مثلث الاحتيال	إطار يُستخدم لشرح العوامل التي تؤدي إلى الاحتيال، ويتكون من (ثلاثة) عناصر: الفرصة، والدافع، والتبرير، والتي يُعتقد أنها تُسهم في السلوك الاحتيالي.
المعهد الوطني للمعايير والتقنية (NIST)	وكالة حكومية أمريكية تطوّر معايير القياس والتقنية وتعزّزها؛ لتحسين الابتكار والأمن الاقتصادي وجودة الحياة.
مخاطر الاحتيال الرقمي	الإمكانية لممارسات الاحتيال التي تجري عن طريق الوسائل الرقمية، مثل: المنصات التقنية، والمعاملات التقنية، أو قنوات الاتصال الرقمية. ويشمل التهديد الذي قد يواجهه الأفراد أو الجهات من حيث الخسائر المالية، وأضرار تتعلّق بالسمعة، أو عواقب قانونية، بسبب الممارسات الخادعة المتعلقة بالأنظمة الرقمية.
مستوى نضج الاحتيال الرقمي (ناشئ)	تُعتمد ممارسات غير منتظمة لإدارة عمليات مكافحة الاحتيال الرقمي، حيث لا توجد عمليات واضحة، وتعتمد على جهود الأفراد دون إطار عمل ثابت.
مستوى نضج الاحتيال الرقمي (متطور)	تُنفذ بعض العمليات الأساسية ولكنها غير موثقة بشكل جيد. تعتمد المنظمات على الخبرات الفردية، مما يؤدي إلى تفاوت في التطبيق.
مستوى نضج الاحتيال الرقمي (متمكن)	تُنفّذ عمليات مكافحة الاحتيال الرقمي بانتظام، حيث توجد ممارسات ممنهجة لتحديد وتقييم وإدارة مخاطر الاحتيال الرقمي.
مستوى نضج الاحتيال الرقمي (متقدم)	تُدار العمليات وتُراقب بمنهجية، حيث تستخدم الجهة البيانات لتقييم الأداء واتخاذ القرارات.
مستوى نضج الاحتيال الرقمي (متميز)	يوجد تركيز على التحسين المستمر من القيادة، حيث تُعزز ثقافة مكافحة الاحتيال الرقمي عبر مستويات الجهة جميعها، وتُعتبر جزءًا من الإستراتيجية العامة.
توحيد البيانات	عملية دمج البيانات من مصادر متعددة، وتنظيفها والتحقق منها عن طريق إزالة الأخطاء، وتخزينها في مكان واحد، مثل: مستودع البيانات أو قاعدة البيانات.

10. المراجع واللوائح ذات الصلة

1- إطار عمل ضوابط إدارة مخاطر الاحتيال وفقًا للمعيار ISO 37003

يوفر إطار عمل ضوابط إدارة مخاطر الاحتيال وفقًا للمعيار(I SO 37003) إرشاداتٍ وأفضل الممارسات للمؤسسات لتحديد مخاطر الاحتيال وتقييمها والحد من آثارها. كما يقدّم نهجًا منظمًا لإدارة مخاطر الاحتيال، مما يساعد المؤسسات على تنفيذ ضوابط وعمليات فعّالة لمنع الاحتيال واكتشافه. ما تزال هذه الوثيقة في مرحلة التشاور، ولكن لا توجد تغييرات كبيرة متوقعة على المسودة الحالية.

2- معيار منع الاحتيال لمحترفي مكافحة الاحتيال

يُحدّد معيار منع الاحتيال لمحترفي مكافحة الاحتيال المعايير والدليل الاسترشادي للمحترفين المشاركين في أنشطة مكافحة الاحتيال. ويهدف إلى تعزيز قدرات ممارسي منع الاحتيال عن طريق توفير نهج منظم لإدارة مخاطر الاحتيال، وتنفيذ تدابير فعالة لمنع الاحتيال.

3- خطة عمل إستراتيجية مكافحة الاحتيال التابعة للمفوضية الأوروبية

تُحدّد خطة عمل إستراتيجية مكافحة الاحتيال التابعة للمفوضية الأوروبية الأهداف الإستراتيجية والإجراءات اللازمة لمكافحة الاحتيال الذي يستهدف ميزانية الاتحاد الأوروبي ومصالحه المالية. وهي تتضمن تدابير لمنع الاحتيال واكتشافه والتحقيق فيه، فضلًا عن المبادرات الرامية إلى تعزيز التعاون بين مؤسسات الاتحاد الأوروبي والدول الأعضاء في مكافحة الاحتيال.

4- ورقة المناقشة الصادرة عن بنك التسويات الدولية بشأن إدارة مخاطر الاحتيال الرقمي

تتناول ورقة المناقشة الصادرة عن بنك التسويات الدولية بشأن إدارة مخاطر الاحتيال الرقمي؛ التحديات وأفضل الممارسات المتعلقة بإدارة مخاطر الاحتيال الرقمي في المؤسسات المالية وخارجها. وتناقش الاتجاهات الناشئة والتقنيات والاعتبارات التنظيمية في مجال منع الاحتيال الرقمي والاستجابة له.

5- إطار عمل البنك المركزي السعودي لمكافحة الاحتيال

أنشأ البنك المركزي السعودي إطار عمل لمكافحة الاحتيال لتمكين المؤسسات الخاضعة لتنظيمه من تحديد المخاطر المتعلقة بالاحتيال ومعالجتها بفاعلية، وذلك بهدف وضع نهج مشترك لمعالجة مخاطر الاحتيال داخل المؤسسات الأعضاء.

6- إطار عمل الأمن السيبراني للبنك المركزي السعودي

مصمم لمساعدة المؤسسات المالية في معالجة عناصر الأمن السيبراني، وتقليل مخاطر الاحتيال الرقمي.

7- وثيقة الضوابط الأساسية للأمن السيبراني من الهيئة الوطنية للأمن السيبراني

وثيقة ضوابط أساسية ملائمة لاحتياجات الأمن السيبراني للجهات والقطاعات جميعها في المملكة العربية السعودية، مما يُسهم في تقليل مخاطر الاحتيال الرقمي بشكل فعّال.

8- الرقابة الداخلية للجنة المنظمات الراعية (COSO)الإطار المتكامل

إطار شامل لإدارة ضوابط الاحتيال الداخلية، يوفر نهجاً متكاملاً لإدارة المخاطر، ويشمل ذلك الاحتيال الرقمي.

9- إطار إدارة مخاطر الاحتيال من جمعية محققي الاحتيال المعتمدين (ACFE)

موّرد شامل يحدد الإستراتيجيات والتقنيات اللازمة لتحديد وتقييم والحد من مخاطر الاحتيال الرقمي، كما يغطي جوانب مختلفة، مثل: الوقاية، والاكتشاف، والتحقيق، والاستجابة.

10- إطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتقنية (NIST)

إطار يهدف إلى مساعدة المؤسسات على إدارة ومراقبة مخاطر الأمن السيبراني، ويشمل ذلك المخاطر المتعلقة بالاحتيال الرقمي، كما أنه يُستخدم على نطاق واسع من الحكومات ومؤسسات القطاع الخاص.

11- ضوابط إدارة المخاطر واستمرارية الأعمال للحكومة الرقمية

أحد التنظيمات ضمن الإطار التنظيمي لأعمال الحكومة الرقمية، يهدف إلى رفع نضج الخدمات وتعزيز قدرة الجهة على تحديد المخاطر والتهديدات بصورة استباقية، عن طريق بناء نظام إدارة المخاطر واستمرارية الأعمال، وتتضمن هذه الوثيقة مصفوفة لتحديد مستوى أثر انقطاع أعمال الحكومة الرقمية.

12- الدليل الاسترشادي لإدارة المخاطر واستمرارية الأعمال للحكومة الرقمية

دليل استرشادي يوضح أهم الإرشادات لتصميم وتنفيذ الإطار والمكونات الأساسية لإدارة المخاطر واستمرارية الأعمال، بما يتناسب مع الجهات الحكومية.

13- المرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ (نظام حماية البيانات الشخصية ولائحته التنفيذية)

نظام يختص بحماية البيانات الشخصية المتعلقة بالأفراد في المملكة العربية السعودية.

14- المرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ (نظام مكافحة جرائم المعلوماتية)

يهدف هذا النظام إلى الحدّ من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم، والعقوبات المقرّرة لكل منها.

15- المرسوم الملكي رقم (م/72) وتاريخ 1442/9/10هـ (نظام مكافحة الاحتيال المالي وخيانة الأمانة)

نظام مختص بمكافحة الاحتيال المالي وخيانة الأمانة، وبيان عقوبة من استولى على مال للغير دون وجه حق، وعقوبة من استولى دون وجه حق على مال سُلّم إليه من غير المال العام، وعقوبة من حرّض غيره على ارتكاب الجرائم المنصوص عليها في هذا النظام، وعقوبة من شرع في القيام بالجرائم المنصوص عليها في هذا النظام، والظروف المشددة، والنص على مصادرة الأدوات والآلات والمتحصلات المتحققة من ارتكاب الجرائم، وعقوبة التشهير، والعفو من العقوبات، فيما تُعتبر النيابة العامة جهة التحقيق والادعاء، والنشر والنفاذ.

