



الوكالة الوطنية للأمن السيبراني  
National Cyber Security Agency



المبادرة الوطنية للسلامة الرقمية  
Digital Safety National Initiative

# المؤتمر الدولي للسلامة الرقمية



في عالم متزايد الترابط وقائم على التكنولوجيا وتطور البنى الرقمية والأنظمة السحابية وأجهزة إنترنت الأشياء؛ اتخذ مفهوم السلامة الرقمية أبعاداً وتحديات جديدة، وتوسّعت مساحة السطح المعرضة للهجمات بشكل كبير؛ فالخدمات التي يقدّمها الفضاء السيبراني تنطوي على مخاطر واسعة.

وتشير المؤشرات السيبرانية الدولية إلى تصاعد حادّ وغير مسبوق في حجم التهديدات السيبرانية التي تُواجه العالم أجمع، وتطال تأثيراتها السلبية الحكومات والشركات والمجتمعات والأفراد، وتظهر هذه التهديدات على مستويين كمّي ونوعي. فعلى المستوى الكمّي، يتعرّض العالم يومياً لملايين الهجمات السيبرانية، ومن المتوقع أن تتجاوز الخسائر الناجمة عن هذه الهجمات 10 تريليونات دولار في عام 2025م.

أمّا على المستوى النوعي، فهناك، وبشكل مستمر، أنماط جديدة من التهديدات السيبرانية، خاصةً في ظل الصعود المتسارع للذكاء الاصطناعي، والذكاء الاصطناعي التوليدي، والتوائم الرقمية، وعوالم الميتافيرس، والتي يتم استخدامها لتطوير أشكال جديدة من التهديدات السيبرانية؛ ما يضع العالم أجمع في تحدٍّ خطير، يتطلب

بذل المزيد من الجهود الدولية لمواجهة تداعيات هذا الواقع، والعمل على تطوير الإستراتيجيات الوقائية في الأمن السيبراني والسلامة الرقمية.

ولذلك، فإن التعامل الفعّال مع التهديدات السيبرانية المتقدمة يتطلب الاستناد إلى منهجيات عمل واضحة وفعّالة ومدروسة، قائمة على تحديد نقاط الضعف في البيئة السيبرانية الدولية، ودراسة الاتجاهات الحالية للفضاء السيبراني، وتحديد أسس التعامل مع هذه المستجدات اعتماداً على منهجية علمية قوية ورصينة، ومن هنا كانت فكرة المؤتمر الدولي للسلامة الرقمية.

إنّ المؤتمر الدولي للسلامة الرقمية والذي يأتي في سياق المبادرة الوطنية للسلامة الرقمية، والتي تنظّمها الوكالة الوطنية للأمن السيبراني في دولة قطر، يتجاوز حدود البحث التقليدي، وابتعد عن التكرار النمطي، وعوضاً عن ذلك يسعى إلى أن يكون علامةً فارقةً في قطاع الأمن السيبراني والسلامة الرقمية، من خلال تركيزه على محاور بالغة الحداثة، وينطلق من المبدأ السيبراني: «جديد اليوم قديم الغد»، وهذا ما يُعزّز فرص نجاحه وتحقيق أهدافه، ليس على مستوى دولة قطر فحسب، بل على مستوى العالم أجمع.



المبادرة الوطنية للسلامة الرقمية  
Digital Safety National Initiative

## المبادرة

### الوطنية للسلامة الرقمية

في سياق سَعْيها لتعزيز مؤشرات الأمن السيبراني والسلامة الرقمية على مستوى الدولة والمجتمع، وانطلاقاً من أهمية استقرار الفضاء السيبراني الوطني؛ أطلقت الوكالة الوطنية للأمن السيبراني المبادرة الوطنية للسلامة الرقمية، والتي تستهدف شرائح المجتمع كافة، وتتوجّه لهم بمحتوى توعويّ سيبراني بالغ الحداثة، وتتبنّى جملةً من الأنشطة والفعاليات المختلفة، والتي تتكامل فيما بينها لتحقيق أهداف المبادرة وبلوغ رؤيتها ورسالتها.

وفي سياق الفعاليات التي تتبنّاها المبادرة الوطنية للسلامة الرقمية؛ سيتم تنظيم المؤتمر الدولي للسلامة الرقمية، والذي يُعدّ منصةً تجمع الخبراء والمتخصصين ومختلف أصحاب المصلحة على المستوى الوطني والإقليمي والدولي؛ بهدف تحديد تعزيز استقرار الفضاء السيبراني، وتحديد أسس التعامل مع التهديدات السيبرانية المتصاعدة، وتعزيز مؤشرات الأمن السيبراني والسلامة الرقمية على مستوى الحكومات والمجتمعات.

## فكرة

## المؤتمر



تنطلق فكرة المؤتمر الدولي للسلامة الرقمية من أهمية الأمن السيبراني والسلامة الرقمية، ومن تصاعد التهديدات السيبرانية التي تواجه الدول والمؤسسات والمجتمعات، ومن ضرورة تضافر الجهود الدولية ومشاركة المعارف والأبحاث الجديدة، وتبادل الخبرات السيبرانية؛ بهدف تعزيز الإستراتيجيات الوقائية السيبرانية. وتتسع فكرة المؤتمر لتشمل مناقشة أفكار ومحاور بالغة الحداثة، والتباحث في قضايا سيبرانية لم يتطرق إليها أحد من قبل؛ فالمؤتمر يسعى للابتعاد عن النمطية والتكرار، والحرص على تقديم قيمة مضافة سيبرانية جديدة على المستوى الوطني والإقليمي والدولي.



## أهمية

## المؤتمر

يستمد المؤتمر أهميته بشكل رئيس من أهمية الأمن السيبراني والسلامة الرقمية، ومن ضرورة مواجهة التحديات السيبرانية المتصاعدة، وفيما يلي تبيان لأهم النقاط التي توضح أهمية المؤتمر:

### تصاعد التهديدات السيبرانية الدولية،

وضرورة تبني منهج علمي في التعامل مع هذه التهديدات.

### الأمن السيبراني والسلامة الرقمية

أصبحت من عناصر الأمن القومي للدول؛ مما يتطلب الاهتمام المتزايد بتعزيز المؤشرات السيبرانية.

### التطورات السيبرانية المتسارعة

والتي تتزامن مع تهديدات سيبرانية مُتقدّمة؛ الأمر الذي يتطلب تضافر الجهود الدولية لمواجهة هذه التحديات.

### ضرورة جمع خبراء ومُتخصّصي الأمن السيبراني

والسلامة الرقمية على المستوى الدولي في منصة واحدة، بما يهيئ بيئة مناسبة لمناقشة الاتجاهات المستقبلية للأمن السيبراني والسلامة الرقمية.

### يُشكّل المؤتمر قيمة معرفية سيبرانية مُضافة

تسهم في تعزيز قدرة الحكومات والمؤسسات على تعزيز أمنها السيبراني.

### ضرورة تطوير منهجية دولية واحدة

للتعامل مع المتغيّرات السيبرانية الدولية، وما تفرزه من مخاطر وتحديات.

### التطور المتسارع للذكاء الاصطناعي

واستخدام هذه التقنية في الهجمات السيبرانية، مما يتطلب السعي إلى وضع أسس لزيادة الاعتماد على الذكاء الاصطناعي في تطوير الإستراتيجيات الوقائية في الأمن السيبراني.

## المؤتمر

تتمحور أهداف المؤتمر بشكل رئيس حول دراسة آفاق السلامة الرقمية وتهديدات الأمن السيبراني في ضوء التطورات التكنولوجية والتحديات المستقبلية، وفيما يلي تبيان للأهداف التفصيلية للمؤتمر:

1

تعزيز موقع دولة قطر كمركز إقليمي ودولي رائد في مجال الأمن السيبراني والسلامة الرقمية.

2

الاستفادة من التجارب الدولية الرائدة في الأمن السيبراني، وإسقاط نتائج هذه التجارب على تجربة دولة قطر.

3

وضع منهج استباقي وشامل لمواجهة التحديات السيبرانية التي تفرضها التهديدات المتطورة.

4

تحسين القدرة على اكتشاف التهديدات والاستجابة لها عبر تطوير أسس لقياس مؤشرات السلامة الرقمية بخلاف المؤشرات التقليدية التي تعكس فعالية الضوابط الأمنية بشكل حقيقي.

5

تحديد دور الذكاء الاصطناعي في دعم السلامة الرقمية، وإمكانية استخدام أدواته وأساليه كتهديد للأمن السيبراني.

6

مناقشة دور المناورة السيبرانية في تطوير قدرات الأمن السيبراني؛ نظراً لدورها الكبير في اختبار قدرات الدفاع والاستجابة ضد الهجمات السيبرانية.

## ضيوف

## المؤتمر

استناداً إلى البُعد الدولي للقضايا التي يطرحها المؤتمر وتعزيزاً للأثر المتوقَّع منه؛ سيتم دعوة شخصيات رائدة على المستوى الدولي في الأمن السيبراني والسلامة الرقمية. وفيما يلي تبيان لأهم الضيوف المقترحين للمؤتمر:



- نخبة من كبار المسؤولين في دولة قطر
- نخبة من الخبراء وأساتذة الجامعات في الأمن السيبراني والسلامة الرقمية
- ممثلون عن كبرى الشركات التكنولوجية الدولية.
- ممثلون عن كبرى المراكز البحثية في مجال السلامة الرقمية.
- صحفيون وإعلاميون.
- ممثلون عن المنظمات الدولية ذات الصلة، مثل:





**مكان وتوقيت**

**المؤتمر**



**الدوحة - قطر**

**أبريل 2025م**







## القيمة المضافة

### للمؤتمر

يُسهم المؤتمر في تقديم قيمة سيبرانية مضافة، تظهر من خلال عدة محاور، فيما يلي تبيان لأهمها:

#### المحور الأول: القيمة السيبرانية المضافة

تظهر القيمة السيبرانية المضافة للمؤتمر؛ من خلال إسهامه في جَمْع خبراء دوليين في مجال الأمن السيبراني والسلامة الرقمية؛ إضافةً لصُناع القرار في مجال الفضاء السيبراني، وأساتذة جامعات، وممثلين عن كبرى الشركات التكنولوجية الدولية، وممثلين عن المراكز البحثية في مجال الأمن السيبراني والسلامة الرقمية.

#### المحور الثاني: القيمة العلمية المضافة

تركيز المؤتمر على القضايا العلمية فائقة الحداثة يُعزّز من قيمته العلمية المضافة، لا سيما أنه يهتمّ بالذكاء الاصطناعي وتأثيره على قضايا الأمن السيبراني والسلامة الرقمية، وكيفية استثمار هذه التقنيات الحديثة في تعزيز المؤشرات السيبرانية، ويُسلّط الضوء على الوقاية من مخاطر التقنيات الحديثة، لا سيما فيما يتعلّق باستثمار الذكاء الاصطناعي في التهديدات السيبرانية.

## منهجية اختيار

### محاور المؤتمر

سعيًا لتحقيق الأثر المتوقع من المؤتمر، وتعزيزاً للقيمة المضافة السيبرانية للمؤتمر، تم اختيار المحاور المقترحة بناءً على منهجية علمية، قائمة على الأسس الآتية:



## المؤتمر

يسعى المؤتمر إلى تغطية عددٍ من المحاور لتحقيق أهدافه، وفيما يلي تبيان لأهمّ المحاور التي يسعى المؤتمر لتغطيتها:

02



الذكاء الاصطناعي والسلامة الرقمية.

01



نحو مؤشّر دولي للسلامة الرقمية.

04



دمج السلامة الرقمية في مناهج التعليم المدرسي والجامعي.

03



الاتجاهات الحديثة في إستراتيجيات التدريب والتوعية بالسلامة الرقمية.

05



مستقبل السلامة الرقمية.

# جلسات المؤتمر



## الجلسة الأولى

### نحو مؤشر دولي للسلامة الرقمية

يَنبُذ من تحليل البيئة الأمنية الدولية أن جهود وأدوات تحقيق الأمن السيبراني والسلامة الرقمية آخذة في الصعود عالمياً، على مستوى الأفراد والدُّول والمؤسسات والجهات في القطاعين العام والخاص؛ من أجل تأمين الفضاء السيبراني، وذلك مع تسارع التقدُّم التكنولوجي، وما يشهده العالم من تزايد التهديدات السيبرانية بكافة أنواعها من جرائم سيبرانية وحروب سيبرانية.

بناءً على ذلك، أصبح العالم في حاجةٍ إلى توحيد جهوده بمجال الأمن السيبراني والسلامة الرقمية لتقويض المخاطر والتهديدات الأمنية على المستويين الوطني والدولي، ويوفّر المؤشر الدولي للسلامة الرقمية إطاراً مُوحّداً لقياس مستوى السلامة الرقمية، وتحديد نقاط الضعف والتحديات التي تُواجه الدول والشركات على حدٍّ سواء؛ حيث يقوم على أُسس جديدة لمؤشرات الأمن السيبراني تعكس فعالية الإجراءات والضوابط الأمنية بشكلٍ واقعيٍّ بخلاف المؤشرات التقليدية التي لم تُعدّ قادرةً على تمثيل الواقع الحقيقي بسبب البيئة الديناميكية للتهديدات الحالية والمستقبلية.

### محاوِر الجلسة

- ملامح الفجوة الأمنية السيبرانية بين الدول النامية والدول المتقدّمة.
- منهجية قياس مؤشرات الأمن السيبراني والسلامة الرقمية.
- ضرورة وجود مؤشر دولي للسلامة الرقمية.

01



## الجلسة الثانية

### الذكاء الاصطناعي والسلامة الرقمية

يشهد الأمن السيبراني تحولاً بفضل الذكاء الاصطناعي (AI)، الذي يعمل على تحسين التدابير الأمنية؛ من خلال تحديد التهديدات الفعلية والتخفيف من آثارها، وتمكين أنظمة الاستجابة الآلية، والقيام بالتحليلات التنبؤية. لذا تتجه الدول والمؤسسات المعنية إلى الاعتماد على تقنيات الذكاء الاصطناعي في إجراء التحليلات المتقدمة للبيانات، وتطوير أنظمة الكشف عن التهديدات، وتقديم حلول أمنية ذاتية التصحيح. إذ يذخر الذكاء الاصطناعي (AI) بالعديد من التطبيقات في مجال الأمن السيبراني التي تعمل على تحسين حماية الأصول الرقمية، وبفضلها تمكّنت الأنظمة المعتمدة على الذكاء الاصطناعي من تحليل كميات كبيرة من البيانات بشكلٍ أسرع. كما أن أتمتة المهام الأمنية المنتظمة، مثل مراقبة حركة مرور الشبكة والاستجابة للحوادث السيبرانية أسهم في تخفيف العبء عن العنصر البشري؛ ليتفرّغ لمواجهة المشكلات السيبرانية الأكثر تعقيداً.

وفي ذات الوقت يتم استغلال الذكاء الاصطناعي في تطوير الهجمات السيبرانية، ما يجعل من هذه التقنية سلاحاً ذا حدين، لذلك لا بد من تطوير منهجيات دولية في التعامل مع الذكاء الاصطناعي، بما يُعزّز من الإيجابيات ويُعالج السلبيات.

### محاوِر الجلسة

- تأثير الذكاء الاصطناعي على السلامة الرقمية: الفرص والتحديات.
- نحو بروتوكول دولي ناظم للذكاء الاصطناعي.
- الذكاء الاصطناعي بين السلامة الرقمية والتهديدات السيبرانية.



## الجلسة الثالثة

### الاتجاهات الحديثة في إستراتيجيات التدريب والتوعية بالسلامة الرقمية

مع ازدياد حجم وتعقيد الهجمات السيبرانية، لم تكن الحاجة إلى الوعي الرقمي والتدريب على الأمن السيبراني بمثل هذا الحجم في أي وقت مضى؛ فالتغييرات السريعة في البيئة السيبرانية، عززت من الحاجة إلى تدريبات متّسقة على كيفية تعزيز مؤشرات الأمن السيبراني والسلامة الرقمية؛ إذ تشير التقديرات إلى أن 95% من انتهاكات الأمن السيبراني ناتجة عن خطأ بشري.

لهذا يساعد التدريب والتوعية الموجهة إلى فئات المجتمع المختلفة في تطوير معرفتهم بأفضل الممارسات للحفاظ على أمان البيانات الحساسة، وإجراءات الاستجابة لمعالجة وإدارة المخاطر، وتعلّم كيفية تحديد التهديدات وتقييم مستويات المخاطر، والإبلاغ عن الحوادث.

وفي هذا السياق تتطور أدوات التوعية السيبرانية، على المستوى الشكلي والمضمون، فالمحتوى التوعوي يتطور بشكل متسارع، كما أن أدوات التوعية هي الأخرى تتطور، ويتم الاعتماد على التدريب والتوعية بالمحاكاة، وباستخدام تقنيات تكنولوجية حديثة.

### محاوّر الجلسة

- فعالية التوعية والتدريب بين الأدوات التقليدية والمبتكرة.
- الذكاء الاصطناعي وتطوير أدوات ومنهجيات التدريب والتوعية.
- دور أصحاب المصلحة في تحديد فاعلية الأدوات التدريبية السيبرانية.

03



## الجلسة الرابعة

### دَمَج السلامة الرقمية في مناهج التعليم المدرسي والجامعي

أدَّى التطور المستمر للتهديدات السيبرانية، وظهور تهديدات جديدة مرتبطة بالتقنيات الناشئة، إلى الحاجة لزيادة مرونة التعامل مع التهديدات المستقبلية عن طريق الوقاية والاستجابة السريعة، ومن أجل تفعيل ذلك اتجهت العديد من دُول العالم إلى دَمَج معايير واشتراطات السلامة الرقمية في المناهج التعليمية. جهود التدريب والتوعية السيبرانية تكتسب فاعليتها من خلال استمراريتها، ولذا فإن بدء جهود التوعية في مراحل عمرية مُبكرة يُعدّ عاملاً حاسماً في تحقيق الفاعلية المطلوبة، ما يُعزّز من أهمية التوجّه بمحتوى توعويّ سيبرانيّ للطلبة في مختلف المراحل الدراسية، بما يشمل طلبة الجامعات؛ من خلال أخذ طبيعة الاحتياجات التوعوية الفعلية بعين الاعتبار، وهنا لا بد من الاستفادة من التجارب الدولية الرائدة في هذا المجال.

#### محاوِر الجلسة

- التحوُّل والتعلُّم الرقمي: نموذج تربوي جديد.
- صناعة المناهج التعليمية ومحو الأمية الرقمية.
- نحو تعليم مُدمَج يُحقِّق السلامة الرقمية.

04





## الجلسة الخامسة

### مستقبل السلامة الرقمية

إنَّ التهديدات السيبرانية المتقدّمة، وتكامل أساليب التهديدات السيبرانية؛ كالهندسة الاجتماعية والتشفير المتطور، وامتلاك الجهات الخبيثة لموارد متطوّرة وقدرات بشرية خبيرة، جميعها شكّلت تحدياً كبيراً لمستقبل السلامة الرقمية، ومدى جهوزية المؤسسات الحكومية والمؤسسات الخاصة بسيناريوهات وإستراتيجيات أمنية وقائية قادرة على الدفاع ضد الهجمات السيبرانية، وتسريع عمليات التعافي عند حدوث هجوم. إنَّ فاعلية الجهود الرامية لتعزيز مؤشرات الأمن السيبراني والسلامة الرقمية، تتطلّب الاهتمام المستمر بدراسة الاتجاهات الدولية في مجال السلامة الرقمية، والاهتمام بالتهديدات الناشئة، وتطوير محتوى توعويّ يتناسب مع هذه التهديدات، فالأدوات التوعوية الفعّالة حالياً لن تكون بذات الفاعلية في المستقبل القريب.

### محاور الجلسة

- السلامة الرقمية والتهديدات الناشئة.
- دور الشركات التكنولوجية في دعم جهود السلامة الرقمية.
- دور المراكز البحثية السيبرانية في تطوير أدوات السلامة الرقمية.

06



الوكالة الوطنية للأمن السيبراني  
National Cyber Security Agency



المبادرة الوطنية للسلامة الرقمية  
Digital Safety National Initiative