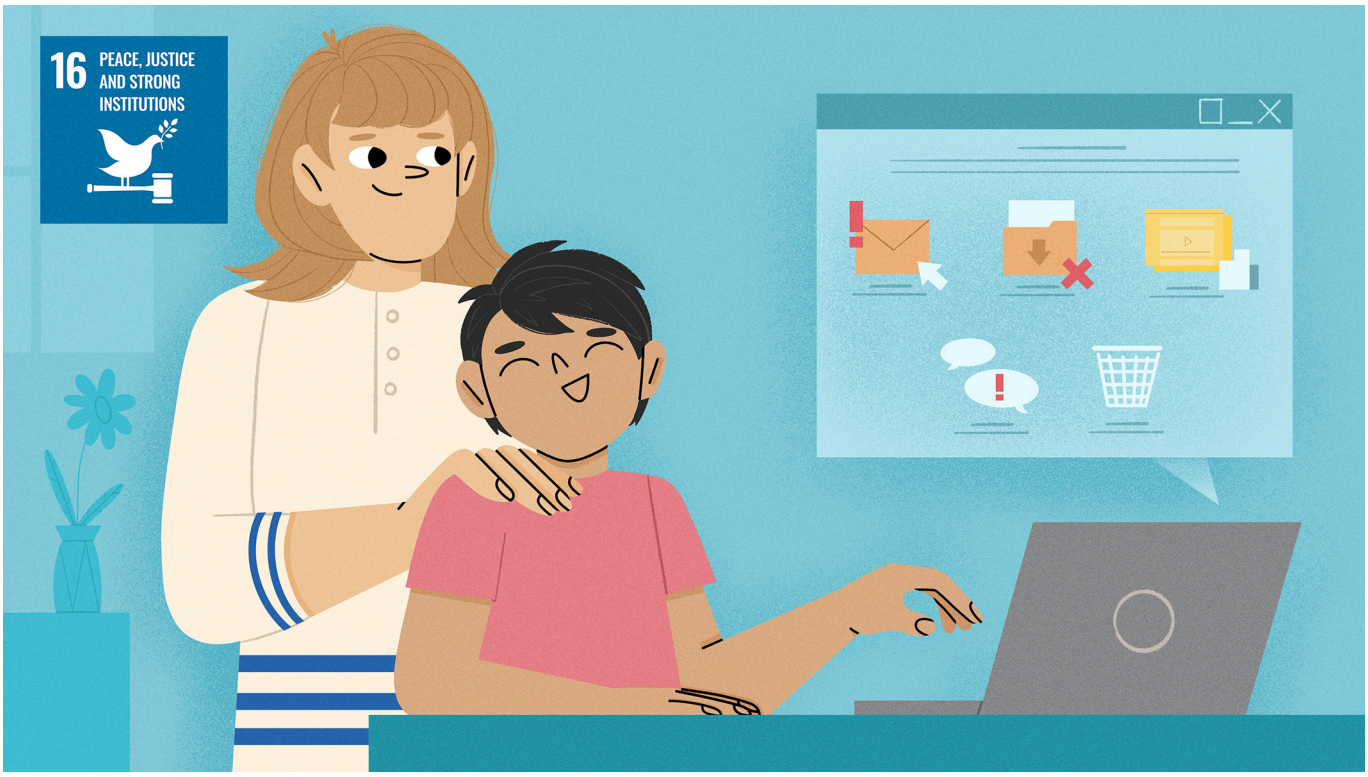
الهندسة والتكنولوجيا
نُشر على الإنترنت بتاريخ: 31 مارس 2025
doi: 10.3389/frym.2024.1396135-ar



معًا لتحقيق الهدف 16 من أهداف التنمية المستدامة: الاستخدام الآمن والمأمون للتكنولوجيات الرقمية

Taous Madi, Charalambos Konstantinou* و Paulo Esteves-Verissimo
قسم العلوم والهندسة الحاسوبية والكهربائية والحسابية، جامعة الملك عبد الله للعلوم والتقنية، ثول، المملكة العربية السعودية

ينصّ الهدف 16 من أهداف التنمية المستدامة للأمم المتحدة (وهو السلام والعدل والمؤسسات القوية) على ضمان أن نعيش جميعًا في مجتمعات آمنة وعادلة وتحمينا من الخطر. وتعني تكنولوجيا المعلومات والاتصالات تلك الأجهزة الرقمية التي نستخدمها، كما تتضمّن استخدام الخدمات الرقمية لإنجاز المهام، على سبيل المثال، استخدام أجهزة الكمبيوتر والأجهزة اللوحية بغرض العمل أو التسوق أو التعلم. ومع ذلك، قد تؤثر تهديدات متعددة على سلامتنا في عالم تكنولوجيا المعلومات والاتصالات، وسرقة المعلومات الخاصة هي أحد أنواع التهديدات. لضمان أمانك في العالم الرقمي، من المهم أن تكون على دراية بتلك المخاطر وأن تستخدم تكنولوجيا المعلومات والاتصالات بمسؤولية. هدفنا في هذه المقالة هو زيادة الوعي بالمخاطر الأمنية لتكنولوجيا المعلومات والاتصالات. سوف

المراجعون الصغار

AISYAH
العمر: 14

KATERINA
العمر: 9

SHIRHAN
العمر: 16

ZAHRAA
العمر: 16

تتعرف على جهود العلماء في الحفاظ على أمن عالمنا الرقمي وكيف يمكن حماية الجميع من تلك المخاطر.

شاهد مقابلة مع مؤلفي هذا المقال لمعرفة المزيد (الفيديو 1).

الفيديو 1 (VIDEO 1)

شاهد مقابلة مع مؤلفي هذه المقالة لمعرفة المزيد.

مخاطر التكنولوجيات الرقمية

الهدف 16 من أهداف التنمية المستدامة (16 SDG)، الذي قدمته الأمم المتحدة في عام 2015، ينصّ على توفير مجتمعات آمنة وعادلة وخالية من الخوف للناس. والأمم المتحدة هي منظمة دولية تأسست في عام 1945، وهي ملتزمة بالحفاظ على السلام والأمن، وتطوير العلاقات الودية بين الأمم، وتعزيز التقدم الاجتماعي وحقوق الإنسان وتحسين مستويات المعيشة في جميع أنحاء العالم. أهداف التنمية المستدامة هي مجموعة من 17 هدفًا عالميًا اعتمدتها الدول الأعضاء في الأمم المتحدة في عام 2015 كجزء من خطة التنمية المستدامة لعام 2030. وهي تغطي مجموعة واسعة من القضايا المترابطة مثل الفقر وانعدام المساواة وتغير المناخ والسلام. والغاية الرئيسية للهدف 16 من أهداف التنمية المستدامة هي تعزيز البيئات السلمية، حيث تُحل النزاعات والخلافات بالطرق الودية. ويؤكد هذا الهدف على أهمية القضاء على جميع أشكال العنف، وخاصة ضد الأطفال. كما يركّز الهدف 16 من أهداف التنمية المستدامة على ضمان تمتع مجموعات الناس والبلدان بحقوق متساوية وهوية محددة وحماية القانون. ومن خلال تطبيق هذه القيم المهمة بين الأفراد والمنظمات والبلدان، سيضمن الهدف 16 من أهداف التنمية المستدامة مجتمعًا سليمًا [1].

تكنولوجيا المعلومات والاتصالات (INFORMATION AND COMMUNICATION TECHNOLOGY (ICT))

جميع الأجهزة الإلكترونية التي نستخدمها، بما فيها استخدام الخدمات القائمة على الإنترنت لإنجاز مهام مختلفة.

البيئة الرقمية (DIGITAL ENVIRONMENT)

البيئة التي أُنشئت باستخدام تكنولوجيا المعلومات والاتصالات، لتسهيل الأنشطة اليومية مثل التواصل والتعاون وحجز المواعيد، وما إلى ذلك.

التنمر على الإنترنت (CYBER-BULLYING)

استخدام منصات التواصل الرقمي لتخويف الأفراد أو الجماعات أو مضايقتهم أو إلحاق الأذى بهم، وغالبًا ما يكون ذلك من خلال السلوك العدواني المتكرر أو نشر محتوى ضار.

