الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

إرشادات الأمن السيبراني

لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

بسم الله الرحمن الرحيم

تنويه: تم إعداد الإرشادات الواردة في هذه الوثيقة بناءً على أفضل الممارسات في مجال الأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية، وهي إرشادات توعوية بهدف تقديم المعلومات فحسب. وعند وجود تعارض بينَ ما ورد في هذه الوثيقة؛ مع أي متطلبات إلزامية؛ فإن المتطلبات الإلزامية يكون لها الأولوية. وللحد من المخاطر المتعلّقة بالأمن السيبراني، والتخفيف من آثارها في الوقت المناسب؛ تحُث الهيئة الوطنية للأمن السيبراني جميع الجهات بإجراء تقييمات دورية لتلك المخاطر.

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج الجهة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس الجهة مع الأشخاص المعنين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين في نفس الجهة أو جهة أخرى على علاقة معهم أو في نفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

بروتوكول الإشارة الضوئية (TLP): 2

1. المقدمة 4
2. الأهداف 5
3. نطاق التطبيق 6
4. العلاقة مع إصدارات الأمن السيبراني الوطنية الأخرى 6
5. إرشادات الأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية 7
6. ملاحق 9

1. المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بإعداد إرشادات الأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية، وذلك بعد إجراء دراسة شاملة لعدة إرشادات ومعايير وأطر وضوابط عالمية تتعلق بالأمن السيبراني، وتحليل الوضع الراهن والمتطلبات التشريعية والتنظيمية ذات العلاقة، وتحليل ماتم رصده من الحوادث والهجمات السيبرانية المرتبطة بالتحقق من الهوية.

تتكون إرشادات الأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية من ثلاثة محاور رئيسية:

- تحديد مستوى ضمان التحقق.
- اختيار تقنيات التحقق المتوافقة مع مستوى ضمان التحقق المستهدف.
- المراجعة والتدقيق.

2. الأهداف

تهدف هذه الإرشادات إلى تضمين أفضل ممارسات الأمن السيبراني وتطبيقها لضمان هوية المستخدم لدى الجهات التي تقوم باستضافة أو تشغيل خدمات الكترونية. وتستند هذه الممارسات إلى المعايير الرائدة مما يساعد الجهات على تقليل مخاطر الأمن السيبراني للخدمات الإلكترونية التي تنشأ من التهديدات المرتبطة بآلية التحقق من الهوية.

وتأخذ هذه الإرشادات في الحسبان المحاور الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

- الاستراتيجية (Strategy)
- الأشخاص (People)
- الإجراء (Process)
- التقنية (Technology)

3. نطاق التطبيق

توصي الهيئة الجهات التي تستضيف أو تشغل أي من الخدمات الإلكترونية في المملكة (ويشار لها جميعًا في هذه الوثيقة باسم "الجهة") باتباع الإرشادات؛ بهدف ضمان تطبيق أفضل الممارسات، والتقليل من مخاطر الأمن السيبراني، التي قد تنتج من استخدام هذه الخدمات الإلكترونية.

ونظرًا للطبيعة المتغيرة باستمرار للتهديدات السيبرانية؛ تحث الهيئة الجهات على المراجعة الدورية لمدى الحاجة إلى اتخاذ تدابير إضافية فيما يتعلق بالأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية.

4. العلاقة مع إصدارات الأمن السيبراني الوطنية الأخرى

تساهم إرشادات الأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية في تعزيز الأمن السيبراني للجهات المشمولة ضمن نطاق الضوابط الأساسية للأمن السيبراني (ECC - 1 : 2018)، كما يمكن لأي جهة أخرى في المملكة الاستفادة من هذه الارشادات.

5. إرشادات الأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية

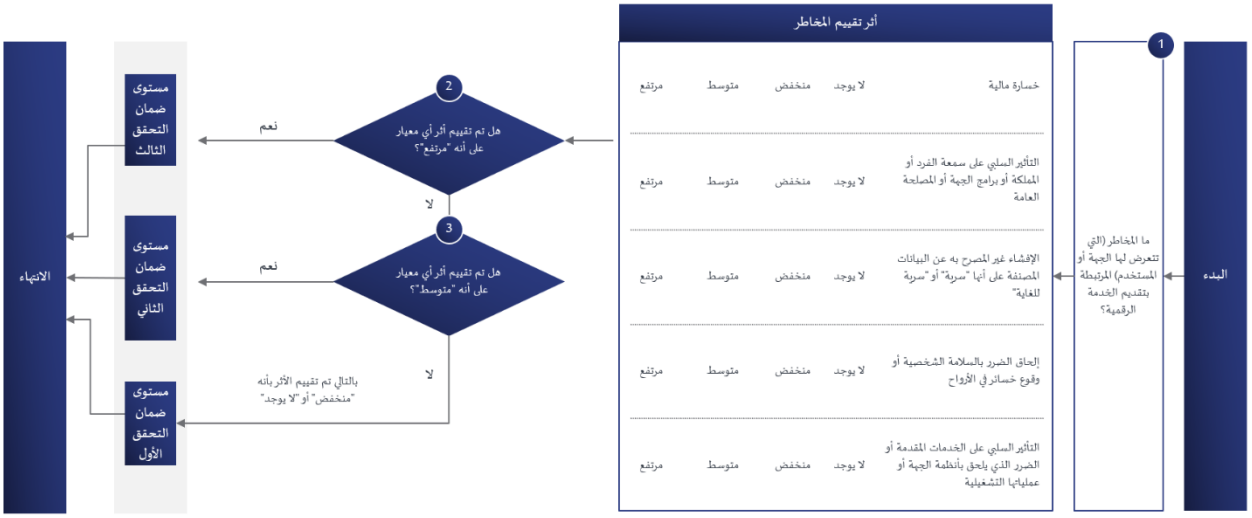
الإرشادات	
1	تحديد مستوى ضمان التحقق
الهدف: تصنيف مستوى الخدمات الإلكترونية حسب مخاطرها؛ لاختيار مستوى التحقق المناسب لكل خدمة	
1.1	تحديد مستويات الأمان والتحقق المطلوبة للوصول إلى الخدمة الإلكترونية، والتي تتكون في الغالب من 3 مستويات وهي: 1.1.1 المستوى الأول (مستوى ضمان التحقق الأول): مستوى منخفض من الأمان والتحقق المطلوب للتأكد من هوية المستخدم، ويتطلب كحد أدنى التحقق أحادي العنصر. 1.1.2 المستوى الثاني (مستوى ضمان التحقق الثاني): مستوى متوسط من الأمان والتحقق المطلوب للتأكد من هوية المستخدم، ويتطلب كحد أدنى التحقق ثنائي العناصر. 1.1.3 المستوى الثالث (مستوى ضمان التحقق الثالث): مستوى مرتفع من الأمان والتحقق المطلوب للتأكد من هوية المستخدم، ويتطلب كحد أدنى التحقق ثلاثي العناصر.
1.2	تقييم الأثر المحتمل من فشل عملية التحقق بناء على المعايير الآتية: 1.2.1 الخسارة المالية: ويعني هذا المعيار التأثير المالي على المستخدم الفرد أو الجهات المتأثرة. 1.2.2 التأثير السلبي على سمعة الفرد أو المملكة أو برامج الجهة أو المصلحة العامة: ويعني هذا المعيار تضرر سمعة الفرد أو المملكة، وكذلك تضرر برامج الجهة أو المصلحة العامة بشكل عام. 1.2.3 الإفشاء غير المصرح به عن البيانات المصنفة على أنها "سرية" أو "سرية للغاية" أو "بيانات شخصية": ويعني هذا المعيار أي تأثير على بيانات ومعلومات المستخدم الفرد أو الجهة، حيث يرتبط ذلك بالمشاركة غير المصرح بها للمعلومات الحساسة أو نشرها. 1.2.4 إلحاق الضرر بالسلامة الشخصية أو وقوع خسائر في الأرواح: ويعني هذا المعيار تأثر سلامة الأفراد، حيث يرتبط ذلك بقضايا السلامة الشخصية. 1.2.5 التأثير السلبي على الخدمات المقدمة أو الضرر الذي يلحق بأنظمة الجهة أو عملياتها التشغيلية.
1.3	تحديد مستويات تقييم الأثر المحتمل من فشل عملية التحقق إلى عدة مستويات، حسب التأثير. مثل: • منخفض. • متوسط. • مرتفع.
1.4	تحديد مستوى ضمان التحقق المطلوب باتباع الخطوات الآتية: 1.4.1 تقييم الأثر المحتمل من فشل عملية التحقق لجميع معايير التأثير المحددة في الفقرة 1.2.

	1.4.2 عند تحليل الأثر، يتم التأكد من مراعاة جميع النتائج المباشرة وغير المباشرة المتوقعة لفشل عملية التحقق، بما في ذلك احتمال وجود أكثر من نتيجة. وفي حال عدم انطباق معيار التأثير، يتم اختيار لا يوجد. 1.4.3 في حال كان تقييم أي معيار من معايير التأثير "مرتفعًا"، يتم اختيار مستوى ضمان التحقق الثالث. أما إذا كان تقييم أي من معايير التأثير "متوسطًا"، فيتم اختيار مستوى ضمان التحقق الثاني. وبخلاف ذلك، يتم اختيار مستوى ضمان التحقق الأول. 1.4.4 يجب ألا يتعارض مستوى ضمان التحقق الذي تم اختياره مع ما يصدر كمتطلبات إلزامية من الهيئة الوطنية للأمن السيبراني
2	اختيار تقنيات التحقق
الهدف: اختيار التقنيات المناسبة للتحقق من هوية مستخدمي الخدمات الإلكترونية بناء على تصنيفها	
2.1	تتكون آلية التحقق من 3 عناصر وهي كالآتي: 2.1.1 عنصر الملازمة: وهو سمة حيوية متعلقة بالمستخدم (Something You Are) مثل صورة الوجه أو بصمات الأصابع. 2.1.2 عنصر الحيازة: وهو شيء يملكه المستخدم (Something You Have) مثل رقم الطلب. 2.1.3 عنصر المعرفة: وهو شيء يعرفه المستخدم (Something You Know) مثل الرمز الشخصي أو كلمة المرور.
2.2	اختيار تقنيات التحقق المتوافقة مع مستوى ضمان التحقق المستهدف (الأمان والتحقق المطلوب)، تشمل التقنيات الآتي: 2.2.1 التحقق أحادي العنصر (One-factor authentication): ● مثال: استخدام تقنية عنصر الحيازة أو عنصر المعرفة. 2.2.2 التحقق ثنائي العناصر (Two-factor authentication): ● مثال: استخدام تقنية عنصر الحيازة وعنصر المعرفة. 2.2.3 التحقق ثلاثي العناصر (Multi-factor authentication): ● مثال: استخدام تقنية عنصر الحيازة وعنصر المعرفة وعنصر الملازمة.
3	المراجعة والتدقيق
الهدف: ضمان التأكد من أن إرشادات الأمن السيبراني لاختيار مستوى التحقق من هوية مستخدمي الخدمات الإلكترونية يتم تطبيقها على أفضل وجه وأن يكون لها الأثر الإيجابي من تقليل المخاطر الناتجة عن التحقق من هوية المستخدمين.	
3.1	مراجعة وقياس أثر تطبيق هذه الارشادات والعمل على تحديثها بشكل دوري.
3.2	مراجعة تطبيق وتحديث التقنيات والمعايير بشكل دوري.

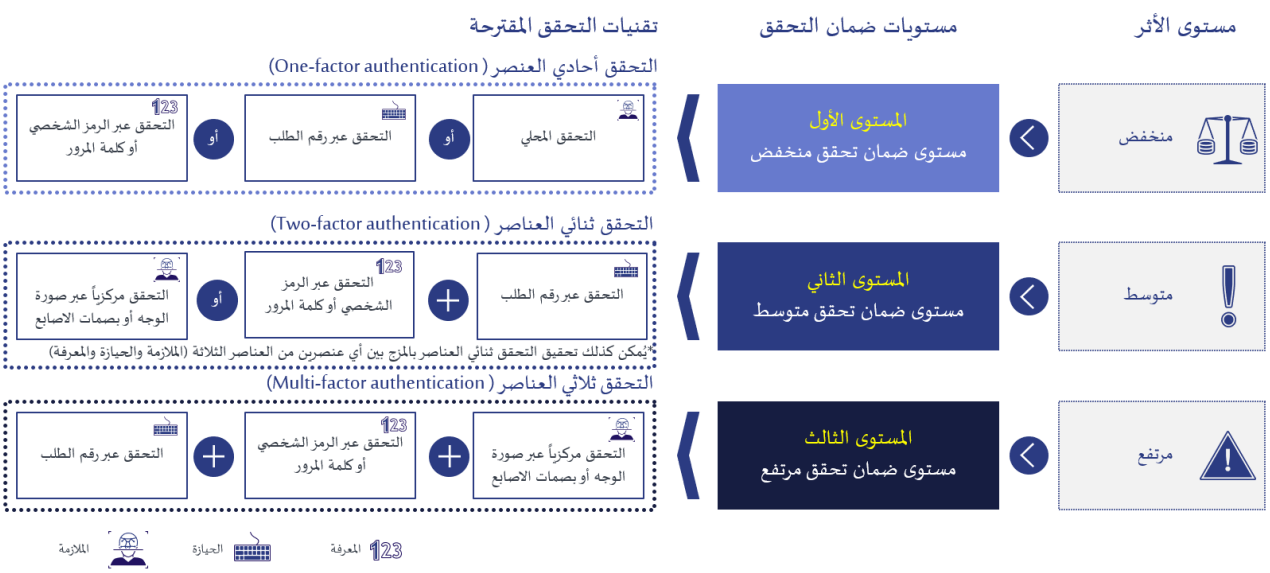
6. ملاحق

6.1 ملحق (أ): آلية تحديد مستوى ضمان التحقق المناسب

الاجراء المقترح لتحديد مستوى ضمان التحقق المناسب لكل خدمة الكترونية



6.2 ملحق (ب): مثال توضيحي لاستخدام تقنيات التحقق في كل مستوى من مستويات ضمان التحقق الثلاثة



6.3 ملحق (ج): مصطلحات وتعريفات

يوضح الجدول (1) أدناه بعض المصطلحات وتعريفاتها، التي ورد ذكرها في هذه الإرشادات.

المصطلح	التعريف
عنصر الملازمة	وهو سمة حيوية متعلقة بالمستخدم (Something You Are) مثل صورة الوجه أو بصمات الأصابع.
عنصر الحيازة	وهو شيء يملكه المستخدم (Something You Have) مثل رقم الهوية.
عنصر المعرفة	وهو شيء يعرفه المستخدم (Something You Know) مثل الرمز الشخصي أو كلمة المرور.

جدول 1 : مصطلحات وتعريفات


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority