Jan 2 AR

Summary

**اعتماد الاستراتيجية الوطنية للأمن السيبراني**

Option 1

تأكيداً على التزام دولة الإمارات بحماية بنيتها التحتية الرقمية وتعزيز مكانتها العالمية، اعتمد مجلس الوزراء برئاسة صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي "رعاه الله"، الاستراتيجية الوطنية للأمن السيبراني. تهدف الاستراتيجية إلى ترسيخ بيئة رقمية آمنة ومرنة عبر خمس ركائز رئيسية وهي الحوكمة والحماية، والابتكار، والمرونة، والشراكة. وأكد الدكتور محمد الكويتي، رئيس الأمن السيبراني، أنها تمثل خطوة مفصلية لحماية التحول الرقمي وتعزيز جاهزية الدولة للتحديات. كما تسهم في رفع كفاءة الكوادر الوطنية وتعزيز التعاون المحلي والدولي. وتعكس الاستراتيجية تطلعات "رؤية 2031" و"مئوية 2071".

Option 2

ترأس صاحب السمو الشيخ محمد بن راشد آل مكتوم اجتماع مجلس الوزراء في قصر الوطن، حيث تم اعتماد الاستراتيجية الوطنية للأمن السيبراني، تأكيداً على التزام الدولة بحماية بنيتها التحتية الرقمية. وبيّن سموه أهمية الأمن السيبراني في الحفاظ على مكتسبات الإمارات الرقمية، مشيراً إلى تصدّر الدولة للمؤشر العالمي للأمن السيبراني 2024. وتشكل الاستراتيجية خارطة طريق شاملة تقوم على الحوكمة، الابتكار، المرونة، الحماية، والشراكة، وتهدف إلى بناء بيئة رقمية آمنة ومرنة. ودعا المجلس إلى توحيد الجهود لتحقيق رؤية الإمارات كدولة رائدة رقمياً، بما ينسجم مع "رؤية 2031" و"مئوية 2071" لبناء اقتصاد معرفي ومستقبل رقمي مزدهر.

audience

الحكومة

Jan 2 EN

**Summary**

**Adoption of the National Cybersecurity Strategy**

The UAE Cabinet approved the National Cybersecurity Strategy, reinforcing the country’s commitment to protecting its digital infrastructure. The strategy is built on five pillars: governance, protection, innovation, capacity building, and partnership. It aims to equip citizens and institutions to address cyber threats through advanced technologies, robust legal frameworks, and strategic collaborations at home and abroad. His Excellency Dr. Mohamed Al Kuwaiti noted that the strategy strengthens the UAE’s position as a global digital hub. The initiative aligns with UAE Centennial 2071 and the “We the UAE 2031” vision for a sustainable, knowledge-based economy.

-Government

Jan 16 AR

**Summary**

**مجلس الأمن السيبراني ينجح في التصدي لهجمات برمجيات الفدية وتهديداتها**

مجلس الأمن السيبراني في الإمارات يُعلن عن نجاح المنظومات الوطنية في التصدي لهجمات "الفدية" الإلكترونية التي استهدفت قطاعات حكومية وخاصة بهدف تسريب البيانات وتعطيل الأنظمة. تم رصد نحو 200 ألف هجمة يومياً وتحديد هوية المخترقين ومواقعهم، بفضل تقنيات الرصد المتقدمة. ولفت المجلس إلى تصاعد استخدام تقنيات الذكاء الاصطناعي في الهجمات، مما يجعل اكتشافها أكثر صعوبة. وشدد على أهمية التزام الجهات بمعايير الأمن السيبراني لتفادي الأضرار، محذراً من الرسائل والروابط المشبوهة. وأكد الدكتور محمد الكويتي، رئيس الأمن السيبراني، أن الإمارات تمتلك بنية تحتية رقمية متطورة قادرة على التصدي لتلك التهديدات بكفاءة ومرونة عالية.

الحكومة

Jan 16 EN

**Cyber Security Council Announces Successful Countering of Ransomware Attacks and Threats**

EN

The UAE Cyber Security Council announced that national cybersecurity systems successfully thwarted malicious ransomware attacks targeting several strategic sectors in both public and private entities. The attacks aimed to breach data and lock digital systems. Approximately 200,000 cyberattacks were detected daily. The hacker’s identity and location were identified through advanced monitoring. The Council noted an increase in the use of sophisticated AI-powered tools in these cyberattacks, complicating detection. The Council emphasized the importance of complying with cybersecurity standards to prevent potential damage and issued warnings about suspicious messages and links. Dr. Mohamed Al Kuwaiti assured that the UAE's advanced digital infrastructure is well-equipped to detect and mitigate cyber threats with high efficiency and speed.

-Government

Feb 4 AR

أطلق مجلس الأمن السيبراني لدولة الإمارات حملة توعوية تهدف إلى تعزيز الوعي بالأمن السيبراني بين الأسر والمجتمع بشكل عام. تُقدَّم هذه الحملة من خلال جلسات توعوية في مجالس أبوظبي، بقيادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة الإمارات، وتركّز المبادرة على حماية الأطفال من التهديدات الرقمية مثل الاستدراج، والابتزاز، والتنمر الإلكتروني، والاحتيال، والإدمان الرقمي. كما تهدف الحملة إلى تزويد أولياء الأمور (أو الآباء والأمهات ) بالمعرفة العملية للتعامل مع هذه المخاطر بمسؤولية، وتعزيز أفضل الممارسات لحماية البيانات الشخصية، وتسليط الضوء على الدور المحوري الذي تؤديه الأسرة في ترسيخ ثقافة الاستخدام الآمن والمسؤول للتقنية.

الأفراد والعائلات

الشركات

Feb 4 EN

**Summary**

**EN**

The UAE Cyber Security Councillaunches a campaign aimed at strengthening cybersecurity awareness among families and the broader community. Delivered through educational sessions at Abu Dhabi majlis gatherings and led by Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, the initiative focuses on protecting children from online threats such as enticement, blackmail, cyberbullying, fraud, and digital addiction. The campaign equips parents with practical knowledge to navigate these risks responsibly, promotes best practices for safeguarding personal data, and emphasizes the role families play in fostering a culture of safe and responsible technology use.

-Individuals & Families

-Government

Feb 10 AR

نظم مجلس الأمن السيبراني لحكومة الإمارات، بالتعاون مع مجالس أبوظبي بمكتب شؤون المواطنين والمجتمع بديوان الرئاسة، جلسة توعوية بعنوان "الإدمان السيبراني عند الأسرة". أقيمت الجلسة في مجلسي الصاروج والفوعة بمدينة العين، بحضور عدد كبير من المواطنين والمتخصصين في مجالي الأمن السيبراني والتربية.

تأتي هذه المبادرة ضمن حملة توعوية مجتمعية أطلقها المجلس بالتعاون مع مجالس أبوظبي، وذلك تماشيًا مع إعلان القيادة الرشيدة عام 2025 عامًا للمجتمع، بهدف تعزيز الوعي بالقضايا الوطنية والتعريف بالمخاطر الناجمة عن التطورات التكنولوجية المتسارعة.

الأفراد والعائلات

Feb 10 EN

**Summary**

**EN**

As part of the Year of the Community 2025, the UAE Cyber Security Council, in collaboration with Majalis Abu Dhabi, organized an awareness session on “Cyber Addiction in Families” at Al Sarouj and Al Foa’a Majalis in Al Ain. H.E. Dr. Mohamed Al Kuwaiti highlighted the psychological and physical risks of gaming addiction and warned of extremist groups exploiting online games to recruit youth. The session emphasized the crucial role of families in protecting children through clear rules, cultural values, content monitoring, and open communication. This initiative reinforces the UAE’s commitment to cybersecurity awareness and community readiness.

-Individuals & Families

Feb 11 AR

**AR**

في القمة العالمية للحكومات 2025، شارك مجلس الأمن السيبراني لدولة الإمارات، بالتعاون مع مركز المسرّعات الحكومية، في جلسة "حوارات المسرّعات العالمية: تسريع الطموحات نحو الاستعداد للمستقبل". جمعت الجلسة أكثر من 60 من القادة العالميين وصنّاع السياسات ورواد الأعمال الشباب، لمناقشة جاهزية الحكومات واستكشاف حلول مبتكرة لمواجهة تحديات المستقبل. وقد تعاون المشاركون على وضع خارطة طريق استراتيجية تُحوّل الطموحات إلى نتائج قابلة للتنفيذ. وشدّد الحوار على أهمية المرونة والابتكار والتعاون بين مختلف القطاعات لبناء حكومات قادرة على مواكبة التحولات العالمية المتسارعة وضمان الازدهار طويل الأمد للأجيال القادمة.

الحكومة

Feb 11 EN

**Summary**

**EN**

At the World Governments Summit 2025, the UAE Cyber Security Council, in collaboration with the Government Accelerators Center, participated in the “Global Accelerators Dialogues: Accelerating Ambitions for Future Readiness.” The session brought together over 60 global leaders, policymakers, and youth entrepreneurs to explore government readiness and design innovative solutions for future challenges. Participants collaborated to create a strategic roadmap translating ambitions into actionable outcomes. The dialogue emphasized the necessity of agility, innovation, and cross-sector cooperation to build resilient governments capable of navigating rapid global transformations and securing long-term prosperity for future generations.

-Government

Feb 18 AR

**Summary**

**AR**

في إطار معرض ومؤتمر آيدكس 2025، وقّع مجلس التوازن، ومجلس الأمن السيبراني لحكومة دولة الإمارات، وشركة "لوكهيد مارتن" خطاب نوايا لإنشاء مركز للتميز في مجال الأمن السيبراني. تهدف المبادرة إلى تعزيز الأمن الرقمي، وتطوير الكفاءات الوطنية، ودعم الابتكار. يأتي المشروع ضمن برنامج التوازن الاقتصادي ويعكس التزام الإمارات ببناء بيئة سيبرانية آمنة. سيركّز المركز على الأبحاث، التدريب، مراكز العمليات الأمنية، ودعم رواد الأعمال المحليين، خصوصًا في القطاعات الحيوية كالدفاع. كما ستعزز الشراكة نقل المعرفة، وتمكين الكفاءات الإماراتية، وترسيخ مكانة الدولة عالميًا في مجال الأمن السيبراني، بما ينسجم مع الاستراتيجية الوطنية وعام المجتمع 2025.

الحكومة

Feb 18 EN

EN

At IDEX 2025, Tawazun Council, the UAE Cyber Security Council, and Lockheed Martin signed a Letter of Intent (Lol) to establish a Cybersecurity Center of Excellence to boost digital security, develop local expertise, and foster innovation. The initiative, enabled by the Tawazun Economic Program, reflects the UAE’s commitment to building a secure cyber environment. The center will focus on advanced research, specialized training, Security Operations Center (SOC) services. It will also support local entrepreneurs, particularly in the defense sector. The partnership will also enhance knowledge transfer, empower Emirati talent, and strengthen the UAE’s global standing in cybersecurity, in line with the National Strategy and the Year of the Community 2025.

-Government

Feb 20 AR

**Summary**

**AR**

تماشيا مع عام المجتمع 2025، أطلق مجلس الأمن السيبراني حملته السنوية للتوعية بالأمن السيبراني، بمحاضرة ألقاها سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني في دولة الإمارات العربية المتحدة، في مجلس ابن لوتيه بمدينة العين، برعاية سمو الشيخ ذياب بن محمد بن زايد آل نهيان. وركّزت المحاضرة على أهمية دور المجتمع في مواجهة التهديدات السيبرانية، خاصة تجاه الأطفال والمراهقين، وأهمية وعي الأسر بأفضل ممارسات الحماية الرقمية. كما شدّد الدكتور الكويتي على أن الوعي السيبراني مسؤولية جماعية تتطلب تضافر جهود الأفراد والمؤسسات. واختُتمت الفعالية بنقاش مع الحضور، وسط إشادة بجهود المجلس في تعزيز الأمن السيبراني في دولة الإمارات.

الأفراد والعائلات

Feb 20

In line with the Year of Community 2025, the UAE Cyber Security Council launched its annual Cybersecurity Awareness Campaign with a lecture delivered by His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, at Ibn Lootah Majlis in Al Ain, under the patronage of His Highness Sheikh Theyab bin Mohamed bin Zayed Al Nahyan. The lecture focused on the vital role of the community in addressing cyber threats, particularly those targeting children and teenagers, and on the importance of families being aware of best practices for digital protection. Dr. Al Kuwaiti underscored that cybersecurity is a shared responsibility that requires the collaborative efforts of both individuals and institutions. The event concluded with an interactive discussion with attendees, who commended the Council’s efforts to advance cybersecurity in the UAE.

* Individuals & Families

Mar 3 EN

The UAE Cyber Security Council participates in the Global Crisis and Emergency Management Summit 2025, held April 8–9 under the theme “Together Towards Building Global Resilience.” Hosted under the patronage of His Highness Sheikh Tahnoun bin Zayed Al Nahyan, the summit gathers key UAE government and private entities to strengthen global crisis response. Dr. Mohamed Al Kuwaiti emphasizes the importance of international cooperation and advanced technology, including AI, to tackle growing cyber threats causing trillions in losses worldwide. The summit features strategic discussions, cooperation agreements, and exhibitions focused on crisis management and preparedness.

-Government

Mar 3 AR

يشارك مجلس الأمن السيبراني لدولة الإمارات في القمة العالمية لإدارة الطوارئ والأزمات 2025، التي تُعقد من 8 إلى 9 أبريل تحت شعار "معاً نحو بناء مرونة عالمية". وتُقام القمة برعاية سمو الشيخ طحنون بن زايد آل نهيان، وتجمع نخبة من الجهات الحكومية والخاصة في دولة الإمارات بهدف تعزيز الاستجابة العالمية للأزمات. ويؤكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، أهمية التعاون الدولي وتوظيف التقنيات المتقدمة، بما في ذلك الذكاء الاصطناعي، لمواجهة التهديدات السيبرانية المتزايدة التي تتسبب بخسائر تُقدّر بتريليونات الدولارات سنوياً. وتشهد القمة مناقشات استراتيجية، وتوقيع اتفاقيات تعاون، إلى جانب معارض متخصصة في إدارة الأزمات والاستعداد للطوارئ.

الحكومة

Mar 28 AR

يشارك مجلس الأمن السيبراني في القمة العالمية لإدارة الطوارئ والأزمات 2025، التي تُعقد في أبوظبي من 8 إلى 9 أبريل، تحت رعاية سمو الشيخ طحنون بن زايد آل نهيان، نائب حاكم إمارة أبوظبي، مستشار الأمن الوطني، وبمشاركة هي الأكبر في تاريخ القمة. وتنظَّم القمة بمشاركة واسعة من الجهات الحكومية والخاصة، وتُعد من أبرز المبادرات الإقليمية والعالمية في مجال تعزيز منظومة الاستجابة للأزمات. وتسلّط القمة الضوء على التحديات المتزايدة، لاسيما التهديدات السيبرانية، في ظل تنامي استخدام الذكاء الاصطناعي والتقنيات المتقدمة. وأكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات العربية المتحدة، أهمية توحيد الجهود الدولية، وتطوير استراتيجيات استباقية لضمان جاهزية شاملة وفعالة في مواجهة الأزمات المستقبلية.

الحكومة

​​

Mar 28 EN

The Cyber Security Council is participating in the Global Crisis and Emergency Management Summit 2025, held in Abu Dhabi from April 8 to 9 under the patronage of His Highness Sheikh Tahnoun bin Zayed Al Nahyan, Deputy Ruler of Abu Dhabi and National Security Advisor. This year’s summit features the largest global participation in its history and is organized by the National Emergency Crisis and Disaster Management Authority (NCEMA) with broad government and private sector involvement. The summit highlights growing challenges, especially cyber threats amid rising AI and advanced technologies. His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, stresses the importance of unifying international efforts and developing proactive strategies for a coordinated, effective response to future crises.

-Government

April 3/4 AR

شارك مجلس الأمن السيبراني، برئاسة سعادة الدكتور محمد الكويتي، في القمة العالمية للثورة الصناعية والذكاء الاصطناعي في أفريقيا، التي انعقدت في رواندا يومي 3 و4 أبريل 2025، تأكيدًا على التزام دولة الإمارات بدعم الابتكار وبناء مستقبل رقمي مستدام. شهدت القمة حضور أكثر من 1000 مشارك من 95 دولة، وتم خلالها عرض الفرص الاستثمارية في مجال الذكاء الاصطناعي بدولة الإمارات، وبحث إشراك شركات إماراتية رائدة مثل G42 وCPX. كما التقى الدكتور الكويتي بعدد من المسؤولين لبحث سبل التعاون في مجالات الأمن السيبراني، والتحول الرقمي، مؤكدًا أهمية الشراكات الدولية لمواجهة التحديات المستقبلية.

الشركات

الحكومة

Apr 3/4 EN

The Cyber Security Council, led by His Excellency Dr. Mohammed Al Kuwaiti, participated in the Global Summit on the Fourth Industrial Revolution and Artificial Intelligence in Africa, held in Kigali, Rwanda, on April 3–4, 2025. The participation reflects the UAE’s commitment to supporting innovation and building a sustainable digital future. The summit gathered over 1,000 participants from 95 countries and showcased AI investment opportunities in the UAE , highlighting Emirati companies such as G42 and CPX. Dr. Al Kuwaiti met with key officials to discuss cooperation in cybersecurity and digital transformation, emphasizing the importance of international partnerships to address future challenges.

-Corporations

-Government

April 10 AR

أعلن مجلس الأمن السيبراني لدولة الإمارات عن إطلاق أول برنامج وطني لجوائز التميز في الأمن السيبراني، في خطوة تهدف إلى تعزيز الابتكار والريادة في هذا المجال الحيوي، وتحفيز الأفراد والمؤسسات على تقديم حلول رقمية متقدمة لمواجهة التهديدات السيبرانية. ويكرّم البرنامج الممارسات المتميزة والنماذج المبتكرة، ويعكس التزام الدولة بتطوير الكفاءات الوطنية ودعم الاقتصاد الرقمي المستدام. وتتماشى هذه المبادرة مع رؤية الإمارات الأوسع الرامية إلى تشجيع الإجراءات الاستباقية للتخفيف من المخاطر السيبرانية، تسليط الضوء على الابتكارات الرائدة وقصص النجاح وتعزيز ثقافة الوعي والمرونة والتعاون بين مختلف القطاعات. يقام حفل توزيع الجوائز في 18 يونيو 2025، وسيتم الإعلان لاحقاً عن تفاصيل الفئات ومعايير الترشح.

الأفراد والعائلات

المؤسسات

الحكومة

April 10 EN

The Cyber Security Council announces the launch of the first National Cybersecurity Awards & Recognition Programme, aiming to foster innovation and leadership in this vital field. The program encourages individuals and organizations to develop advanced digital solutions to combat cyber threats. It honors outstanding practices and pioneering models, reflecting the UAE’s commitment to developing national competencies and supporting a sustainable digital economy. This initiative aligns with the broader UAE vision to promote proactive cybersecurity risk mitigation, highlight leading innovations and success stories, and strengthen a culture of awareness, resilience, and collaboration across all sectors. The awards ceremony will be held June 18, 2025, with details on categories and nomination criteria to be announced soon.

* Individuals & Families
* Corporations
* Government

April 10 (2) AR

أعلنت دولة الإمارات، بالتعاون مع شركة جوجل كلاود، عن إطلاق مركز عالمي للتميز في الأمن السيبراني في أبوظبي، في خطوة استراتيجية تهدف إلى ترسيخ مكانتها كمركز عالمي للتكنولوجيا والأمن الرقمي. يُشرف على المشروع مجلس الأمن السيبراني، ويهدف إلى تعزيز قدرات الدولة في مواجهة التهديدات السيبرانية، وتجسيد رؤية القيادة الرشيدة في تعزيز الابتكار وبناء مستقبل رقمي آمن ومزدهر.ويتضمن المركز أول أكاديمية متخصصة، ويوفر برامج تدريبية بالتعاون مع شركة Mandiant لتأهيل الكفاءات الوطنية. من المتوقع أن يسهم المركز في خلق أكثر من 20,300 فرصة عمل في قطاع الأمن السيبراني، واستقطاب استثمارات بقيمة 1.4 مليار دولار. وتعكس هذه المبادرة حرص الدولة على مواكبة التطورات التكنولوجية المتسارعة، والالتزام ببناء منظومة رقمية آمنة ومتقدمة تواكب التطورات العالمية وتوفر بيئة موثوقة للأعمال والمؤسسات في مختلف القطاعات.

الحكومة

April 10 (2) EN

The UAE, in partnership with Google Cloud, announces the launch of a global Cybersecurity Center of Excellence in Abu Dhabi, marking a strategic step to establish the UAE as a global hub for technology and digital security. Overseen by the Cyber Security Council, the Center aims to strengthen national capabilities in addressing cyber threats and embodies the visionary leadership’s commitment to fostering innovation and building a secure, prosperous digital future. The center will feature the region’s first specialized cybersecurity academy and deliver training programs in collaboration with Mandiant to develop national talent. The initiative is expected to create over 20,300 cybersecurity jobs and attract $1.4 billion in investments. This project reflects the UAE’s dedication to keeping pace with rapid technological advancements and building a trusted digital ecosystem that supports business across all sectors.

-Government

Apr 11 EN

The UAE Cyber Security Council participated in the Google Cloud Next 2025 summit in Las Vegas. During the event, the Council announced the launch of a Global Cybersecurity Center of Excellence in Abu Dhabi, in collaboration with Google, aligning with the UAE 2031 Vision. This initiative reinforces the UAE’s leadership in digital transformation, cybersecurity, and artificial intelligence. The Center will host Google’s first regional cybersecurity academy, offer advanced training programs and support startups. It is projected to create over 20,000 specialized jobs and attract $1.4 billion in direct foreign investment, delivering significant economic and social benefits while advancing the UAE’s secure digital ecosystem.

-Corporations

-Government

April 11 AR

شارك مجلس الأمن السيبراني لدولة الإمارات في قمة "جوجل كلاود نيكست 2025" التي أقيمت في لاس فيغاس. وخلال الحدث، أعلن المجلس عن إطلاق مركز عالمي للتميز في الأمن السيبراني في أبوظبي، بالتعاون مع شركة جوجل، وذلك انسجاماً مع رؤية الإمارات 2031. وتأتي هذه المبادرة لتعزيز ريادة الدولة في مجالات التحول الرقمي والأمن السيبراني والذكاء الاصطناعي. وسيضم المركز أول أكاديمية إقليمية للأمن السيبراني تابعة لجوجل، كما سيقدم برامج تدريبية متقدمة ويدعم الشركات الناشئة. ومن المتوقع أن يسهم المركز في توفير أكثر من 20,000 وظيفة متخصصة واستقطاب استثمارات أجنبية مباشرة بقيمة 1.4 مليار دولار، محققاً فوائد اقتصادية واجتماعية كبيرة، وداعماً لمنظومة رقمية آمنة ومستدامة في الدولة.

الشركات

الحكومة

Apr 19 EN

During his Washington visit, H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, underscores the importance of international partnerships in strengthening digital security. Hosted by the UAE–U.S. Business Council and the U.S. Chamber of Commerce, discussions focus on rapid technological transformation, emerging cyber threats, and preparations for the upcoming GISEC Global conference in Dubai. The dialogue highlights the UAE’s efforts to build a trusted business ecosystem, promote public-private collaboration, and deepen cooperation between research institutions. This visit advances UAE–U.S. strategic cooperation to enhance cybersecurity capabilities, foster innovation, and support sustainable development through advanced technologies.

-Government

Apr 19 AR

خلال زيارته إلى واشنطن، أكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات على أهمية الشراكات الدولية في تعزيز الأمن الرقمي. واستضاف المجلس الإماراتي - الأميركي للأعمال وغرفة التجارة الأميركية جلسات حوار تناولت التحول التكنولوجي السريع، والتهديدات السيبرانية الناشئة، والاستعدادات لمؤتمر جيسيك جلوبل المرتقب في دبي. وسلطت المناقشات الضوء على جهود دولة الإمارات في بناء بيئة أعمال موثوقة، وتعزيز التعاون بين القطاعين العام والخاص، وتوسيع آفاق التعاون مع المؤسسات البحثية. وتأتي هذه الزيارة في إطار تعزيز التعاون الاستراتيجي بين الإمارات والولايات المتحدة لتطوير قدرات الأمن السيبراني، ودعم الابتكار، والمساهمة في التنمية المستدامة من خلال التقنيات المتقدمة.

الحكومة

Apr Gisec EN

EMT, in collaboration with the UAE Cyber Security Council and GISEC 2025, announces the 2nd edition of the exclusive and immersive “Cyber Escape Experience” at the Dubai World Trade Center. This interactive experience will challenge participants to solve cybersecurity-related puzzles and scenarios in a race against time, testing their knowledge of the latest security practices and innovations. H.E. Dr. Mohamed Al-Kuwaiti expresses strong support for the initiative, highlighting its importance in advancing cybersecurity awareness through industry partnerships. EMT CEO Mo Mobasseri emphasizes combining education with immersive entertainment to engage professionals and the broader public. The Cyber Escape Room is a key highlight of GISEC 2025.

-Government

ِApril Gisec AR

أعلن مجلس الأمن السيبراني لحكومة دولة الإمارات عن تعاون مع شركة إي إم تي و معرض ومؤتمر الخليج لأمن المعلومات 2025، عن إطلاق النسخة الثانية من تجربة "غرفة الهروب السيبراني" التفاعلية والمميزة، وذلك في مركز دبي التجاري العالمي. تهدف هذه التجربة التفاعلية إلى تحدي المشاركين من خلال حل ألغاز وسيناريوهات مرتبطة بالأمن السيبراني ضمن سباق مع الزمن، ما يختبر معرفتهم بأحدث الممارسات والابتكارات في هذا المجال. وأعرب سعادة الدكتور محمد الكويتي عن دعمه الكامل لهذه المبادرة، مؤكداً أهميتها في رفع الوعي السيبراني عبر شراكات فاعلة مع القطاع. من جانبه، شدد الرئيس التنفيذي لشركة إي إم تي، السيد مو مباصري، على أهمية الدمج بين التعليم والترفيه التفاعلي لجذب المهنيين والجمهور العام، مشيراً إلى أن غرفة "الهروب السيبراني" تُعد من أبرز فعاليات معرض ومؤتمر الخليج لأمن المعلومات 2025.

الحكومة

May 6/8 AR

اختتم مجلس الأمن السيبراني فعاليات "جيسيك جلوبال 2025" بتحقيق 11 رقمًا قياسيًا عالميًا جديدًا في موسوعة غينيس، من خلال التمرين السيبراني الدولي بمشاركة وفود من أكثر من 130 دولة. عكس الحدث ريادة الإمارات في الأمن السيبراني، تزامناً مع تصدرها مؤشر الأمن السيبراني العالمي لعام 2024. شملت الفعاليات تمارين متقدمة، وورش توعية، ومحاكاة لهجمات إلكترونية، لتعزيز الاستجابة الوطنية والعالمية للتهديدات السيبرانية. وأكد الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات العربية المتحدة، أهمية التعاون الدولي وبناء القدرات البشرية في ظل التحول الرقمي المتسارع. كما أثنى الاتحاد الدولي للاتصالات على دور المجلس، مؤكداً استمرار الشراكة لدعم الابتكار السيبراني. ويُعد التمرين منصة استراتيجية لتبادل الخبرات وتعزيز الجاهزية السيبرانية عالمياً.

الحكومة

MAY 6/8 EN

The UAE Cyber Security Council concluded the “GISEC Global 2025” event, achieving 11 new Guinness World Records through the International Cybersecurity Drill with the participation of delegations from over 130 countries. The event reflected the UAE’s leadership in cybersecurity, coinciding with its top ranking on the 2024 Global Cybersecurity Index. The activities featured advanced exercises, awareness workshops, and simulated cyberattacks designed to enhance national and global response to cyber threats. H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, emphasized the vital role of international cooperation and capacity-building amid rapid digital transformation. The International Telecommunication Union praised the Council’s leadership, confirming the continuation of their partnership to support innovation in cybersecurity. The drill served as a strategic platform for exchanging expertise and advancing global cybersecurity readiness.

-Government

May 8 AR

اختتم مجلس الأمن السيبراني مشاركته في "جيسيك جلوبال 2025"، أكبر معرض للأمن السيبراني في المنطقة، محققاً 11 رقماً قياسياً جديداً في موسوعة غينيس، ومؤكداً ريادة الإمارات في الأمن السيبراني. شهد الحدث إطلاق النسخة الثانية من التمارين السيبرانية الدولية بمشاركة 130 دولة، وتوقيع اتفاقيات مع جهات محلية ودولية، إلى جانب استعراض مبادرات مبتكرة مثل "النبض السيبراني" وغرفة الهروب السيبرانية. أكد الدكتور محمد الكويتي أهمية المعرض في مواجهة التحديات الرقمية وتعزيز الشراكات الدولية، فيما شدد الاتحاد الدولي للاتصالات على ضرورة الاستثمار في الأمن السيبراني لضمان مستقبل رقمي آمن. ويواصل المجلس ترسيخ مكانة الدولة كمركز عالمي للابتكار والتعاون في مواجهة التهديدات السيبرانية.

الحكومة

May 8 EN

The UAE Cyber Security Council concluded its participation in GISEC Global 2025, the largest cybersecurity exhibition in the region, achieving 11 new Guinness World Records and reaffirming the UAE’s leadership in cybersecurity. The event featured the launch of the second edition of the International Cybersecurity Drills with participation from 130 countries, signing agreements with local and international entities, and showcasing innovative initiatives such as the ‘Cyber Pulse’ project and the Cyber Escape Room. Dr. Mohamed Al Kuwaiti highlighted the importance of the exhibition in addressing digital challenges and strengthening international partnerships. Meanwhile, the International Telecommunication Union emphasised the need to invest in cybersecurity to ensure a secure digital future. The Council continues to solidify the UAE’s position as a global hub for innovation and cooperation in combating cyber threats.

-Government

May 29 AR

نظّمت دائرة الصحة في أبوظبي، بالتعاون مع مجلس الأمن السيبراني، تمرينًا سيبرانيًا شاملًا لتعزيز مرونة القطاع الصحي في مواجهة التهديدات الرقمية، ضمن شراكة استراتيجية تهدف لحماية البنية التحتية الرقمية للدولة. شمل التمرين محاكاة لهجمات إلكترونية محتملة، واختبار جاهزية المنشآت الصحية وخطط الاستجابة، مع التركيز على حماية بيانات المرضى واستمرارية الخدمات. وأشاد الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات العربية المتحدة، بجهود دائرة الصحة في تسخير الحلول الرقمية للارتقاء بجودة الرعاية، مؤكدًا التزام المجلس بدعم الجهات الحكومية عبر التدريب والاستشارات. ويُعد هذا التمرين جزءًا من استراتيجية رائدة لأمن المعلومات في أبوظبي، تعزز الجاهزية السيبرانية وتكرّس ثقافة أمن المعلومات في القطاع الصحي.

الأفراد والعائلات

الشركات

May 29 EN

The Department of Health – Abu Dhabi, in partnership with the UAE Cyber Security Council, conducted a comprehensive cybersecurity drill to boost the healthcare sector’s resilience against digital threats. This initiative is part of a strategic effort to protect the nation’s digital infrastructure. The drill featured simulated cyberattacks to test the readiness of healthcare facilities and their response plans, focusing on safeguarding patient data and ensuring uninterrupted service. H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, commended the Department of Health’s use of digital solutions to enhance care quality and reaffirmed the Council’s commitment to supporting government entities through specialized training and advisory services. This drill is a key component of Abu Dhabi’s pioneering information security strategy, designed to strengthen cyber readiness and foster a culture of information security within the healthcare sector.

-Individuals & Families

-Corporations

Immersive AR

أعلنت شركة "إيميرسيف" عن إطلاق وحدة محتوى جديدة عبر منصتها Immersive One لدعم امتثال المؤسسات في الشرق الأوسط للمتطلبات السيبرانية والتنظيمية، مثل IAR وISR وADHICS. وتركّز الوحدة على تطوير الكفاءات السيبرانية من خلال مختبرات وتمارين واقعية، وتقييمات دورية، ولوحات تقارير متقدمة، مع تحديثات مستمرة لمواكبة التغيرات التنظيمية. تهدف هذه المبادرة إلى تمكين القادة من تعزيز جاهزيتهم الأمنية، وتحويل الالتزام التنظيمي من عبء إلى فرصة استراتيجية. وأكد الدكتور محمد الكويتي، رئيس الأمن السيبراني في حكومة دولة الإمارات، على أهمية التدريب المستمر في مواجهة التحديات التنظيمية المتسارعة، فيما أشار مسؤولو "إيميرسيف" إلى أن هذه الوحدة تسهم في تقليل المخاطر وتحقيق امتثال فعال ومستدام.

الحكومة

Immersive EN

Immersive announces a new content module on its Immersive One platform to help Middle East organizations demonstrate and strengthen their cybersecurity and regulatory compliance, covering standards like the UAE Information Assurance Regulation (IAR), DESC Information Security Regulation (ISR), and Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS). The module offers hands-on labs, scenario-based exercises, regular assessments, and advanced reporting dashboards, with continuous updates to stay ahead of evolving regulations. This initiative empowers leaders to boost their security readiness and turn compliance from a challenge into a strategic advantage. H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, highlights the importance of ongoing training to keep up with fast-changing regulations, while Immersive’s team points to the module’s role in reducing risks and ensuring effective, lasting compliance.

-Government

Microsoft Defender AR

أعلن مجلس الأمن السيبراني لحكومة دولة الإمارات، بالتعاون مع شركة Digital Reach التابعة لمجموعة Reach وشركتها Shieldworkz، عن تطوير أول إرشادات وطنية للأمن السيبراني للطائرات بدون طيار في الدولة. تهدف الإرشادات إلى حماية المجال الجوي والبنية التحتية وسلامة البيانات، مع تزايد استخدام هذه الطائرات في قطاعات الزراعة، والرصد البيئي، والخدمات اللوجستية. أكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، أهمية وضع أطر تنظيمية استباقية للتقنيات الناشئة، فيما شدد مالك ملحم، الرئيس التنفيذي لمجموعة Reach، ومحمد خالد،نائب رئيس النمو والتحول المؤسسي في مجموعة Reach، على تعزيز الجاهزية الوطنية ودعم الابتكار الآمن. المبادرة تمثل خطوة استراتيجية لترسيخ ريادة الإمارات عالمياً، وضمان عمليات تشغيلية مرنة وآمنة ومتوافقة مع أفضل الممارسات الدولية.

الحكومة

Microsoft Defender EN

The UAE Cyber Security Council, in collaboration with Reach Digital, a subsidiary of Reach Group, and a cybersecurity firm Shieldworkz, announced the development of UAE’s first Drone Cybersecurity Guidelines. The guidelines aim to protect the nation’s airspace, infrastructure, and data integrity amid the increasing use of drones in sectors such as agriculture, environmental monitoring, and logistics. H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, emphasized the importance of proactive regulatory frameworks for emerging technologies. Malik Melhem, CEO of Reach Group, and Mohammad Khaled, Vice President of Growth and Business Transformation at Reach Group, highlighted the need to enhance national readiness and support secure innovation. This initiative represents a strategic step to strengthen the UAE’s global leadership and ensure flexible and secure global best practices.

-Government

Second Edition of Cyber Awarness AR

أطلق مجلس الأمن السيبراني النسخة الثانية من الحملة الوطنية للتوعية بالأمن السيبراني، ضمن جهود الإمارات لتعزيز الأمن الرقمي وبناء مجتمع واعٍ بالمخاطر الإلكترونية. تستمر الحملة عاماً كاملاً، وتشمل 52 موضوعاً أسبوعياً ضمن مبادرة "النبض السيبراني"، لتزويد الأفراد والمؤسسات بمهارات اكتشاف التهديدات والتصدي لها، ونشر أفضل الممارسات الوقائية. تتضمن الفعاليات أنشطة عبر منصات التواصل، وورش عمل، وندوات، وتحذيرات أمنية فورية. وأكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، أن الحملة تدعم رؤية "الإمارات 2031" لبناء مجتمع رقمي آمن، وتشكل خط الدفاع الأول ضد المخاطر السيبرانية، وترسخ مكانة الدولة كمركز إقليمي ودولي رائد في الأمن السيبراني.

الأفراد والعائلات

الشركات

Second Edition of Cyber Awarness EN

The UAE Cybersecurity Council has announced the launch of the second edition of the National Cybersecurity Awareness Campaign, as part of the UAE’s ongoing efforts to enhance digital security and build a cyber-aware society. Running for a full year, the campaign will introduce 52weekly topics under the Cyber Pulse initiative to equip individuals, government entities, and private institutions with the skills to detect and counter threats while promoting preventive best practices. The program includes events and activities across all social media platforms, alongside workshops, seminars, and real-time security alerts on emerging risks. H.E. Dr. Mohammed Al-Kuwaiti, Head of Cyber Security for the UAE Government, affirmed that the campaign supports UAE Vision 2031 to build a secure digital society, serves as the first line of defense against cyber risks, and reinforces the UAE’s position as a leading regional and global hub for cybersecurity.

-Individual & Families

-Corporations

CSC Drill AR

أطلق مجلس الأمن السيبراني لحكومة دولة الإمارات التمرين الدولي للأمن السيبراني خلال معرض "جيسيك جلوبال 2025" من 6 إلى 8 مايو في دبي، بمشاركة أكثر من 160 دولة، تعزيزاً للتعاون الدولي لمواجهة التهديدات الإلكترونية. يهدف التمرين إلى رفع الوعي وتطوير القدرات الدفاعية عبر محاكاة هجمات سيبرانية، وورش عمل، وجلسات استراتيجية تركز على الذكاء الاصطناعي والدفاع الرقمي. يؤكد الحدث ريادة الإمارات في الأمن السيبراني بعد تصدرها مؤشر الأمن السيبراني العالمي 2024، ويدعم رؤية التعاون الإقليمي والدولي لحماية البنية التحتية الحيوية. يشمل البرنامج تدريبات عملية، تبادل خبرات، وتطوير مهارات الاستجابة السريعة، بما يعزز المرونة والأمن الرقمي عالمياً.

الحكومة

CSC Drill EN

The UAE Cyber Security Council launched the International Cybersecurity Drill at GISEC Global 2025, held in Dubai from May 6 to 8, with participation from over 160 countries to strengthen international cooperation in responding to cyber threats. The drill aims to raise awareness and build defensive capabilities through advanced cyberattack simulations, educational and interactive workshops, and strategic sessions focused on AI and digital defense. The event underscores the UAE’s global leadership in cybersecurity following its top ranking on the 2024 Global Cybersecurity Index and supports regional and international collaboration to safeguard critical information infrastructure. The program features hands-on training, knowledge-sharing among national cybersecurity centers and incident response teams, and rapid-response skill development to bolster global cyber resilience and digital security.

-Government

June 19 AR

برعاية سمو الشيخ منصور بن زايد آل نهيان، أعلن مجلس الأمن السيبراني عن الفائزين بـ "جوائز التميز السيبراني" في حفل بسبيس 42 أرينا بأبوظبي. من أبرز الفائزين: معالي زكي أنور نسيبة (أفضل برنامج تعليمي)، معالي راشد سعيد العامري (أفضل مسؤول أمن معلومات)، معالي عهود الرومي (أفضل سيدة)، وزارة الداخلية ووزارة المالية (الامتثال)، منصة "تم" (أفضل استخدام للذكاء الاصطناعي)، Microsoft Copilot (الذكاء الاصطناعي – خاص/حكومي)، جامعة خليفة وكليات التقنية (ابتكار مناهج)، Spidersilk (أفضل شركة ناشئة)، محمد الحرسوسي (أفضل إماراتي)، أحمد الزرعوني (الإنجاز مدى الحياة)، فاطمة المنصوري (النجم الصاعد). الجوائز شملت 50 فئة فردية ومؤسسية وأكاديمية.

الشركات

June 19 EN

The UAE Cyber Security Council announced the winners of the first National Cybersecurity Excellence Awards, held under the patronage of His Highness Sheikh Mansour bin Zayed Al Nahyan at Space 42 Arena, Abu Dhabi. The pioneering initiative recognized 23 honorees across five categories, celebrating outstanding individuals, public and private sector achievements, academic excellence, and startups driving innovation in cybersecurity. Aligning with the UAE’s vision, the awards highlight best practices, innovative models, and collaborative efforts to strengthen the nation’s position as a global cybersecurity leader. The program reinforces the Council’s commitment to fostering talent, resilience, and sustainable digital transformation across all sectors.

-Government

June 21 AR

نظمت مجالس أبوظبي، بالتعاون مع مجلس الأمن السيبراني، جلسة حوارية بعنوان "التوعية السيبرانية للأبناء" في مجلس مزيد، قدمها سعادة الدكتور محمد الكويتي. تناولت الجلسة سبل حماية الأبناء من التهديدات الرقمية كالتنمر والاحتيال، وأهمية تمكينهم بالمعرفة الرقمية منذ الصغر، وتعزيز دور الأسرة في المراقبة الواعية، وإدماج التوعية السيبرانية في المناهج الدراسية. شددت على سد الفجوة المعرفية بين الأجيال، والتوعية القانونية، وبناء بيئة رقمية آمنة بالتعاون بين الأسرة والمدرسة والمجتمع. وأكد الكويتي أن الحماية تتطلب تكامل الأدوار، مع إجراءات وقائية وتقنيات آمنة، لضمان خصوصية الأبناء واستغلال التكنولوجيا بشكل إيجابي وآمن.

الأفراد والعائلات

June 21 EN

Majalis Abu Dhabi, in collaboration with the UAE Cyber Security Council, hosted a dialogue session titled “Cyber Awareness for Children” at Mazid Majlis, led by His Excellency Dr. Mohamed Al Kuwaiti. The session addressed how to protect children from escalating digital risks such as cyberbullying and online fraud, highlighting the importance of early digital literacy, empowering parents with knowledge and smart guidance-based monitoring, and integrating cybersecurity awareness into school curricula. It also emphasized bridging the knowledge gap between generations, strengthening legal awareness of online behavior, and building a safe digital environment through coordinated efforts among families, schools, and the community. Dr. Al Kuwaiti underscored that effective protection requires shared responsibility and complementary roles, combining preventive measures and secure technologies to safeguard children’s privacy and promote safe, positive digital engagement.

-Individuals & Families

June 27 AR

نظمت مجالس أبوظبي، بالتعاون مع مجلس الأمن السيبراني، جلسة حوارية بعنوان "دور الأسرة في الوقاية السيبرانية" في مجلس الريف، قدمها سعادة الدكتور محمد الكويتي. تناولت الجلسة التحديات الرقمية التي تواجه الأسر، خصوصًا الأطفال، جراء انتشار الأجهزة الذكية والألعاب والتطبيقات، وما يصاحبها من مخاطر كالعنف الرقمي، الإدمان، والاحتيال. شددت على أهمية تدخل الأسرة المبكر، واعتماد آليات ذكية للمراقبة تحترم الخصوصية، وتعزيز الشراكات بين القطاعين العام والخاص لتطوير حلول حماية فعّالة. أكد الكويتي أن تمكين الآباء والأبناء بالمهارات الرقمية والتعاون مع المدارس أساس لبناء جيل واعٍ، وأن الإمارات تسعى لتكون نموذجًا عالميًا في الحماية السيبرانية المجتمعية.

الأفراد والعائلات

June 27 EN

Majalis Abu Dhabi, in collaboration with the UAE Cyber Security Council, hosted a high-level dialogue session titled “The Family’s Role in Cyber Protection” at Al Reef Majlis, led by H.E. Dr. Mohammed Al Kuwaiti, Head of Cyber Security for the UAE Government. The session addressed the rise in smart device, gaming, and app use among children and the associated risks—online fraud, cyberbullying, exposure to violent or age-inappropriate content, and digital addiction. It emphasized early family intervention, the use of smart, guidance-based monitoring tools that respect privacy, and strengthening public-private partnerships to develop effective protection solutions. Dr. Al Kuwaiti underscored that empowering parents and children with digital skills, together with close school–family collaboration, is essential to building a digitally aware, resilient generation, reaffirming the UAE’s ambition to serve as a global model for community-based cybersecurity.

-Individuals & Families

CSC Governance Summit EN

The UAE Cyber Security Council hosted the UAE Cyber Governance Summit in Ajman on 8 July 2025, convening over 100 government officials, cyber regulators, and cybersecurity professionals. The summit served as a platform to advance the UAE’s cyber security vision, strengthen cross-emirates collaboration, and share insights on cyber initiatives and governance frameworks. H.E. Dr. Mohamed Hamad Al Kuwaiti underscored digital infrastructure; H.E. Dr. Ohoud Ali Shehail highlighted cybersecurity as a necessity and announced the launch of AjmanOne Security Operations Center (SOC). Sessions covered the UAE Cyber Security Strategy 2031, NSOC, the National Cyber Index Platform, and policy and governance frameworks, plus panels on emirate-level resilience and cloud security. The summit underscored cooperation, adaptive regulation, and national capabilities to secure the UAE’s digital future.

-Government

CSC Governance Summit AR

استضاف مجلس الأمن السيبراني لدولة الإمارات قمّة حوكمة الأمن السيبراني التي عُقدت في إمارة عجمان في 8 يوليو 2025، بحضور أكثر من 100 من كبار المسؤولين الحكوميين والمنظمين السيبرانيين والمتخصصين في الأمن السيبراني.

وقد شكلت القمة منصة استراتيجية لتعزيز رؤية الدولة في مجال الأمن السيبراني، ودعم التعاون بين مختلف الإمارات، وتبادل الرؤى الحصرية حول المبادرات السيبرانية الناشئة وأطر الحوكمة ذات الصلة. وأكد سعادة الدكتور محمد حمد الكويتي أهمية البنية التحتية الرقمية، فيما شدّدت سعادة الدكتورة عهود علي شهيل في كلمتها الافتتاحية على أن الأمن السيبراني لم يعد خيارًا بل ضرورة استراتيجية، حيث أعلنت عن إطلاق مركز عمليات الأمن السيبراني لحكومة عجمان (AjmanOne SOC). وسلّطت محاور القمة الضوء على استراتيجية الإمارات للأمن السيبراني 2031، والمركز الوطني لعمليات الأمن السيبراني (NSOC)، ومنصة المؤشر الوطني للأمن السيبراني، وأطر السياسات والحوكمة الوطنية للأمن السيبراني. أمّا في الجلسات النقاشية، تمّت مناقشة كيفية تعزيز الصمود السيبراني على مستوى الإمارات وحماية بيئات العمل السحابية. وقد أكدت القمة على أهمية تعزيز التعاون، وتطوير السياسات وبناء القدرات الوطنية لحماية المستقبل الرقمي في الإمارات.

الحكومة

SCAM Incident EN

The UAE Cyber Security Council is urging the public to avoid sharing personal information and to steer clear of downloading unverified apps to protect against cyber fraud. The Council warned that unsolicited messages or calls can open the door to phishing and scams. With criminals now using advanced tools, including AI, cyber fraud has become more sophisticated—exploiting online services, apps, and networks. In response, the Council has launched workshops, Majalis sessions, and awareness campaigns promoting safe digital habits, from downloading only from official stores to verifying sources and keeping systems updated. Public awareness, it emphasized, remains the nation’s first line of defense.

-Individuals & Families

-Corporations

SCAM Incident AR

يحثّ مجلس الأمن السيبراني لدولة الإمارات المواطنين على أخذ الحيطة والحذر في موضوع مشاركة المعلومات والبيانات الشخصية، والامتناع عن تحميل التطبيقات غير الموثوقة، وذلك لتجنّب العمليات السيبرانية الاحتيالية. كما حذّر المجلس من التعامل مع الرسائل والمكالمات مجهولة المصدر والتي قد تكون نافذة لعمليات التصيد والاحتيال الإلكتروني. ومع التقدّم التكنولوجي الذي يستغلّه المحتالون، أهمها أدوات الذكاء الاصطناعي، أصبح الاحتيال السيبراني أكثر تطوراً مستغلاً الخدمات الإلكترونية، والتطبيقات الذكية، والشبكات الرقمية. لذلك نظّم المجلس ورش عملٍ وجلساتٍ حوارية وحملاتٍ توعويةٍ تهدف إلى تعزيز السلوك الرقمي الآمن من خلال تحميل التطبيقات من المتاجر الرسمية، والتحقق من المصادر، وتحديث الأنظمة بشكل مستمر. وأكّد المجلس أن وعي الأفراد هو خط الدفاع الأول لحماية المجتمع الإماراتي رقمياً.

الأفراد والعائلات

الشركات

CSC x CPX x Google Cloud EN

The UAE Cyber Security Council signed a strategic contract with Rilian Technologies, in coordination with CPX Holding, to secure critical infrastructure. Through the National Security Operations Center (NSOC), NSOC will implement the Rilian Defense Platform (RDP) to integrate, operate, and automate cybersecurity solutions across Operational Technology (OT). Leveraging advanced technologies from partners including Google Cloud, the program will deliver a next-generation security operations platform with real-time threat detection, automated incident response, and advanced analytics. The agreement also tasks Rilian and CPX with developing AI agents to automate defenses and assess OT risk.

-Government

CSC x CPX x Google Cloud- AR

وقّع مجلس الأمن السيبراني لدولة الإمارات عقداً مع "ريليان تكنولوجيز" لتأمين البنية التحتية الحيوية في الإمارات، بالتنسيق مع شركة CPX القابضة، بهدف تأمين البنية التحتية الحيوية للدولة. وسيقوم المركز الوطني لعمليات الأمن السيبراني (NSOC) في الإمارات بالعمل مع ريليان تكنولوجيز لتطبيق منصة ريليان للدفاع (RDP) ودمج وتشغيل وأتمتة حلول الأمن السيبراني المختلفة في تكنولوجيا التشغيل (OT). ويعتمد المشروع على التقنيات المتقدّمة من الشركاء العالميين بما في ذلك جوجل كلاود، لتقديم منصة عمليات أمنية من الجيل التالي تتميّز باكتشاف التهديدات في الوقت الفعلي، والاستجابة التلقائية للحوادث، والتحليلات المتقدمة. كما سيكلّف الاتفاق شركتي ريليان و"CPX" لتطوير عملاء الذكاء الاصطناعي لأتمتة حلول التهديدات السيبرانية وتقييم المخاطر على البنية التحتية الوطنية الحيوية.

الحكومة

Awareness 4 EN

The UAE Cyber Security Council kicked off the first week of the Cyber Pulse Initiative’s 52-week awareness campaign under the theme “Backing up your data is no longer an option—it’s a necessity.” The week highlights backup as the first line of defense for individuals and institutions, reducing data loss, enabling rapid incident response, ensuring business continuity, and supporting compliance with regulatory standards. The Council urges daily backups of customer and operational data, weekly backups of operational data, and regular testing of backup effectiveness. Robust, verified backups help organizations recover faster from cyberattacks and minimize downtime and impact.

-Corporations

Awareness 4 AR

أطلق مجلس الأمن السيبراني لدولة الإمارات فعاليات الأسبوع الأول من الحملة التوعوية لمبادرة النبض السيبراني الممتدة على مدار 52 أسبوعاً، تحت شعار "النسخ الاحتياطي لم يعد خيارًا.. بل واجبًا". وسلّط هذا الأسبوع الضوء على أهمية عمليات النسخ الاحتياطي للملفات الهامة للمؤسسات والشركات، والتي تسهم في تقليل فرص فقدان البيانات، والاستجابة السريعة للحوادث، وضمان استمرارية الأعمال، والامتثال للمعايير التنظيمية.

وشدد المجلس على إجراء النسخ يومياً للبيانات التشغيلية وبيانات العملاء، ونسخ الأسبوعية للبيانات التشغيلية، وبالإضافة إلى اختبار فعالية النسخ الاحتياطي بانتظام. وتضمن هذه الاستراتيجية قدرة المؤسسات على التعافي من آثار الهجمات الإلكترونية بسرعة، وتقليل زمن التعطل والتكاليف المترتبة عليها.

الشركات

Awareness 5 AR

أطلق مجلس الأمن السيبراني الأسبوع الثاني من حملة "النبض السيبراني" للتوعية وناقش مخاطر شبكات الواي فاي المجانية وسبل حماية البيانات الشخصية، وحملت الحملة شعار "خدمة الواي فاي المجانية قد تكشف بياناتك الشخصية". حذرت الحملة من أن هذه الشبكات، خاصة في الأماكن العامة، قد تُستغل لاختراق كلمات المرور والمعلومات المالية، وتثبيت برمجيات خبيثة. وقدمت ثلاثة إرشادات أساسية: استخدام تطبيق VPN موثوق، تفعيل التصفح الآمن، وتجنب الدخول للحسابات الحساسة. تأتي الحملة، التي تستمر 52 أسبوعاً، ضمن جهود الدولة لتعزيز الثقافة والمرونة السيبرانية، وبناء فضاء رقمي آمن يواكب التطورات التقنية ويحمي المستخدمين من التهديدات الإلكترونية.

الأفراد والعائلات

الشركات

Awareness 5 EN

The UAE Cyber Security Council launched the second week of the Cyber Pulse Initiative’s awareness campaign, spotlighting the risks of using free and public Wi-Fi networks and practical ways to protect personal data. Under the slogan “Free Wi-Fi could expose your personal data,” the message warns that unsecured networks, especially in public places, can be exploited to steal passwords and financial information or install malware. The Council set out three main steps for safer browsing on open networks: use a reliable VPN application, enable ‘Safe Browsing’ in your browser, and avoid signing in to sensitive accounts. Running for 52 weeks, the campaign is part of the UAE’s broader effort to enhance cyber awareness and resilience, building a secure digital environment that keeps pace with rapid technological change and protects users from evolving threats.

-Individual & Families

-Corporations

Awareness 6 AR

أطلق مجلس الأمن السيبراني في الأسبوع الثالث من حملة "النبض السيبراني" التوعوية، تحت شعار "إهمال التحديثات يعني مخاطر سيبرانية أعلى - الأرقام تحذر"، رسائل توضح خطورة تجاهل تحديثات البرامج والأنظمة الرقمية. أظهرت الإحصاءات اكتشاف أكثر من 30,000 ثغرة جديدة في 2024، وأن 70% من الأنظمة غير المحدّثة عرضة للهجمات. ودعا المجلس لتفعيل التحديثات التلقائية للهواتف، الحواسيب، المتصفحات، أجهزة التوجيه، وأجهزة المنزل الذكي، لتجنب البرمجيات الخبيثة وسرقة البيانات. شدد على أن التحديثات تمثل دروع حماية رقمية أساسية. وتستمر الحملة 52 أسبوعاً، في إطار جهود الإمارات لتعزيز الثقافة والمرونة السيبرانية وبناء فضاء رقمي آمن يواكب التطورات التقنية.

الأفراد والعائلات

الشركات

Awareness 6 EN

The UAE Cyber Security Council launched the third week of the Cyber Pulse Initiative’s awareness campaign across social media under the slogan “Neglecting updates means higher cybersecurity risk — the numbers are alarming.”The message highlights the dangers of ignoring software and digital system updates: recent figures point to 30,000+ new vulnerabilities in 2024, and 70% of out-of-date systems remain highly susceptible to attack. The Council urges users to enable automatic updates on smartphones, laptops, browsers, routers, and smart home devices to reduce the risk of malware, data theft, and network breaches, underscoring that updates are essential digital protection shields. Running for 52 weeks, the campaign forms part of the UAE’s ongoing effort to enhance cyber awareness and resilience and build a secure digital environment that keeps pace with rapid technological change.

-Individual & Families

-Corporations

Awareness 7 AR

حذرت حملة "النبض السيبراني" في أسبوعها الرابع من تزايد الهجمات الإلكترونية على المنازل الذكية، مؤكدة أن 70% من أجهزة إنترنت الأشياء المنزلية عرضة للاختراق في حال غياب الحماية الكافية. وأوضحت أن أجهزة مثل المساعدات الصوتية، وأنظمة المراقبة، والإضاءة والتكييف الذكي، قد تشكل أهدافاً سهلة للمخترقين عند استخدام الإعدادات الافتراضية أو ضعف الوعي الأمني. ودعت الحملة إلى اعتماد كلمات مرور قوية، وتحديث الأنظمة بانتظام، وفصل شبكة الأجهزة الذكية عن الشبكة الرئيسية، مع تعطيل المساعدات الصوتية عند عدم الحاجة. تأتي هذه الجهود ضمن رؤية الإمارات لتعزيز الأمن السيبراني وحماية الخصوصية في ظل التطورات الرقمية المتسارعة.

الأفراد والعائلات

الشركات

Awareness 7 EN

The UAE Cyber Security Council’s Cyber Pulse Initiative launched the fourth week of its awareness campaign, warning of rising attacks on smart homes and noting that 70% of IoT devices used within homes are vulnerable without adequate protection. The message highlights that voice assistants, surveillance systems, and smart lighting and HVAC have become an attractive target for hackers, especially given the weak security awareness among some users or reliance on default device settings. The Council urges users to adopt strong, unique passwords, keep devices up to date, place smart devices on a separate network from the main home Wi-Fi, and switch off voice assistants when not in use. Part of a 52-week program, these efforts align with the UAE’s vision to enhance cybersecurity and protect privacy amid rapid digital transformation.

-Individual & Families

-Corporations

Awareness 8 AR

ركّز الأسبوع الخامس من حملة "النبض السيبراني" على مخاطر إهمال تأمين البصمة الرقمية، مبيّناً أن كل نشاط إلكتروني يترك أثراً يمكن تتبعه واستغلاله. وأشار مجلس الأمن السيبراني إلى أن أكثر من 1.4 مليار حساب يتم اختراقه شهرياً عالمياً، وأن البصمة الرقمية تنقسم إلى سلبية تُجمع دون علم المستخدم، وأخرى نشطة يتركها طوعاً عبر المنشورات والتفاعلات. وشدد على ضرورة الحذر من التطبيقات غير الموثوقة، وتفعيل المصادقة الثنائية، ومراجعة الصلاحيات وطلبات الصداقة، وتجنب مشاركة الموقع الجغرافي. وتأتي هذه الجهود ضمن رؤية الإمارات لتعزيز الثقافة السيبرانية، وحماية الخصوصية، وبناء فضاء رقمي آمن يواكب التطورات التقنية ويحمي الأفراد من التهديدات الإلكترونية.

الأفراد والعائلات

الشركات

Awareness 8 EN

The UAE Cybersecurity Council’s Cyber Pulse Initiative devoted its fifth week to the risks of an unsecured digital footprint because every login, post, and click leaves a trace that can be tracked and exploited. Recent figures indicate that more than 1.4 billion accounts are compromised globally each month. The Council distinguishes between a passive footprint (data collected about you without your knowledge) and an active footprint (content you intentionally share through posts and interactions). To reduce exposure, download apps only from official stores, avoid untrusted applications, enable two-factor authentication, review app permissions and friend requests regularly, and limit location sharing. As part of a 52-week program, the campaign supports the UAE’s effort to strengthen cyber awareness and resilience, protect privacy, and build a secure digital environment that keeps pace with rapid technological change.

-Individual & Families

-Corporations

AR Awareness against Digital Threats

حثّ مجلس الأمن السيبراني وشرطة أبوظبي الجمهور على توخي الحذر عند التعامل مع الرسائل أو المكالمات المجهولة، محذرين من إمكانية استغلالها في عمليات التصيّد والاحتيال الإلكتروني. وأكدت الجهات المعنية أنّ التطورات التكنولوجية المتسارعة وسوء استخدام تقنيات الذكاء الاصطناعي أسهما في تصاعد الهجمات السيبرانية الأكثر تعقيداً، مما يبرز الحاجة إلى اليقظة، والاستخدام المسؤول للتطبيقات الرقمية، والاعتماد حصراً على المنصات الرسمية. كما شدّدوا على أهمية الحملات التوعوية وورش العمل والمبادرات المستمرة الهادفة إلى حماية المجتمع من مخططات الاحتيال، داعين إلى الإبلاغ الفوري عن أي أنشطة مشبوهة عبر القنوات الرسمية لشرطة أبوظبي.

* الأفراد والعائلات

EN Awareness against Digital Threats

The Cyber Security Council and Abu Dhabi Police urged the public to exercise caution when dealing with unknown messages or calls, warning that they may be used for phishing and online fraud. The authorities stressed that rapid technological advancements and the misuse of artificial intelligence have fueled more sophisticated cyberattacks, underscoring the need for vigilance, responsible use of digital applications, and reliance only on official platforms. They further highlighted ongoing awareness campaigns, workshops, and initiatives aimed at protecting the community from fraudulent schemes, while urging immediate reporting of suspicious activity through official Abu Dhabi Police channels.

* Individuals & Families

August Week 1 EN

The Cyber Security Council, through its Cyber Pulse Initiative, warned against the growing risks of social engineering, stressing that 98% of cyberattacks rely on this form of deception to target individuals and institutions. The message, issued during the sixth week of the 52-week national awareness campaign, highlighted how fraudsters manipulate trust, emotions, and urgency to trick victims into disclosing sensitive personal or financial data. The Council urged the public to remain vigilant, avoid sharing confidential information, and rely on official guidance to strengthen digital awareness and resilience in the face of evolving cyber threats.

* Individuals & Families
* Corporations

August Week 1 AR

حذر مجلس الأمن السيبراني، من خلال ”مبادرة "النبض السيبراني"، من المخاطر المتزايدة للهندسة الاجتماعية، مشدداً على أن 98% من الهجمات السيبرانية تعتمد على هذا النوع من الخداع لاستهداف الأفراد والمؤسسات. وأبرزت الرسالة، التي صدرت خلال الأسبوع السادس من حملة التوعية الوطنية التي تستمر 52 أسبوعًا، كيف يستغل المحتالون الثقة والعواطف والحاجة الملحة لخداع الضحايا وكشفهم عن بياناتهم الشخصية أو المالية الحساسة. وحث المجلس الجمهور على توخي الحذر وتجنب مشاركة المعلومات السرية والاعتماد على الإرشادات الرسمية لتعزيز الوعي الرقمي والقدرة على الصمود في مواجهة التهديدات السيبرانية المتطورة.

-الأفراد والعائلات

-الشركات

August Week 2 EN + AR

The Cyber Security Council, through its ‘Cyber Pulse’ Initiative, warned that 60% of smartphone users ignore essential device updates, leaving their phones, tablets, and laptops exposed to cyberattacks. As part of the campaign’s seventh weekly awareness message, the Council highlighted the rising risks of malware and mobile hacking, which have surged by 50% in recent years, and stressed that securing personal devices has become a necessity to protect sensitive data, financial information, and communications. The Council urged the public to adopt safe practices such as regularly updating operating systems and applications, enabling biometric security features, and downloading apps only from trusted sources to strengthen digital protection at both individual and institutional levels.

* Individuals & Families

حذّر مجلس الأمن السيبراني، من خلال مبادرة "النبض السيبراني"، من أنّ 60% من مستخدمي الهواتف الذكية يتجاهلون التحديثات الأساسية لأجهزتهم، مما يعرّض هواتفهم وأجهزتهم اللوحية والمحمولة لهجمات سيبرانية. وفي إطار الرسالة التوعوية الأسبوعية السابعة للحملة، سلط المجلس الضوء على تصاعد مخاطر البرمجيات الخبيثة واختراق الهواتف الذكية، والتي ارتفعت بنسبة 50% في السنوات الأخيرة، مؤكداً أنّ تأمين الأجهزة الشخصية أصبح ضرورة لحماية البيانات الحساسة والمعلومات المالية والاتصالات. وحث المجلس الجمهور على تبنّي ممارسات آمنة، مثل التحديث المنتظم لأنظمة التشغيل والتطبيقات، وتفعيل ميزات الأمان البيومترية، وتحميل التطبيقات حصراً من المصادر الموثوقة، وذلك لتعزيز الحماية الرقمية على المستويين الفردي والمؤسسي.

الأفراد والعائلات

August Week 3 EN + AR

The Cyber Security Council, through its ‘Cyber Pulse’ Initiative, dedicated the 8th week of its awareness campaign to protecting financial data and securing digital banking transactions. The Council revealed that 60% of cyberattacks start with stolen login credentials, while safe practices can reduce data theft risks by up to 40%. It urged users to enable biometric logins and multi-factor authentication, regularly update financial applications, and avoid sharing personal information through calls, messages, or unverified platforms. Emphasizing that protecting banking accounts is essential for individuals, businesses, and national economic stability, the Council warned that unsecured devices can lead to financial loss and identity theft, and called on the public to adopt secure digital behaviors as a collective responsibility.

* Individuals & Families

خصّص مجلس الأمن السيبراني، من خلال مبادرة "النبض السيبراني"، الأسبوع الثامن من حملته التوعوية لحماية البيانات المالية وتأمين المعاملات المصرفية الرقمية. وكشف المجلس أن 60٪ من الهجمات السيبرانية تبدأ بسرقة بيانات تسجيل الدخول، في حين أن الممارسات الآمنة يمكن أن تقلل من مخاطر سرقة البيانات بنسبة تصل إلى 40٪. وحث المجلس المستخدمين على تمكين تسجيل الدخول البيومتري والمصادقة متعددة العوامل، وتحديث التطبيقات المالية بانتظام، وتجنب مشاركة المعلومات الشخصية عبر المكالمات أو الرسائل أو المنصات غير المؤكدة. وشدد المجلس على أن حماية الحسابات المصرفية أمر ضروري للأفراد والشركات والاستقرار الاقتصادي الوطني، وحذّر من أن الأجهزة غير الآمنة يمكن أن تؤدي إلى خسائر مالية وسرقة الهوية، ودعا الجمهور إلى تبني سلوكيات رقمية آمنة باعتبارها مسؤولية جماعية.

الأفراد والعائلات

August Week 4 EN + AR

The Cyber Security Council, through its ‘Cyber Pulse’ Initiative, warned of rising cyber fraud risks linked to the rapid expansion of ‘Buy Now, Pay Later’ (BNPL) services. In its 9th weekly awareness message, the Council highlighted that while BNPL offers convenience, weak security measures and fraudulent schemes can expose users to account takeovers, data breaches, and financial losses. It urged the public to remain cautious during online transactions, avoid unverified links and fake offers, and adopt preventive measures such as multi-factor authentication, trusted payment providers, and regular monitoring of financial accounts. The Council stressed that digital awareness remains the strongest defense against cyber fraud and that safeguarding online transactions is essential for long-term financial stability and digital safety.

* Individuals & Families

حذر مجلس الأمن السيبراني، من خلال مبادرة "النبض السيبراني"، من تزايد مخاطر الاحتيال السيبراني المرتبطة بالتوسع السريع في خدمات "اشترِ الآن، ادفع لاحقاً". في رسالته التوعوية الأسبوعية التاسعة، سلط المجلس الضوء على أنه في حين توفر خدمات "اشترِ الآن، ادفع لاحقاً" الراحة، إلا أنّ ضعف إجراءات الأمان والممارسات الاحتيالية يمكن أن يعرض المستخدمين لخطر الاستيلاء على حساباتهم، وانتهاك بياناتهم، وخسائر مالية. وحث المجلس الجمهور على توخي الحذر أثناء المعاملات الإلكترونية، وتجنب الروابط غير الموثوقة والعروض الوهمية، واتخاذ تدابير وقائية مثل المصادقة متعددة العوامل، ومقدمي خدمات الدفع الموثوق بهم، والمراقبة المنتظمة للحسابات المالية. وشدد المجلس على أن الوعي الرقمي يظل خط الدفاع الأقوى ضد الاحتيال السيبراني، وأن حماية المعاملات الإلكترونية أمر ضروري لتحقيق الاستقرار المالي والسلامة الرقمية على المدى الطويل.

* الأفراد والعائلات

Expo Japan - Full Agenda EN+AR

The Cyber Security CounciL, in collaboration with the National Emergency Crisis and Disaster Management Authority (NCEMA), launched a series of interactive cybersecurity dialogues and activities at the UAE Pavilion in Expo 2025 Japan, Osaka. The sessions address themes including cyber diplomacy, AI and IoT threat readiness, resilience through cyber drills, and youth talent enablement, while NCEMA is presenting initiatives on community engagement, resilient infrastructures, and business continuity. H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, and H.E. Ali Saeed Al Neyadi, Chairman of NCEMA, emphasized the importance of proactive strategies, AI-driven forecasting, and global collaboration to confront emerging threats and strengthen readiness. The joint participation underscores the UAE’s commitment to international cooperation in building safer and more resilient digital societies.

* Corporations

أطلق مجلس الأمن السيبراني، بالتعاون مع الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث، سلسلة من الحوارات والأنشطة التفاعلية حول الأمن السيبراني في جناح دولة الإمارات بإكسبو 2025 اليابان - أوساكا. وتتناول الجلسات محاور عدة تشمل الدبلوماسية السيبرانية، والاستعداد لمخاطر الذكاء الاصطناعي وإنترنت الأشياء، وتعزيز المرونة من خلال التمارين السيبرانية، وتمكين المواهب الشابية، فيما تستعرض الهيئة مبادرات خاصة بالتفاعل المجتمعي، والبنى التحتية المرنة، واستمرارية الأعمال. وأكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، وسعادة علي سعيد النيادي، رئيس الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث، على أهمية الاستراتيجيات الاستباقية، والتنبؤ المدعوم بالذكاء الاصطناعي، والتعاون الدولي في مواجهة التهديدات الناشئة وتعزيز الجاهزية. وتؤكد المشاركة المشتركة التزام دولة الإمارات بالتعاون الدولي لبناء مجتمعات رقمية أكثر أماناً ومرونة.

الشركات

MOE Collaboration EN+AR

The Ministry of Education announced that the Cyber Security Council will oversee the national cybersecurity curriculum, to be implemented across all public and private schools from Grade 1 to Grade 12. The initiative, aligned with UAE Vision 2031, represents a strategic step to enhance digital awareness, strengthen resilience against cyber threats, and prepare future generations with the skills needed to thrive in a secure digital environment. H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, affirmed that introducing cybersecurity education from early grades is a vital investment in human capital, supporting the UAE’s transition to a knowledge-based economy and reinforcing its position as a global leader in digital innovation and security.

* Individuals & Families

أعلنت وزارة التربية والتعليم أن مجلس الأمن السيبراني سيشرف على المنهج الوطني للأمن السيبراني، الذي سيتم تنفيذه في جميع المدارس الحكومية والخاصة من الصف الأول إلى الصف الثاني عشر. وتمثل هذه المبادرة، التي تتماشى مع رؤية الإمارات 2031، خطوة استراتيجية لتعزيز الوعي الرقمي، وتقوية القدرة على مواجهة التهديدات السيبرانية، وإعداد الأجيال القادمة بالمهارات اللازمة للنجاح في بيئة رقمية آمنة. أكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة الإمارات، أن إدماج التعليم السيبراني منذ المراحل الدراسية المبكرة يُعد استثماراً حيوياً في رأس المال البشري، بما يدعم انتقال دولة الإمارات إلى اقتصاد قائم على المعرفة ويعزز مكانتها كقوة رائدة عالمياً في الابتكار الرقمي والأمن السيبراني.

الأفراد والعائلات

EN+AR Ajman Crown Prince Meets

H.H. Sheikh Ammar bin Humaid Al Nuaimi, Crown Prince of Ajman and Chairman of the Executive Council, received H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, and H.E. Dr. Ohoud Shaheel of the Ajman Cyber Security Council, in the presence of H.H. Sheikh Rashid bin Humaid Al Nuaimi. The meeting discussed ways to enhance Ajman’s digital and cloud infrastructure, with a focus on strengthening cybersecurity, protecting data privacy, and advancing digital government services. Emphasis was placed on cloud computing, artificial intelligence, and analytics as key enablers of efficiency and smart city development, while building robust cybersecurity frameworks was highlighted as essential to safeguarding infrastructure, ensuring operational continuity, and supporting the UAE’s vision for secure digital transformation.

* Corporations

استقبل سمو الشيخ عمار بن حميد النعيمي، ولي عهد عجمان رئيس المجلس التنفيذي، كلاً من سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، وسعادة الدكتورة عهود شهيل من مجلس عجمان للأمن السيبراني، وذلك بحضور سمو الشيخ راشد بن حميد النعيمي.

وبحث الاجتماع سبل تعزيز البنية التحتية الرقمية والحوسبة السحابية في إمارة عجمان، مع التركيز على تعزيز الأمن السيبراني، وحماية خصوصية البيانات، وتطوير الخدمات الحكومية الرقمية. وتم التأكيد على دور الحوسبة السحابية، والذكاء الاصطناعي، والتحليلات المتقدمة كممكّنات رئيسية للكفاءة وتطوير المدن الذكية، فيما جرى التشديد على بناء أطر قوية للأمن السيبراني باعتباره عنصراً أساسياً لحماية البنية التحتية، وضمان استمرارية العمليات، ودعم رؤية دولة الإمارات للتحول الرقمي الآمن.

الشركات

EN + AR CSC Participates in Bahrain’s Cyber Drill

The Cyber Security Council participated in Bahrain’s National Cyber Drill ‘Cyber Shield 2025,’ held under the patronage of H.H. Sheikh Nasser bin Hamad Al Khalifa and organized by the National Cybersecurity Center of Bahrain. The exercise, focused on supply chain attacks, brings together government entities, critical sectors, and private organizations to test cyber readiness and strengthen regional cooperation. H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, highlighted the importance of expanding collaboration, knowledge exchange, and joint preparedness with Bahrain and regional partners to confront emerging cyber threats and build resilient digital infrastructures.

* Corporations

شارك مجلس الأمن السيبراني في التمرين الوطني للأمن السيبراني "الدرع السيبراني 2025" في البحرين، والذي أقيم برعاية سمو الشيخ ناصر بن حمد آل خليفة ونظّمه المركز الوطني للأمن السيبراني في البحرين. وركز التمرين على هجمات سلاسل التوريد، جامعاً بين الجهات الحكومية والقطاعات الحيوية والمؤسسات الخاصة لاختبار الجاهزية السيبرانية وتعزيز التعاون الإقليمي.

وأكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، على أهمية توسيع التعاون وتبادل المعرفة وتعزيز الجاهزية المشتركة مع مملكة البحرين والشركاء الإقليميين لمواجهة التهديدات السيبرانية الناشئة وبناء بنى تحتية رقمية مرنة.

-الشركات

EN + AR Sheikh Zayed Visit to CSC

H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, welcomed H.E. Sheikh Zayed bin Hamad Al Nahyan, Chairman of the National Anti-Narcotics Authority, during an official visit to the Cyber Security Council. The meeting reviewed the Council’s initiatives to strengthen the nation’s digital infrastructure and emphasized the role of cybersecurity in supporting national efforts to combat organized crime and drug trafficking. Both sides underlined the importance of leveraging advanced technologies, including artificial intelligence, to enhance prevention, awareness, and resilience, while reaffirming their commitment to continued cooperation to safeguard community security and reinforce the UAE’s comprehensive approach to national security.

Government

Corporations

رحب سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة الإمارات، بسعادة الشيخ زايد بن حمد آل نهيان، رئيس الجهاز الوطني لمكافحة المخدرات، خلال زيارة رسمية لمجلس الأمن السيبراني. استعرض الاجتماع مبادرات المجلس لتعزيز البنية التحتية الرقمية للدولة، وشدد على دور الأمن السيبراني في دعم الجهود الوطنية لمكافحة الجريمة المنظمة وتهريب المخدرات. أكد الجانبان على أهمية الاستفادة من التقنيات المتقدمة، بما في ذلك الذكاء الاصطناعي، لتعزيز الوقاية والوعي والمرونة، مع إعادة تأكيد التزامهما بالتعاون المستمر لحماية أمن المجتمع وتعزيز النهج الشامل لدولة الإمارات العربية المتحدة في مجال الأمن القومي.

الحكومة

الشركات

Expo Japan - First Day AR

بمشاركة مجلس الأمن السيبراني والهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث انطلقت جلسات حوارية وأنشطة سيبرانية تفاعلية في جناح الدولة بمعرض إكسبو اليابان 2025 بأوساكا. وفي اليوم الأول لفعاليات إكسبو اليابان، شارك مجلس الأمن السيبراني بالتعاون مع الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث (NCEMA) في جناح الدولة من خلال سلسلة جلسات نقاشية وأنشطة تفاعلية ركزت على الأمن السيبراني والتهديدات الرقمية المتسارعة.

استهدفت الفعاليات تعزيز تبادل الخبرات الدولية، وعرض الابتكارات الإماراتية في الأمن السيبراني وإدارة الأزمات، مع عقد جلسات حول الدبلوماسية السيبرانية، الاستعداد للذكاء الاصطناعي وإنترنت الأشياء، بناء الدول المرنة، وتمكين الشباب والمواهب.

الحكومة

Expo Japan - First Day EN

بمشاركة مجلس الأمن السيبراني والهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث انطلقت جلسات حوارية وأنشطة سيبرانية تفاعلية

في جناح الدولة بمعرض إكسبو اليابان 2025 بأوساكا. وفي اليوم الأول لفعاليات إكسبو اليابان، شارك مجلس الأمن السيبراني بالتعاون مع الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث (NCEMA) في جناح الدولة من خلال سلسلة جلسات نقاشية وأنشطة تفاعلية ركزت على الأمن السيبراني والتهديدات الرقمية المتسارعة.

استهدفت الفعاليات تعزيز تبادل الخبرات الدولية، وعرض الابتكارات الإماراتية في الأمن السيبراني وإدارة الأزمات، مع عقد جلسات حول الدبلوماسية السيبرانية، الاستعداد للذكاء الاصطناعي وإنترنت الأشياء، بناء الدول المرنة، وتمكين الشباب والمواهب.

الحكومة

With the participation of the Cyber Security Council and the National Emergency Crisis and Disaster Management Authority (NCEMA), interactive cybersecurity dialogues and activities were launched at the UAE Pavilion during Expo 2025 Japan in Osaka. On the opening day, CSC and NCEMA hosted a series of sessions and activities focused on cybersecurity and emerging digital threats, aimed at enhancing international knowledge exchange and showcasing Emirati innovations in cybersecurity and crisis management. The program included sessions on cyber diplomacy, AI and IoT readiness, building resilient nations, and empowering youth and cyber talent.

* Government

Expo Japan HE visit

قام سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، بزيارة إلى جناح جناح الإمارات المشارك في معرض "إكسبو 2025 أوساكا" في اليابان، والذي يحمل شعار "من الأرض إلى الأثير"، كما زار سعادته عدداً من الأجنحة المشاركة في المعرض. واطّلع سعادته على أبرز ما يقدمه الجناح من محتوى يعكس الرؤية المستقبلية لدولة الإمارات، ومساهمتها العالمية في مجالات الاستدامة، والصحة، والتكنولوجيا، والفضاء، بالإضافة إلى استعراض إنجازات الدولة ودورها في تعزيز التقدم المشترك، وتمكين الأفراد من خلال البحث العلمي، والابتكار، وتفعيل دور الشباب. وأشاد سعادته بالإمكانات الكبيرة التي يوفرها المعرض حيث يستقبل هذا الحدث العالمي نحو 158 دولة ومنطقة إلى جانب 7 منظمات دولية،

الحكومة

Expo Japan HE visit EN

H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, visited the UAE Pavilion at Expo 2025 Osaka, held under the theme *‘From Earth to Ether.’* He was briefed on the pavilion’s highlights, which reflect the UAE’s forward-looking vision and global contributions in sustainability, health, technology, and space, as well as its achievements in research, innovation, and youth empowerment. Dr. Al Kuwaiti praised the distinguished efforts behind the pavilion’s presentation and noted the importance of Expo Osaka 2025, which hosts 158 countries and seven international organizations.

CSC&NECMA expo Japan.

استمرت الفعاليات التي ينظمها مجلس الأمن السيبراني بالتعاون مع الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث NCEMA خلال فعاليات جناح الدولة بمعرض "إكسبو اليابان 2025" في أوساكا - اليابان، عبر مجموعة من الجلسات النقاشية والأنشطة التفاعلية تناولت الأمن السيبراني والتهديدات الرقمية بهدف تعزيز تبادل الخبرات والمعلومات على المستوى الدولي حول قضايا الأمن السيبراني والتهديدات الرقمية المتسارعة إضافة إلى بحث سبل تعزيز الاستجابة للأزمات المحتملة. واستضاف مجلس الأمن السيبراني والهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث NCEMA بجناح الدولة سلسلة من الجلسات بمشاركة وفود دولية ومجموعة من الخبراء والمتخصصين في الأمن السيبراني.

الحكومة

CSC&NECMA expo Japan EN

The Cyber Security Council, in collaboration with the National Emergency Crisis and Disaster Management Authority (NCEMA), continued its activities at the UAE Pavilion during Expo 2025 Japan in Osaka. The program featured panel discussions and interactive sessions on cybersecurity and digital threats, aimed at strengthening international knowledge exchange and exploring strategies to enhance readiness for potential crises. The sessions brought together international delegations, experts, and specialists to discuss emerging challenges and opportunities in cybersecurity.

Japan, Financial conference

شملت أنشطة مجلس الأمن السيبراني خلال اليوم الثاني من مشاركته في فعاليات معرض إكسبو أوساكا 2025 ، المشاركة في المنتدي المالي متعدد الأطراف والذي جمع عدداً من الشخصيات من اليابان والولايات المتحدة والشرق الأوسط، وركز المنتدى على استكشاف فرص الاستثمار وبناء جسور تعاون جديدة بين مختلف الأطراف الفاعلة، مع مشاركة عدد من الشخصيات البارزة في مجال الأمن السيبراني في الجلسة النقاشية. بالتوازي مع ذلك، شارك المجلس في المنتدى المالي السيبراني متعدد الأطراف وتضمن المنتدى مسارين رئيسيين: "المنتدى المالي السيبراني" و"منتدى الميناء السيبراني"، حيث اجتمع كبار صناع السياسات وخبراء الأمن السيبراني لمناقشة تحديات الأمن السيبراني، وتبادل الدروس المستفادة.

الحكومة

Japan, Financial conference EN

The Cyber Security Council continued its participation at Expo 2025 Osaka with a series of forums and dialogue sessions. On the second day, the Council took part in the Multilateral Finance Forum, which brought together leading figures from Japan, the United States, and the Middle East to explore investment opportunities and build new avenues of cooperation. The Council also joined the Multilateral Cyber Finance Forum, which featured two tracks, the Cyber Finance Forum and the Cyber Port Forum, where senior policymakers and cybersecurity experts discussed challenges, shared lessons, and exchanged insights on strengthening international collaboration.

Government

Expo Japan - Third day

شارك مجلس الأمن السيبراني في فعاليات المؤتمر العالمي للأمن السيبراني "سايبرتك طوكيو 2025" في العاصمة اليابانية، حيث تناولت الجلسات التحديات والفرص في حماية الفضاء الرقمي عالميًا.كما شارك المجلس في جلستين رئيسيتين ركزت الأولى على الأمن السيبراني لقطاع الموانئ والأمن البحري، فيما ناقشت الثانية تعزيز التعاون الدولي وبناء شراكات لمكافحة الجرائم الإلكترونية وتبادل المعلومات حول التهديدات السيبرانية.

وعلى هامش المؤتمر، عقد المجلس جلسات ثنائية رفيعة المستوى مع وزارة الخزانة الأمريكية، والجانب الياباني، والهندي لمناقشة التعاون في الأمن السيبراني المالي، وحماية البنى التحتية الحيوية، وتبادل الخبرات لتعزيز الحوكمة الرقمية وبناء منظومة أمنية عالمية متكاملة.

الحكومة

Expo Japan - Third day EN

The Cyber Security Council participated in the Global Cybersecurity Conference “Cybertech Tokyo 2025” in the Japanese capital, where sessions addressed global challenges and opportunities in protecting the digital space. The Council also took part in two main sessions, the first focusing on cybersecurity for ports and maritime security, while the second discussed enhancing international cooperation and building partnerships to combat cybercrime and exchange threat intelligence.

On the sidelines of the conference, the Council held high-level bilateral meetings with delegations from the United States, Japan, and India to discuss collaboration in financial cybersecurity, critical infrastructure protection, and knowledge sharing to strengthen global digital governance.

Government

Cyber Pulse Tenth week

في إطار الحملة الأسبوعية التوعوية لمبادرة "النبض السيبراني" التي أطلقها مجلس الأمن السيبراني، ناقش الأسبوع الرابع من الحملة التهديدات التي تواجه المنازل الذكية. وتستمر الحملة على مدار 52 أسبوعاً، مقدمة برامج وإرشادات توعوية للأفراد والمؤسسات، بهدف زيادة الوعي السيبراني وتعزيز المرونة والثقافة الرقمية، مع تقديم إرشادات عملية لمواجهة التهديدات السيبرانية المختلف.ركز الأسبوع الرابع على تزايد الهجمات الإلكترونية التي تستهدف المنازل الذكية، مع تسليط الضوء على المخاطر المرتبطة باستخدام أجهزة مراقبة الأطفال.

الأفراد والعائلات

الشركات

Cyber Pulse Tenth week EN

As part of the weekly *Cyber Pulse* awareness campaign launched by the Cyber Security Council, the 4th week addressed the threats facing smart homes. The campaign, which runs across 52 weeks, delivers awareness programs and guidance for individuals and institutions, aiming to increase cyber awareness, strengthen resilience, and promote digital culture through practical tips on confronting cyber threats. The 4th week highlighted the growing cyberattacks targeting smart homes, with particular emphasis on the risks associated with baby monitoring devices.

Individuals & Families  
Corporations

TDRA, CSC, and Meta

أطلقت شركة ميتا حملة "مكافحو الاحتيال"، بالتعاون مع هيئة تنظيم الاتصالات والحكومة الرقمية (تدرا) ومجلس الأمن السيبراني، بهدف رفع الوعي بالمخاطر السيبرانية المتزايدة مع التركيز على عمليات الاحتيال الإلكترونية، وتعريف مستخدمي الإنترنت بأنواعها وكيفية تحديدها، والأدوات المتاحة للإبلاغ عنها وحظرها، بما يسهم في ترسيخ ثقافة الإنترنت الآمن. وتستمر هذه الحملة على مدار الشهرين القادمين، وتُعد جزءًا من الجهود المشتركة لتثقيف المواطنين والمقيمين في دولة الإمارات حول المخاطر والتهديدات الإلكترونية لا سيما تزايد عمليات الاحتيال الإلكتروني من حيث الحجم والتعقيد، مدفوعة بشبكات إجرامية عابرة للحدود تستخدم مخططات متطورة لاستهداف الأشخاص عبر الإنترنت.

الأفراد والعائلات

الشركات

TDRA CSC &META EN

Meta, in cooperation with the Telecommunications and Digital Government Regulatory Authority (TDRA) and the Cyber Security Council, launched the *“Scambusters”* campaign to raise awareness of growing cyber risks, with a focus on online fraud. The initiative aims to educate internet users on different types of scams, how to identify them, and the tools available to report and block them, thereby promoting a safe online culture. The campaign will run for two months as part of joint efforts to protect citizens and residents from digital threats driven by increasingly complex, cross-border criminal networks.

**Individuals & Families  
Corporations**

Majaliss Abu Dhabi

نظمت مجالس أبوظبي جلسة نقاشية رفيعة المستوى بعنوان "الأسرة والتصدي للرسائل الخبيثة" في مجلس الطوية، بالتعاون مع مجلس الأمن السيبراني، وقدمها سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات. تأتي الجلسة ضمن سلسلة لقاءات مجتمعية تهدف لتعزيز الوعي الرقمي وحماية الأسرة من التهديدات السيبرانية المتزايدة.

تركز المناقشات على دور الأسرة في مواجهة الرسائل الخبيثة التي تنتشر عبر المنصات الرقمية ووسائل التواصل الاجتماعي، وتستهدف اختراق الأجهزة وسرقة البيانات. كما تناقش كيفية توعية الأبناء وتوجيههم لتجنب الروابط المزيفة والخسائر المالية والمعلوماتية الناتجة عن الاحتيال السيبراني.

الأفراد والعائلات

Majaliss Abu Dhabi EN

Majalis Abu Dhabi, in collaboration with the Cyber Security Council, organized a high-level discussion session at Al Tiwayya Majlis under the title *‘The Family and the Fight Against Malicious Messages.’*  Led by H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, the session highlighted the role of families in protecting children and society from the risks of fraudulent digital messages that spread across platforms and social media to steal data or cause financial loss.

**Individuals & Families**

CyberQ Announcement AR + EN

أعلن مجلس الأمن السيبراني عن انعقاد النسخة الثانية مؤتمر "سايبركيو" خلال شهر نوفمبر المقبل، وتأتي نسخة هذا العام من المؤتمر، الذي يعتبر أحد أبرز الأحداث على مستوى الأمن السيبراني في منطقة الشرق الأوسط، تحت شعار "حين يلتقي الكم والذكاء الاصطناعي والأمن السيبراني" وذلك يومي 26 و27 نوفمبر المقبل في مركز أدنيك أبوظبي. وسيجمع الحدث خبراء وصنّاع قرار وقادة من قطاعات مختلفة يمثلون أكثر من 100 دولة، لمناقشة التأثير التحويلي للحوسبة الكمومية والذكاء الاصطناعي على الأمن السيبراني، وستتطرق الجلسات إلى الهجمات المدعومة بالذكاء الاصطناعي، وأتمتة الدفاعات، والحاجة الملحة للانتقال إلى تقنيات ما بعد الكم. كما سيسلط المؤتمر الضوء على التقدم في مجال التشفير الكمومي، والمعايير الدولية، والمخاطر الناشئة مثل الجريمة السيبرانية المنظمة.

الحكومة

The Cyber Security Council announced the 2nd edition of the *CyberQ Conference*, set to take place on 26–27 November at ADNEC, Abu Dhabi, under the theme *“Where Quantum, AI, and Cybersecurity Converge.”* The conference will bring together experts, decision-makers, and leaders from more than 100 countries to discuss the transformative impact of quantum computing and artificial intelligence on cybersecurity. Sessions will cover AI-driven attacks, automated defenses, and the urgent shift toward post-quantum technologies, alongside progress in quantum cryptography, international standards, and emerging risks such as organized cybercrime.

**Government**

Billington Cyber Summit AR + EN

شارك مجلس الأمن السيبراني برئاسة سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، في فعاليات الدورة السادسة عشرة لقمة بيلينغتون للأمن السيبراني في واشنطن، تحت عنوان "حدود الأمن السيبراني والذكاء الاصطناعي: استراتيجيات لحكومة أكثر أمانًا وذكاءً. وشارك المجلس في جلسة رئيسية بعنوان "تأمين المستقبل - الذكاء الاصطناعي، والمرونة السيبرانية، والابتكار العالمي" حول تأثير الذكاء الاصطناعي والأتمتة على مشهد الأمن السيبراني العالمي والقدرات الدفاعية والهجومية المتطورة. وعلى هامش القمة، عقد سعادة الدكتور الكويتي لقاءات مع مسؤولين أمريكيين من وزارة الخزانة وقادة شركات عالمية لمناقشة تعزيز التعاون الدولي في الأمن السيبراني.

الحكومة

The Cyber Security Council, led by His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, participated in the 16th edition of the Billington Cybersecurity Summit in Washington, D.C., held under the theme *“Cyber and AI Frontiers: Strategies for a Secure and Smarter Government.”*

The Council took part in a main session titled *“Securing the Future – AI, Cyber Resilience, and Global Innovation,”* which explored the impact of artificial intelligence and automation on the global cybersecurity landscape. On the sidelines, Dr. Al Kuwaiti also held high-level meetings with senior U.S. officials from the Department of the Treasury and global technology leaders to discuss strengthening international cooperation in financial cybersecurity, safeguarding critical infrastructure, and advancing joint initiatives.

**Government**

HE Speech first week AR + EN

في مقاله "منازل ذكية.. ولكن!"، يسلط الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات الضوء على انتشار المنازل الذكية وأثرها في حياتنا اليومية، حيث توفر الراحة وتسهّل المهام المختلفة، لكنها تطرح تحديات كبيرة تتعلق بأمن البيانات والمعلومات. يشير المقال إلى أن اعتماد الأجهزة الذكية في المنازل يتيح جمع ونقل كميات كبيرة من البيانات الشخصية، ما يزيد من خطر الاستغلال السيبراني. ويحذر سعادة الدكتور الكويتي من أن عدم معرفة المستخدمين بالطرق الآمنة للتعامل مع هذه الأجهزة يجعلهم عرضة لاختراق الخصوصية وسرقة البيانات المالية والشخصية، مؤكدًا أهمية التوعية والاحتياطات الرقمية لضمان حماية الأفراد والمجتمع.

الأفراد والعائلات

الشركات

In his article *‘Smart Homes… But!’*, His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, highlights the growing reliance on smart homes and their role in providing convenience and efficiency in daily life. He warns, however, that these devices collect and transmit large amounts of personal data, creating serious risks of cyber exploitation. Dr. Al Kuwaiti cautions that limited user awareness of safe practices makes individuals vulnerable to privacy breaches and the theft of financial and personal information, stressing the importance of digital awareness and protective measures to safeguard both individuals and society.

Individuals & Families  
Corporations

Weekly Campaign AR+EN

في إطار الحملة الأسبوعية لمبادرة "النبض السيبراني"، حذّر مجلس الأمن السيبراني من تجاهل حماية الاجتماعات عبر تطبيقات المشاركة وتأمين استخدام الكاميرا، خاصة اجتماعات العمل عن بُعد، داعيًا لتفعيل خاصية "غرفة الانتظار" وعدم منح التطبيقات الوصول المباشر للكاميرا. وتشمل الحملة برامج وإرشادات توعوية أسبوعية لتعزيز الوعي بالمخاطر السيبرانية وطرق الوقاية، بما في ذلك استخدام شبكات VPN، تحديث الأجهزة تلقائياً، والتأكد من برامج الحماية. كما شدّد المجلس على اليقظة عند استخدام الكاميرات في الاجتماعات الحكومية والخاصة، الدروس التعليمية، والألعاب الإلكترونية لضمان حماية البيانات والخصوصية الرقمية.

الأفراد والعائلات

الشركات

As part of the weekly awareness campaign of the *Cyber Pulse* initiative, the Cyber Security Council warned against neglecting to secure meetings held through collaboration applications, and stressed the importance of securing the use of cameras during online and virtual meetings, particularly remote work sessions. The Council stressed the importance of activating the “waiting room” feature and avoiding granting applications direct access to the camera. The campaign, which delivers weekly programs and awareness guidelines, also highlighted the need to use VPNs, enable automatic updates, and verify security software. CSC emphasized the importance of remaining vigilant when using cameras in government and private meetings, virtual classrooms, and electronic games to safeguard data and privacy.

**Individuals & Families  
Corporations**

HE Speech 2 week AR + EN

في مقاله "الاجتماعات الافتراضية: كيف تحمي خصوصية أعمالك؟"، أكد سعادة الدكتور محمد الكويتي، رئيس الأمن السيبراني لحكومة دولة الإمارات، أن المخاطر السيبرانية الناتجة عن إهمال تأمين الاجتماعات الافتراضية والتطبيقات التشاركية أصبحت تهديداً متزايداً في العصر الرقمي، خاصة مع الاستخدام اليومي للتقنيات الحديثة في العمل والحياة الشخصية. وأوضح أن عدم اتخاذ التدابير الوقائية يعرض البيانات الحساسة والخطط الاستراتيجية للاختراق وسرقة المعلومات. وشدد على أن حماية الاجتماعات الافتراضية مسؤولية مشتركة بين المؤسسات والأفراد، وأن الوعي والتدابير الوقائية واستراتيجيات الأمان المحدثة ضرورية للحد من المخاطر، وضمان بيئة رقمية آمنة، تحافظ على الخصوصية والأمان الإلكتروني في ظل الاعتماد المتزايد على التكنولوجيا.

الأفراد والعائلات

الشركات

**In his article ‘Virtual Meetings: How to Protect Your Business Privacy?’, H.E. Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, stressed that the cyber risks resulting from neglecting the security of virtual meetings and collaboration applications have become an increasing threat in the digital age, particularly with the daily reliance on modern technologies in both work and personal life. He explained that failing to adopt preventive measures exposes sensitive data and strategic plans to breaches and information theft. Dr. Al Kuwaiti emphasized that safeguarding virtual meetings is a shared responsibility between institutions and individuals, highlighting that awareness, preventive measures, and updated security strategies are essential to mitigate risks and ensure a secure digital environment that preserves privacy and cybersecurity amid growing dependence on technology.**

**Individuals & Families  
Corporations**

Information security

شدّد مجلس الأمن السيبراني على أهمية أن تعزز المؤسسات قدراتها السيبرانية، وتلتزم بالمعايير الرشيدة، وتضع الأمان في صميم التخطيط الاستراتيجي لضمان استمرارية الخدمات وحماية البيانات. ولقت الى أن التهديدات السيبرانية المتزايدة على القطاعات الحكومية والخاصة والحيوية تجعل الأمن السيبراني ضرورة وجودية، وليس رفاهية، حيث يؤدي الإهمال إلى خسائر مادية وبشرية وفقدان الثقة وتعطيل الخدمات الأساسية. وأشار إلى أن تسارع الهجمات نتيجة الاعتماد الكبير على الخدمات الرقمية والتقنيات المتصلة بالإنترنت، مثل المصرفية الرقمية وأنظمة التحكم عن بُعد للطاقة، يجعل هذه الأنظمة أكثر عرضة للاختراق.

الشركات

The Cyber Security Council stressed the importance of strengthening institutional cyber capabilities, adhering to recognized standards, and integrating security into strategic planning to ensure service continuity and data protection. The Council emphasized that with cyber threats increasingly targeting government, private, and critical sectors, cybersecurity has become a necessity rather than an option. Negligence, it warned, can result in financial and human losses, erosion of trust, and disruption of essential services.It further noted that the rapid escalation of attacks, driven by heavy reliance on digital services and internet-connected technologies such as online banking and remote energy control systems, has made these sectors more vulnerable to breaches.

Corporations