16-ضوابط تصنيف الخدمات الحكومية الرقمية الحساسة ومستويات التحقق الصادرة من هيئة الحكومة الرقمية

تُسهم في تحديد مستويات وتقنيات التحقق المناسبة للجهات الحكومية حسب حساسية خدماتها الرقمية لتمكين المستخدمين من الاستفادة من الخدمات الحكومية الرقمية، وضمان استمرارية تلك الخدمات وعدم تأثرها.

11. الملاحق

الملحق (أ)-- التقييم الذاتي الأولي لمخاطر الاحتيال الرقمي

الملحق (ب)-- دراسات حالة الحوادث

الملحق (ج)-- استبانة مكافحة الاحتيال الرقمي بواسطة التصميم

الملحق (د)-- جدول الشهادات المهنية

الملحق (أ)- التقييم الذاتي الأولي لمخاطر الاحتيال الرقمي

يحتوي النموذج -أدناه- على أسئلة إرشادية مصممة لتمكين صناع القرار من تحديد وتقييم مستوى النضج المؤسسي الحالي بشكل أفضل للتخفيف من مخاطر الاحتيال الرقمي وإدارتها ومراقبتها. وتهدف الأسئلة إلى المساعدة على تحديد تصنيفات الاحتمالية والتأثير والسرعة التي تُخَصص ذاتيًّا أيضاً. وبناءً على تصنيف المخاطر الإجمالي، قد يختار مديرو الجهات الحكومية وضع أُطر أكثر تفصيلاً لمخاطر الاحتيال الرقمي، أو تحديث الإجراءات الحالية لتغطية أيّ مخاطر متبقية بناءً على بيانات تقبُّل المخاطرة المحددة.

الرقم	العنصر	التصنيف	السؤال	نعم/لا	يُرجى إيضاح الإجابة
1	الوقاية	عملية	هل تستعينون بخبراء الاحتيال الرقمي أو المخاطر أو الأمن السيبراني في مرحلة تصميم منتجكم الرقمي؟		
2		عملية	هل تدرّبون موظفيكم وعملاءكم على مخاطر الاحتيال الرقمي وكيفية تجنبها؟		
3		عملية	هل لدى جهتكم سياسات وإجراءات واضحة وموثقة للتعامل مع الاحتيال الرقمي؟		
4		عملية	هل تتضمن خطط الرقابة الداخلية لديكم أيّ ضوابط خاصة بالاحتيال الرقمي؟		
5		تقنية	هل لديكم آليات للتحكم في الوصول إلى المعلومات الرقمية الحساسة ومراقبة هذا الوصول لمنع استخدام هذه المعلومات في عمليات احتيال؟		
6		تقنية	هل لديكم نظام أو مجموعة من الأدوات لحماية هوية المؤسسة؟		
7	الرصد	عملية	هل سبق أن تعرضت الجهة أو مستخدموها أو المستفيدون منها لحوادث احتيال رقمي؟		
8		عملية	هل تحدّدون وتوثقون المخاطر المحتملة للاحتيال الرقمي التي قد تواجهها مؤسستكم؟		
9		عملية	هل لديكم نظام لتصنيف الحوادث الأمنية يسمح بتحديد حالات الاحتيال الرقمي وتصنيفها؟		
10		تقنية	هل تخضع أنظمتكم لفحوصات دورية للكشف عن الثغرات التي يمكن استغلالها في عمليات الاحتيال الرقمي؟		
11		تقنية	هل لديكم نظام لإدارة الشكاوى، وهل يسجل حالات الاحتيال على الأفراد عن طريق خدمات الجهات الحكومية المزيفة؟		
12		تقنية	هل لديكم بروتوكولات محددة لتحديد العمليات الرقمية ذات مخاطر الاحتيال الرقمي العالية؟		
13	الاستجابة	عملية	هل لديكم خطة موثقة للاستجابة للاحتيال الرقمي؟		
14		عملية	هل لديكم إجراءات تصعيدية للتعامل مع حوادث الاحتيال الرقمي؟		
15		عملية	هل لديكم عملية لإخطار العملاء أو المستخدمين المتضررين من حوادث الاحتيال الرقمي؟		
16		عملية	هل تُجرون التحقيق في التقارير المتعلقة بالأنشطة المشبوهة سواء من المستفيدين أو الموظفين؟		
17		كادر بشري	هل تتضمن خطة استجابتكم للحوادث الأمنية إبلاغ الجهات الحكومية الأخرى عند حدوث حالات احتيال رقمي محتملة؟		
18		تقنية	هل لديكم نظام تنبيهات آلي ينشط عند اكتشاف أيّ نشاط مشبوه؛ ليبدأ عملية الاستجابة للحوادث الأمنية؟		

الرقم	العنصر	التصنيف	السؤال	نعم/لا	يُرجى إيضاح الإجابة
19	التحسين المستمر	عملية	هل تحلّلون الدروس المستفادة من التغيرات في طبيعة مخاطر الاحتيال الرقمي، والاستفادة منها في تطوير إجراءاتكم الأمنية؟		
20		عملية	هل تُؤخذ حوادث الاحتيال الرقمي بعين الاعتبار عند تصميم المنتجات والخدمات الرقمية الجديدة؟		
21		تقنية	هل هناك حلول تقنية جاهزة لإجراء تثقيف داخلي شامل للموظفين بشأن عمليات الاحتيال الرقمية؟		
22		كادر بشري	هل يتلقى مدراء مخاطر الاحتيال الرقمي تدريبًا مستمرًا لمواكبة التطورات في هذا المجال؟		
23		كادر بشري	هل تتفاعلون مع المؤسسات الأخرى ذات الصلة بشأن عمليات الاحتيال الرقمية؟		
24		كادر بشري	هل تُقيّم الإدارة العليا أداء المؤسسة في مجال إدارة مخاطر الاحتيال الرقمي باستمرار؟		
25	الإبلاغ	عملية	هل تسجلون أو تُبلّغون عن أرقام حوادث الاحتيال الرقمي؟		
26		عملية	هل تسجلون أو تُبلّغون عن أعداد عمليات الاحتيال الرقمية المتعلقة بخدمات الجهات المحتملة؟		
27		عملية	هل يجري تزويد كبار المديرين بمعلومات دوريّة حول أبرز مؤشرات مخاطر الاحتيال الرقمي بطريقة موحدة وسهلة الفهم؟		
28		كادر بشري	هل تُبلّغون الجهات الرقابية الوطنية المختصة عند وقوع حوادث احتيال رقمي؟		
29		عملية	هل هناك معايير قياس ثابتة لمراقبة وتوجيه منع الاحتيال الرقمي واكتشافه؟		
30		تقنية	هل لديكم نظام مركزي لتسجيل الحوادث الأمنية يتيح الإبلاغ عن حالات الاحتيال الرقمي؟		
31	الحوكمة	عملية	هل لديكم إطار حوكمة يتناول إدارة مخاطر الاحتيال/ التضليل الاحتيالي الرقمي؟		
32		عملية	هل لديكم مسؤول تنفيذي أو عضو مجلس إدارة مسؤول عن الإشراف على إدارة مخاطر الاحتيال الرقمي؟		
33		عملية	هل تتوافق سياساتكم وإجراءاتكم المتعلقة بالاحتيال الرقمي مع المعايير التنظيمية والقطاعية ذات الصلة؟		
34		عملية	هل تُراعى سيناريوهات الاحتيال الرقمي المحتملة عند تصميم وتنفيذ ضوابط الرقابة الداخلية ومراقبة جودة المنتجات؟		
35		عملية	هل لديكم بيان واضح ومحدّد يُحدّد مستوى قبول المخاطر المتعلقة بالاحتيال الرقمي، إضافة إلى الضوابط والإجراءات اللازمة للتعامل مع هذه المخاطر؟		
36		كادر بشري	هل يُجري مجلس الإدارة مراجعة دورية لمخاطر الاحتيال الرقمي وإستراتيجيات الحدّ من تأثيره؟		

الأسئلة السابقة تهدف إلى أن تكون مجموعة أولية لتحديد مدى تطبيق مبادئ مكافحة الاحتيال الرقمي بواسطة التصميم، لكنها ليست شاملة. كلما زاد عدد الأسئلة التي أُجيب عنها بـ"نعم"، زاد مستوى نضج الجهة فيما يتعلق بمبادئ مكافحة الاحتيال الرقمي بواسطة التصميم.

بناءً على الأسئلة المطروحة، يمكن للمتخصصين في إدارة المخاطر داخل الجهة أن يكونوا قادرين على تحديد احتمالية التعرض لمخاطر الاحتيال الرقمي وتقييم تأثيره. نظرًا للطبيعة السريعة لظهور هذه المخاطر، لا تُؤخذ السرعة في الاعتبار عند إجراء التقييم الذاتي الأولي لمخاطر الاحتيال الرقمي.

يُستخدم الجدول -أدناه- بِعدّه أداةً مؤقتةً لقياس الاستعداد، وليس تحليلًا شاملًا للمخاطر. ويمكن أن تُسهم هذه الجهود في تقديم تقدير مبدئي للاحتمالات والتأثيرات، بما يدعم التقييم الكامل لمخاطر الاحتيال الرقمي.

القياسات- التقييم الذاتي للجهات بشأن مكافحة الاحتيال الرقمي

	التقييم الذاتي بشأن مكافحة الاحتيال الرقمي					
	العنصر	0 سؤال أُجيب عنه بـ"نعم"	2 سؤالان أُجيب عنهما بـ"نعم"	3 أسئلة أُجيب عنها بـ"نعم"	5-4 أسئلة أُجيب عنها بـ"نعم"	6 أسئلة أُجيب عنها بـ"نعم"
		ناشئ	متطور	متمكن	متقدم	متميز
التقييم الذاتي الأولي لإطار عمل مكافحة الاحتيال الرقمي	الوقاية					
	الرصد					
	الاستجابة					
	الإبلاغ					
	التحسين المستمر					
	الحوكمة					

الملحق (ب)- دراسات حالة الحوادث

التزييف العميق - حادثة فيراري

الخلفية

- في واحدة من أحدث محاولات النصب، نجحت شركة فيراري في تجنب الوقوع ضحيةً لعملية نصب معقدة. استخدمت هذه الخدعة تقنية الذكاء الاصطناعي المتقدمة لانتحال شخصية الرئيس التنفيذي لشركة فيراري بِنِدِتّو فينيا بطريقة مقنعة. كان هدف الجناة هو الاحتيال على الشركة من خلال انتحال شخصية فينيا في الاجتماعات والاتصالات الافتراضية.

التداعيات

على الرغم من عدم وجود تأثير فوري، يشير الحادث نفسه إلى أن المؤسسة مستهدفة من قبل جهات تهديد منظمة تنظيمًا جيدًا.

الدروس المستفادة

تصرف المدير التنفيذي المستهدَف تصرفًا صحيحًا، إذ طرح سؤالاً فريدًا لا يعرفه بحكم علاقته، إلا الرئيس التنفيذي.

نظرة عامة على الحادث

- تلقى أحد كبار المسؤولين التنفيذيين في مجلس إدارة فيراري رسالة عبر تطبيق واتساب يزعم أنه الرئيس التنفيذي (بِنِدِتّو فينيا).
- جاءت الرسائل من رقم لم يكن الرقم المعتاد للرئيس التنفيذي.
- أشارت الرسائل إلى أن سبب استخدام رقم مختلف كان بسبب إجراء عملية استحواذ في الصين، وأن الأمر يتطلب أقصى درجات الحيطة.
- ثم أصر الجاني على إجراء اتصال هاتفي، وكان صوت فينيا مقنعًا للغاية، إذ كان متوافقًا مع لهجة جنوب إيطاليا.
- بدأ الجاني يقول إنه بحاجة إلى مناقشة أمر سري -صفقة قد تواجه بعض العقبات المرتبطة بالصين وتتطلب إجراء معاملة تَحَوُّط عملة غير محددة.

وهنا بدأ المسؤول التنفيذي المعني يرتاب، فطرح سؤالًا - طلب من الجاني أن يسمي الكتاب الذي أوصى به الرئيس التنفيذي للمسؤول التنفيذي - فأُنهيت المكالمة فورًا.

فشل التحكم في الوصول - سوسيتيه جِنِرال

الخلفية

- تشكل حادثة التداول التي وقعت في عام 2008في شركة سوسيتيه جِنِرال، وبطلها المُتداوِل جيروم كيرفْييل، مثالًا واضحًا على الكيفية التي يمكن أن تؤدي فيها حالات فشل التحكم في الوصول إلى نتائج كارثية في القطاع المالي. كان كيرفْييل قد انضم إلى الشركة للعمل في مجال الامتثال وكان يستطيع الدخول إلى أنظمة الامتثال التي احتفظ بها عندما انضم إلى قسم التداول.

التداعيات

سمحت ضوابط الوصول الضعيفة لكيرفييل ببدء تداولات غير مصرح بها، وهو ما أدى إلى خسارة قدرها 4.9 مليار دولار حين أُلغيت تلك التداولات.

الدروس المستفادة

كان للحادثة آثار واسعة النطاق على القطاع المصرفي، وفيها عِبرة للتحذير من المخاطر المحتملة المرتبطة بالأسواق المالية الحديثة.

نظرة عامة على الحادث

- التلاعب بالأنظمة الداخلية: استغل كيرفييل قدرته على الدخول إلى أنظمة الامتثال، وهو ما سمح له بإنشاء صفقات وهمية وتواريخ سابقة للمعاملات.
- أصبح هذا التلاعب ممكنًا لأن ضوابط الوصول الخاصة بالبنك لم تفصل بشكلٍ كافٍ بين الواجبات بين دوره السابق في الامتثال ومسؤولياته التجارية الجديدة.
- عادةً ما ينطوي التحكم السليم في الوصول على فصل الواجبات لمنع تضارب المصالح والعمليات غير المصرح بها.

في حالة كيرفييل، كان قادرًا على أداء مهمات كان ينبغي فصلها - مثل بدء الصفقات وحجزها ثم التلاعب بالسجلات لإخفاء المستوى الحقيقي للمخاطر.

انتحال شخصية الحكومة – الولايات المتحدة

الخلفية

- من أبرز حوادث الاحتيال انتحال شخصية الحكومة في أثناء جائحة كورونا في الولايات المتحدة. فقد استغل المحتالون الارتباك والخوف الناجمين عن الجائحة لانتحال شخصية مسؤولين ومؤسسات حكومية.

التداعيات

بين أكتوبر 2020 وسبتمبر 2021، قدرت لجنة التجارة الفدرالية أن 2 مليار دولار أمريكي سُلِبت من المستفيدين من خلال انتحال صفة مؤسسات حكومية.

نظرة عامة على الحادث

- استخدم الجُناة أساليب مختلفة مثل المكالمات الهاتفية ورسائل البريد الإلكتروني والرسائل النصية لخداع الناس وإقناعهم بأنهم يتعاملون مع ممثلين حكوميين شرعيين. وفي كثير من الحالات انتحل الجناة صفة:
- وكلاء مصلحة الضرائب: هدد الجناةُ المتضررين بالاعتقال أو الغرامات إذا لم يدفعوا الضرائب المتأخرة المفترضة أو يقدموا معلومات شخصية.
- إدارة الضمان الاجتماعي: زعم المحتالون أن رقم الضمان الاجتماعي للمتضرر قد عُلِّق بسبب نشاط مشبوه، لذلك طالبوا بمعلومات شخصية لإعادة تنشيطه.
- مراكز السيطرة على الأمراض والوقاية منها: أرسل المحتالون رسائل بالبريد الإلكتروني ورسائل مزيفة تدعي أنها من مراكز السيطرة على الأمراض والوقاية منها تقدم معلومات عن كورونا أو تطلب تبرعات.
- لجنة التجارة الفِدرالية: استخدم المنتحلون اسم لجنة التجارة الفِدرالية لإضفاء مصداقية على عمليات الاحتيال التي تنطوي غالبًا على مسابقات أو مِنَح مزيفة.

الدروس المستفادة

يجب نشر آليات حماية الهوية المؤسسية وحملات التوعية على نطاق واسع في أوقات الاضطرابات الاجتماعية.

استخدام أنظمة الإبلاغ لمكافحة الاحتيال

الخلفية

- في عام 2015كشف مكتب إدارة الموظفين في الولايات المتحدة أن أنظمته تعرضت للاختراق، وأن هذا أدى إلى سرقة معلومات شخصية حساسة لأكثر من 21 مليون موظف فِدْرالي حالي وسابق ومحتمل، وهذا يجعلها واحدة من أكبر خروقات البيانات الحكومية وأهمها في تاريخ الولايات المتحدة.

التداعيات

كان نظام إبلاغ المستخدمين أمرًا مهماً في إبلاغ المتضررين وتزويدهم بالموارد اللازمة للحد من المخاطر المرتبطة بالاختراق.

نظرة عامة على الحادث

ما إن اكتُشِف الاختراق، حتى وضع مكتب إدارة الموظفين نظاماً شاملاً لإخطار المستخدمين وتنبيه المتضررين. تضمنت عملية الإخطار هذه عدة خطوات خففت بشكل فعال إلى حد ما من خطر الاحتيال الرقمي الذي يفرضه خرق البيانات هذا:

- إشعارات البريد الإلكتروني: أرسل مكتب إدارة الموظفين الملايين من رسائل البريد الإلكتروني إلى الأفراد المتضررين لإخطارهم بالخرق وتقديم معلومات بشأن البيانات التي اختُرِقت.
- الإخطارات البريدية: أما من ليس لديهم عناوين بريد إلكتروني متاحة أو محدَّثة، فقد أرسل مكتب إدارة الموظفين رسائل ورقية لإبلاغهم بالخرق.
- موقع ويب وخط ساخن مخصصان: أنشأ مكتب إدارة الموظفين موقعَ ويب مخصصا وخطًا ساخنًا مجانيًا حيث يمكن للأفراد التحقق إن كانوا قد تأثروا بالخرق ولتلقِّي إرشادات بشأن الخطوات اللازمة لحماية أنفسهم مثل التسجيل في خدمات حماية سرقة الهوية.
- حماية سرقة الهوية ومراقبتها: في إطار الإخطار، قدم مكتب إدارة الموظفين للأفراد المتضررين مراقبة ائتمانية مجانية وتأمين سرقة الهوية وخدمات حماية أخرى لعدة سنوات.
- الإعلانات العامة: بالإضافة إلى الإخطارات المباشرة، أصدر مكتب إدارة الموظفين إعلاناتٍ وتحديثاتٍ عامةً من خلال البيانات الصحفية والإحاطات الإعلامية والموقع الرسمي على الويب لإبقاء عامة الناس على اطلاع بالحادث.

الدروس المستفادة

كان للحادث عواقب وخيمة ولكن بفضل نظام إخطار المستخدمين المتطور، يُقَدَّر أن هذا النظام تلافى قدرًا كبيرًا من الاحتيال الرقمي.

استخدام تحليلات البيانات لمكافحة الاحتيال

الخلفية

- كان الاحتيال الضريبي مشكلة كبيرة لمصلحة الضرائب الأمريكية منذ فترة طويلة، حيث كان الجناة يُقدِّمون إقرارات ضريبية احتيالية للمطالبة باسترداد عائدات لا يستحقونها. ومع تزايد شيوع التقديم الرقمي، أصبح المحتالون يوماً بعد يوم يستخدمون المعلومات الشخصية المسروقة لتقديم إقرارات مزيفة. ونما حجم المشكلة مع ظهور سرقة الهوية وغيرها من التكتيكات المتطورة.

التداعيات

أدى استخدام مصلحة الضرائب الأمريكية لتحليلات البيانات إلى منع صرف مليارات الدولارات من الإقرارات الضريبية الاحتيالية. وقد أفادت مصلحة الضرائب أن نظام الكشف عن الاحتيال الذي تعتمد عليه في الكشف عن الاحتيال منع صرف أكثر من 4 مليارات دولار من عمليات الاسترداد الاحتيالية في عام 2016.

الدروس المستفادة

من شأن التطبيق الواسع النطاق لتحليلات البيانات أن يؤدي إلى نتائج ممتازة عند مكافحة الاحتيال على المستوى الحكومي.

نظرة عامة على الحادث

نفَّذت مصلحة الضرائب الأمريكية تحليلات بيانات متقدمة للكشف عن الإقرارات الضريبية الاحتيالية ومنعها، كما استخدمت التعلم الآلي للنمذجة التنبؤية وتحليل البيانات الضخمة لفحص بيانات الإقرارات الضريبية في الوقت الفعلي.

التعرف على الأنماط: وضعت مصلحة الضرائب نماذج يمكنها التعرف على الأنماط المشبوهة في الإقرارات الضريبية مثل الشذوذ في تقارير الدخل والخصومات وتاريخ الإيداع. وقد أشارت هذه النماذج إلى الإقرارات التي انحرفت بشكل كبير عن المعايير المعمول بها.

الكشف عن الحالات الغير معتادة: استُخْدِمت أدوات التحليلات للكشف عن الحالات الغير معتادة في سلوك دافعي الضرائب مثل أوقات التقديم غير المعتادة، وتناقضات عنوان IP، والمعلومات المالية غير المتطابقة. وفي كثير من الأحيان أشارت حالات الشذوذ هذه إلى احتيال محتمل.

•تكامل البيانات: دمجت مصلحة الضرائب مصادر بيانات مختلفة بما في ذلك سجلات التقديم السابقة، والبيانات المالية لأطراف ثالثة، والمعلومات من وكالات حكومية أخرى – لإنشاء رؤية أكثر شمولًا لكل إقرار ضريبي. وقد ساعد هذا على مطابقة البيانات والتحقق من صحة البيانات المقدمة في الملفات.

•التعلم الآلي: تعمل خوارزميات التعلم الآلي على تحسين نماذج اكتشاف الاحتيال باستمرار من خلال التعلم من محاولات الاحتيال الناجحة وغير الناجحة. وقد سمح هذا النهج التكيفي لمصلحة الضرائب برصد التطورات في التكتيكات.

التعاون مع الشركاء الخارجيين: تعاونت مصلحة الضرائب مع المؤسسات المالية ودافعي الرواتب ووكالات الضرائب الحكومية لمشاركة البيانات وتحديد أنماط الاحتيال بشكل أنجع. وسَّع هذا النهجُ المتعددُ الأطراف مجموعةَ البيانات وعزَّز القدرة التحليلية.

نموذج للإبلاغ عن حوادث الاحتيال الرقمي

الخلفية

- إشرح عن خلفية الحادث

التداعيات

التداعيات الأساسية

الدروس المستفادة

التحسينات الأساسية التي تم تنفيذها

نظرة عامة على الحادث

كتابة نظرة عامة عن الحادث

الملحق (ج)- استبانة مكافحة الاحتيال الرقمي بواسطة التصميم

الرقم	السؤال	نعم / لا
1	هل تُقيّمون مخاطر الاحتيال الرقمي عند استخدام منتجاتكم؟	
2	هل يُشترط إلزاميًّا إشراك خبراء في مخاطر الاحتيال الرقمي في مرحلة بناء متطلبات المنتج المُوجه للمستفيدين؟	
3	هل هناك حد أدنى لتأثير مخاطر الاحتيال يُستخدم للتمييز بين التطبيقات ذات المخاطر العالية والمنخفضة؟	
4	هل هناك شرط إلزامي لتقييم مخاطر الاحتيال الرقمي في المنتجات والتطبيقات والخدمات جميعها الموجهة للمستفيدين؟	
5	هل تتضمن التطبيقات والمنتجات والخدمات خاصية الإبلاغ عن الحوادث كجزء من تجربة المستخدم؟	
6	هل تحتوي التطبيقات والمنتجات والخدمات على ميزة الإشعارات المشفرة؟	
7	هل صُمّمت التطبيقات والمنتجات والخدمات لتكون قابلة للتكيف مع بيئات الضوابط النشطة؟	
8	هل يُخصص معرّف فريد عند تصميم الخدمات الحكومية الرقمية لربط الحوادث بالتطبيقات أو المنتجات والخدمات الرئيسة؟	
9	هل تتمتع منتجاتكم وتطبيقاتكم وخدماتكم بالقدرة على تعطيل الاحتيال الرقمي الحاد؟	
10	هل هناك شرط تصميمي يلزم استخدام وسائل اتصال مشفرة في التطبيقات والمنتجات والخدمات عالية المخاطر جميعها؟	

الأسئلة السابقة تهدف إلى أن تكون مجموعة أولية لتحديد مدى تطبيق مبادئ مكافحة الاحتيال الرقمي بواسطة التصميم، لكنها ليست شاملة. كلما زاد عدد الأسئلة التي أُجيب عنها بـ"نعم"، زاد مستوى نضج الجهة فيما يتعلق بمبادئ مكافحة الاحتيال الرقمي بواسطة التصميم.

الملحق (د)- جدول الشهادات المهنية

#	اسم المؤهل / البرنامج	الجهة المانحة
1	شهادة احترافية في الوقاية من الاحتيال	CIFAS
2	شهادة احترافية في التحقيق في الاحتيال	CIFAS
3	أخصائي مكافحة احتيال معتمد	CIFAS
4	ممارس مكافحة الاحتيال الرقمي معتمد	CIFAS
5	أخصائي الأدلة الجنائية الرقمية	SANS
6	محترف معتمد في منع الاحتيال	ACFE
7	مُدقق احتيال معتمد	ACFE
8	أخصائي مكافحة احتيال معتمد	CFS
9	أخصائي معتمد في الجرائم المالية	ACFE
10	محقق معتمد في الجرائم الإلكترونية	ACFCI

هيئة الحكومة الرقمية
Digital Government Authority

DGA.GOV.SA