أمن الفضاء الإلكتروني (CYBERSECURITY)

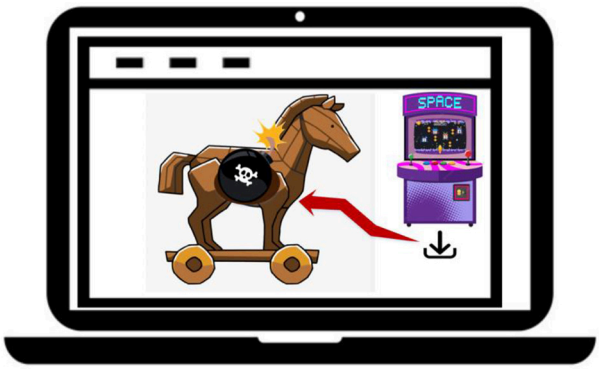
الجهد المستمر للحفاظ على أمان تكنولوجيا المعلومات والاتصالات والتصدي لسوء السلوك وإساءة الاستخدام، مثل سرقة المعلومات أو حذف الملفات.

تكنولوجيا المعلومات والاتصالات، مثل منصات التواصل الاجتماعي وتطبيقات المراسلة ومواقع التسوق عبر الإنترنت، لها دور مهم في حياتنا. فنحن نعيش الآن فيما يسمى بالبيئة الرقمية، ولكن هذه البيئة قد تكون غير آمنة في بعض الأحيان. قد يواجه مستخدمو تكنولوجيا المعلومات والاتصالات تهديدات متعددة، مثل التنمر على الإنترنت الذي يعد شكلاً من أشكال العنف، أو سرقة معلوماتهم الخاصة، مما يهدد سلامتهم. لذلك، فإن الاستخدام الحذر لتكنولوجيا المعلومات والاتصالات أمر بالغ الأهمية لتحقيق الهدف 16 من أهداف التنمية المستدامة.

المخاطر المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات

يتزايد عدد الأشخاص من جميع الأعمار الذين يستخدمون التكنولوجيا في العديد من أنواع الأنشطة. وفي العديد من المدارس، يستخدم الطلاب المواقع الإلكترونية والرسائل الإلكترونية للتعليم والتواصل. وتُستخدم تطبيقات الهاتف الجوال لأغراض تشمل الترفيه والتدريب وتتبع النشاط البدني. ويتواصل الأصدقاء على وسائل التواصل الاجتماعي لمشاركة تجاربهم، في حين يلتقي البعض على منصات الألعاب. على الرغم من أن هذه الأدوات مفيدة، إلا أنها تنطوي على العديد من مخاوف أمن الفضاء الإلكتروني والسلامة التي يجب أن تكون على علم بها كمستخدم شاب لتكنولوجيا المعلومات والاتصالات.

من منظور أمن الفضاء الإلكتروني، هناك ثلاثة مخاوف رئيسية يجب الانتباه إليها. وأولى هذه المخاوف عندما يتم الكشف عن المعلومات السرية، مثل كلمات المرور، لأشخاص آخرين. الأمر كما لو أن شخصًا غريبًا حصل بطريقة ما على نسخة من مفتاح منزلك أو يحاول استخدام هويتك للغش في الامتحان. وهذا ما يسمى بمشكلة الحفاظ على السرية. وثاني المخاوف عندما يتم تغيير المستندات والملفات، مثل تقارير الدراسة، دون موافقة المالك وعلمه. تخيّل ذلك كما لو أن أحد زملائك يفسد مشروعك الدراسي دون علمك.



شكل 1

وهذه مشكلة صحة البيانات. وثالث المخاوف عندما لم يعد بالإمكان استخدام أجهزتك على النحو المعتاد بسبب استخدامها من قِبل أشخاص غير مسموح لهم بذلك. ويُعرف هذا بمشكلة التوافر.

كيف تظهر مشاكل الأمن في الفضاء الإلكتروني هذه في حياتنا اليومية؟

المواقع الإلكترونية وصناديق البريد الإلكتروني

نحن نستخدم المواقع الإلكترونية وصناديق البريد الإلكتروني كل يوم لإنجاز المهام أو التفاعل مع بعضنا البعض أو تعلّم الأشياء. على الرغم من جاذبية بعض المواقع الإلكترونية، فإنها يمكن أن تلحق الضرر بأجهزتنا أو تعرض لنا محتوى غير لائق. على سبيل المثال، إذا نقرت على عنصر مريب ومشكوك فيه، فقد يُعاد توجيهك إلى موقع ويب آخر، ربما موقع يعرض محتوى غير مناسب. وفي حالات أخرى بعد النقر، يمكن أن يتم تنزيل برامج ضارة على جهازك. اعتمادًا على طبيعة البرامج الضارة، يمكن أن تتفاوت أنواع الضرر الناتجة عنها [2].

قد تؤدي البرامج الضارة إلى إتلاف بياناتك، على سبيل المثال عن طريق محو محتوى ملفاتك. أو قد تخلّ بمبدأ الحفاظ على السرية من خلال السماح بالوصول إلى معلومات حساسة، مثل معلومات هويتك أو عنوان منزلك أو تفاصيل حسابك البنكي. تستهدف بعض أنواع البرامج الضارة التوافر من خلال استهلاك جميع الموارد (مثل طاقة المعالجة ومساحة التخزين) الموجودة على أجهزتنا. على سبيل المثال، يُعدّ حصان طروادة من أنواع البرامج الضارة المعروفة التي يمكن أن تتيح للمخترقين

الحفاظ على السرية (CONFIDENTIALITY)

ضمان منع الوصول إلى المعلومات الحساسة أو الإفصاح غير المصرح عنها. في سياق تكنولوجيا المعلومات والاتصالات وأمن الفضاء الإلكتروني، يضمن مبدأ الحفاظ على السرية منع الوصول إلى البيانات إلا للمصرح لهم بالاطلاع عليها أو استخدامها.

شكل 1

عند النقر على رموز تنزيل معينة، قد يتم تنزيل حصان طروادة على جهازك دون أن تدرك الأمر. وبعد تنزيله، ينفذ حصان طروادة عمليات مضرّة، مثل منح المخترقين إمكانية الوصول إلى جهازك. ومصطلح حصان طروادة مستوحى من القصة الإغريقية القديمة للحصان الخشبي العملاق الذي أدى إلى سقوط مدينة طروادة. ظنّ أهل طروادة أن الحصان العملاق كان هدية، فأدخلوه من البوابات، ولكن فُتح الحصان الخشبي العملاق ليلاً وتسلل الجنود منه وغزوا المدينة.

صحة البيانات (INTEGRITY)

يعني هذا المصطلح أن تكون البيانات دقيقة وكاملة ولم تتعرّض لأي تغيير. في مجال أمن الفضاء الإلكتروني، تشير صحة البيانات إلى الحفاظ على اتساق البيانات وموثوقيتها، وضمان عدم التلاعب بها أو تعديلها بطريقة غير مصرح بها.

البرامج الضارة (MALWARE)

برنامج ضار يتم تثبيته على الأجهزة دون موافقة المستخدم. توجّه البرامج الضارة الجهاز إلى إساءة السلوك بطريقة تخلّ بالحفاظ على السرية وصحة البيانات والتوافر.

الوصول إلى أجهزتنا (الشكل 1). يمكنك تخيل هؤلاء المخترقين كلصوص إلكترونيين يحاولون أخذ أشياء لا تخصهم في البيئة الرقمية. يمكن أن تكون هذه الأشياء صورًا أو كلمات مرور أو حتى وثائق أمنية مهمة لبلد ما، في حالة اختراق جهاز موظف حكومي.

تطبيقات الهاتف الجوال

يقوم العديد من مستخدمي تكنولوجيا المعلومات والاتصالات بتنزيل التطبيقات على الهواتف الجوالة، ويحب الكثير من المستخدمين الألعاب وتطبيقات تتبع النشاط البدني. على الرغم من أن هذه التطبيقات قد تبدو آمنة، قد يحتوي بعضها على برامج ضارة، وغالبًا ما تكون على شكل أدوات نقر تلقائي.

وأداة النقر التلقائي هي برنامج ضار بسيط يحاكي تصرفات المستخدم وينقر على العديد من الأماكن في آنٍ واحد (الشكل 2). ويتسبب ذلك في استهلاك أجهزتنا للكثير من الموارد، مما يجعلها بطيئة في إنجاز المهام. يمكن لأدوات النقر التلقائي أيضًا النقر على أزرار التنزيل وتنزيل المزيد من البرامج الضارة على أجهزتنا، والتي يمكن للمخترقين استخدامها بعد ذلك للوصول إلى معلوماتنا. وللأسف، تشيع التطبيقات التي تحتوي على برامج ضارة، على سبيل المثال، من بين 56 تطبيقًا للهاتف الجوال وُجدت بها برامج ضارة، كان هناك 24 تطبيقًا منها للأطفال [3].

شكل 2

شكل 2

أداة نقر تلقائي تنقر عدة مرات بطريقة آلية. تخيّل ذلك كأخطبوط بأرجل متعددة، وجميعها تقوم بنقرات آلية بالتوازي، على سبيل المثال على الإعلانات وإعلانات البانر التي تظهر في التطبيقات.

وكل هذه التهديدات الأمنية قد تؤثر على سلامتنا في البيئة الرقمية، وتعرّض أموالنا للخطر، وتمنع وصولنا إلى الخدمات المهمة. عند تخيّل حدوث ذلك على مستوى الدولة، وكيف يمكن أن يؤثر ذلك على سلامة وصحة وخصوصية بيانات المواطنين بشكل عام، فمن السهل أن نفهم أن أمن الفضاء الإلكتروني يؤثر بشكل مباشر على مدى سلامة المجتمع وعدالته وقوته.

كيف يمكن للعلم أن يساعدنا؟

لحسن الحظ، يتعاون العديد من الأشخاص لزيادة أمان البيئة الرقمية. يسخّر الباحثون في مجال أمن الفضاء الإلكتروني جهودهم المستمرة لحماية العالم الرقمي من التهديدات، فهم يطورون طرقًا لاكتشاف البرامج الضارة وإيقافها قبل أن تتسبب في

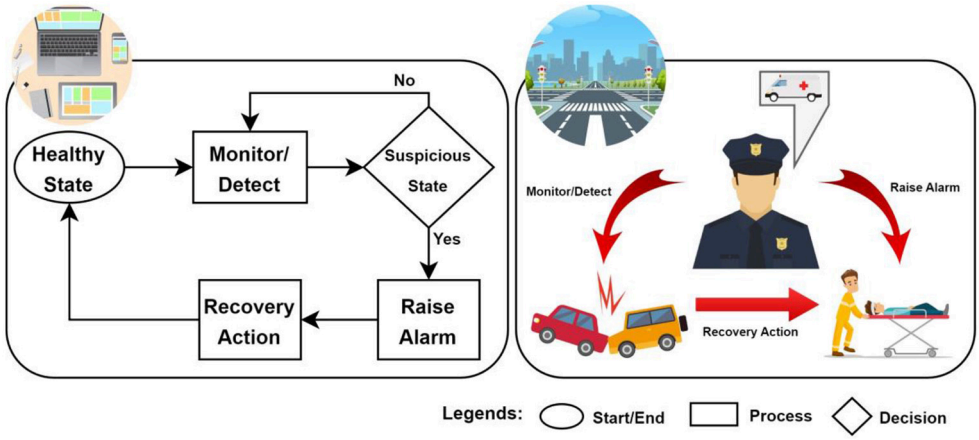
أي ضرر، كما أنهم يحاولون معرفة المسؤول عن الأفعال السيئة، مثل سرقة الهوية. لتعزيز المستوى الأمني لتكنولوجيا المعلومات والاتصالات، يعمل الباحثون أيضًا على ميزات مثل المصادقة، والتي تعني التحقق من هوية المستخدمين لإثبات هويتهم، أو التحكم في الوصول، مثل تحديد مَن يمكنه الوصول إلى موارد أو بيانات معينة.

المصادقة (AUTHENTICATION)

عملية التحقق من هوية الشخص أو الجهاز، تمامًا كإبراز بطاقة الهوية لإثبات هويتك.

وكمثال على أحد مشاريعنا البحثية، بدأنا في ابتكار برامج يمكنها منع الأضرار التي قد تلحق بأنظمة تكنولوجيا المعلومات والاتصالات حتى عند وقوع الأحداث الضارة. بعبارة أخرى، تساءلنا عما إذا كان بإمكاننا بناء برنامج يمكنه حماية الأجهزة من أي أنشطة ضارة [3, 4]. ويحتوي البرنامج على مكوّنين رئيسيين، مكوّن الكشف ومكوّن الاسترداد. تخيّل مكوّن الكشف كرجل شرطة ومكوّن الاسترداد كمنقذ سيارة إسعاف.

على غرار مهام رجل الشرطة، يراقب مكوّن الكشف باستمرار ما يحدث في الجهاز ويتحقق من حدوث أي أنشطة غير عادية، وهذا ما يسمى بالمراقبة. عندما يشتبه مكوّن الكشف في وجود خطأ ما، فإنه يطلق إنذارًا طلبًا للانتباه والتصرف الفوري. يقوم الإنذار على الفور بتشغيل مكوّن الاسترداد الذي يعمل على إصلاح أي تلف محتمل، لإعادة الجهاز إلى حالته السليمة (الشكل 3).



شكل 3

شكل 3

بطلنا الرقمي، وهو برنامج يتكون من جزأين رئيسيين: مكوّن الكشف الذي يعمل كمراقب يقظ يشبه رجل الشرطة الذي يراقب الطرق، ومكوّن الاسترداد الذي يقوم بدور منقذ سيارة الإسعاف الذي يقدم المساعدة الحاسمة في حالات الطوارئ.

الأمر كما لو أن رجل شرطة يتصّل بسيارة إسعاف بعد وقوع حادث. يقوم المنقذ في سيارة الإسعاف بجمع المعلومات المهمة من رجل الشرطة ويحاول فهم الأضرار وإنقاذ المصابين. من خلال اختبار برنامجنا في مواجهة تهديدات قمنا بمحاكاتها، وجدنا أنه نجح في اكتشاف التهديدات واستطاع إصلاح الضرر الذي تسبب به الهجوم الوهمي. باختصار، قمنا ببناء بطل رقمي لحماية بيئتنا الرقمية.

الاستمتاع بتجربة آمنة ومأمونة أثناء استخدام أجهزتنا

تنفذ العديد من المؤسسات خططًا لمساعدة الناس على استخدام تكنولوجيا المعلومات والاتصالات بأمان. على سبيل المثال، يقدم الاتحاد الدولي للاتصالات (وكالة الأمم

المتحدة المتخصصة في التكنولوجيا الرقمية) سلسلة من المبادئ التوجيهية حول كيفية تقليل المخاطر وحماية الأطفال أثناء استخدام تكنولوجيا المعلومات والاتصالات [5]. في الولايات المتحدة الأمريكية، وُضع قانون حماية خصوصية الأطفال على الإنترنت (COPPA) لحماية الأطفال الذين يستخدمون تكنولوجيا المعلومات والاتصالات. بموجب هذا القانون، يُحظر على المواقع الإلكترونية الحصول على المعلومات الشخصية للأطفال دون موافقة أولياء أمورهم [6].

لكي تحافظ على سلامتك أثناء الاستمتاع بعالم تكنولوجيا المعلومات والاتصالات، يجب أن تكون على دراية بالمخاطر وأن تحسن التصرّف. كن حذرًا عند الدخول إلى المواقع الإلكترونية وصناديق البريد الإلكتروني واستخدامها، وادخل فقط إلى المواقع المقترحة والمعتمدة من قبل المعلمين/ أولياء الأمور، ولا تقم بتنزيل ملفات من مرسلين غير معروفين، وقلل من عدد التطبيقات التي يتم تنزيلها على أجهزتك، وأخيرًا، أخبر المعلمين/ أولياء الأمور بأي سلوكيات غير طبيعية أو مسيئة، مثل التنمر على الإنترنت أو رسائل الكراهية.

الخاتمة

يمكن استخدام تكنولوجيا المعلومات والاتصالات لأغراض التعلم والعمل والترفيه. ومع ذلك، يمكن أن تتسبب هذه التكنولوجيات أيضًا في تهديدات تعرّض سلامة الجميع للخطر. في هذه المقالة، تحدثنا عن أمثلة لتلك التهديدات ولخصنا بعض الطرق التي يتبعها مجتمع الأبحاث ومؤسساته لجعل تكنولوجيا المعلومات والاتصالات أكثر أمانًا وسلامة. كما قدمنا بعض النصائح الاحترازية الأساسية التي يمكنك اتباعها لاستخدام تكنولوجيا المعلومات والاتصالات دون خوف. من خلال ضمان استخدام الجميع لتكنولوجيا المعلومات والاتصالات بأمان، يمكننا أن نحافظ على حماية الجميع وأن نضمن لهم حياة أكثر أمانًا وسعادة، في بلدان قوية وموثوق بها تمامًا حسب رؤية الهدف 16 من أهداف التنمية المستدامة. نأمل أن تصبح أكثر وعيًا بأمن الفضاء الإلكتروني وتشاركنا جهودنا للحفاظ على أمن مجتمعاتنا.

شكر وتقدير

نودّ أن نشكر نيكي تالبوت في جامعة الملك عبد الله للعلوم والتقنية على دعمها الثمين لنا خلال عملية المراجعة، والذي لولاه لما اكتملت هذه المجموعة. كما نود أن نعرب عن امتناننا لمكتب الاستدامة والمكتب القُطري لبرنامج الأمم المتحدة الإنمائي في المملكة العربية السعودية لتفانيهم في رفع مستوى الوعي بأهمية أهداف التنمية المستدامة للأمم المتحدة في رحلتنا نحو عالم أكثر استدامة.

المراجع

1. United Nations 2015. *Transforming Our World: The 2030 Agenda for Sustainable Development*. Available at: https://www.un.org/sustainabledevelopment/development-agenda/
2. Blancaflor, E., Beltran, S. S., Jayag, J. E., Obog, A., Salem, F. E., and Sungahid, M. D. 2022. ''A security assessment on malwares disguised as children's applications'', *2022 7th International Conference on Multimedia communication Technologies (ICMCT)* (Xiamen, China). p. 15–19. doi: 10.1109/ICMCT57031.2022.00012
3. Madi, T., and Esteves-Verissimo, P. 2022. ''A fault and intrusion tolerance framework for containerized environments: a specification-based error detection approach'', *2022 International Workshop on Secure and Reliable Microservices and Containers (SRMC)* (IEEE).
4. Konstantinou, C., Wang, X., Krishnamurthy, P., Khorrami, F., Maniatakos, M., and Karri, R. 2022. HPC-based malware detectors actually work: transition to practice after a decade of research. *IEEE Des. Test.* 39:23–32. doi: 10.1109/MDAT.2022.3143438
5. International Telecommunication Union n.d. *Child Online Protection Guidelines*. Available at: https://www.itu-cop-guidelines.com/
6. Children's Online Privacy Protection Act 1998. 15 U.S.C. §§ 6501–6506. Available at: https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act

نُشر على الإنترنت بتاريخ: 31 مارس 2025

المحرر: Rúben Martins Costa

مرشدو العلوم: Emma Louise Nason

الاقتباس: Esteves-Verissimo P و Madi T, Konstantinou C (2025) معًا لتحقيق الهدف 16 من أهداف التنمية المستدامة: الاستخدام الآمن والمأمون للتكنولوجيات الرقمية. Front. Young Minds. doi: 10.3389/frym.2024.1396135-ar

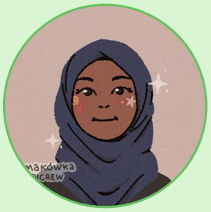
مُترجَم ومقتبس من: Madi T, Konstantinou C and Esteves-Verissimo P (2024) Towards SDG 16: Safe and Secure Use of Digital Technologies. Front. Young Minds 12:1396135. doi: 10.3389/frym.2024.1396135

إقرار تضارب المصالح: يعلن المؤلفون أن البحث قد أُجري في غياب أي علاقات تجارية أو مالية يمكن تفسيرها على أنها تضارب محتمل في المصالح.

المراجعون الصغار

AISYAH، العمر: 14
أحب العلوم بعض الشيء، ولكن الدراسات الاجتماعية هي مادتي المفضلة. في الأوقات التي لا أدرس فيها، أشغل نفسي بالطهي أو لعب الريشة الطائرة أو الانهماك في دورة برمجة.

KATERINA، العمر: 9
أحب الحيوانات والنباتات، ولديّ فضول كبير لاستكشاف العالم الذي أعيش فيه وتعلم المزيد عن العلوم. وهواياتي هي الجمباز والسباحة والذهاب إلى المدرسة، وكذلك الموسيقى والفن والرياضيات.



SHIRHAN، العمر: 16
مادتي المفضلة في المدرسة هي العلوم، ومن العلوم التي أهتم بها حقًا علوم الأرض والنبات، ولكن علم الفلك لطالما أبهرني. في الأوقات التي لا أهتم فيها بالعلوم المختلفة، أستمتع بالقراءة والكتابة الإبداعية. لقد كان من دواعي سروري أن أعمل مع العديد من الأشخاص في مشروع Frontiers for Young Minds.

ZAHRAA، العمر: 16
أنا طالبة متفانية ومهتمة بالعلوم والرياضيات وتطبيقاتهما في حياتنا اليومية. استمتعتُ بالانضمام إلى برنامج Frontiers for Young Minds وتنمية معرفتي بأمور مثل أمن الفضاء الإلكتروني والعالم من حولنا.

المؤلفون

TAOUS MADI
تعمل Taous Madi حاليًا باحثة متمرسة في شركة إريكسون، كندا. وشغلت سابقًا منصب عالمة أبحاث في مركز الحوسبة المرنة والأمن السيبراني (RC3) في جامعة الملك عبد الله للعلوم والتقنية. وهي حاصلة على درجة الدكتوراة في هندسة نظم المعلومات من جامعة كونكورديا

في مونتريال. تشمل اهتماماتها البحثية الأمن في شبكات الجيل الخامس وما بعد شبكات الاتصالات، وتعلم الآلة، والتحقق الشكلي. شاركت في تأليف كتاب والعديد من مقالات المجلات ووقائع المؤتمرات لجهات مرموقة متخصصة في مجال أمن الفضاء الإلكتروني.

CHARALAMBOS KONSTANTINOU

يعمل Charalambos (Harrys) Konstantinou حاليًا أستاذًا مشاركًا في قسم العلوم والهندسة الحاسوبية والكهربائية والحسابية في جامعة الملك عبد الله للعلوم والتقنية بالمملكة العربية السعودية. وهو الباحث الرئيسي في المجموعة البحثية "مختبر الأنظمة الصامدة الآمنة للجيل القادم" (مختبر SENTRY). حصل على درجة الماجستير في الهندسة الكهربائية والحاسوبية من الجامعة التقنية الوطنية في أثينا باليونان، ودرجة الدكتوراة في الهندسة الكهربائية من جامعة نيويورك في الولايات المتحدة الأمريكية. وقبل انضمامه إلى جامعة الملك عبد الله للعلوم والتقنية، عمل أستاذًا مساعدًا في مركز أنظمة الطاقة المتقدمة في جامعة ولاية فلوريدا. تشمل اهتماماته البحثية أمن البنى التحتية الحيوية وصمودها مع التركيز بشكل خاص على تكنولوجيات الشبكات الذكية، وتكامل الطاقة المتجددة، والمحاكاة في الوقت الحقيقي. *charalambos.konstantinou@kaust.edu.sa

PAULO ESTEVES-VERISSIMO

يعمل Paulo Esteves-Veríssimo أستاذًا في جامعة الملك عبد الله للعلوم والتقنية ومديرًا لمركز أبحاث الأمن السيبراني والحوسبة الصامدة. وهو أيضًا زميل باحث في المركز متعدد التخصصات للأمن والموثوقية والثقة (SnT) في جامعة لوكسمبورج (LU) وأستاذ مساعد في قسم الهندسة الكهربائية والحاسوبية في جامعة كارنيغي ميلون (الولايات المتحدة)، كما أنه زميل في معهد مهندسي الكهرباء والإلكترونيات (IEEE)، وزميل في جمعية آلات الحوسبة (ACM)، وله أكثر من 200 منشور تمت مراجعته من قبل الأقران، وشارك في تأليف 5 كتب. وهو مهتم حاليًا بالحوسبة الصامدة في مجالات مثل: البنى التحتية القائمة على الشبكات المعرّفة بالبرامج (SDN)، أو المركبات ذاتية القيادة، أو أنظمة التحكم الموزعة، أو الصحة الرقمية وعلم الجينوم، أو سلسلة الكتل والعملات المشفّرة.

النسخة العربية مقدمة من
Arabic version provided by

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology