

خبراء: حماية النظام المالي من الهجمات السيبرانية أولوية قصوى



«دبي:» الخليج

أكد خبراء في القطاع المصرفي أن اعتماد معايير الأمن السيبراني للجهات الحكومية يرسخ التعامل الآمن مع البيانات في المجتمع، ويشجّع القطاع الخاص على التماهي مع هذه المعايير والاستثمار في المشاريع التكنولوجية والتحول الرقمي.

جاء ذلك خلال جلسة نقاشية استضافها معهد الإمارات للدراسات المصرفية والمالية، بهدف تقييم تحديات الأمن السيبراني التي قد تواجه المؤسسات والخدمات المالية في الإمارات، وأهمية اتخاذ خطوات استباقية لحماية الشركات من الهجمات السيبرانية.

وتأتي الندوة الإلكترونية التي أقيمت بعنوان «تحديات الأمن السيبراني وحماية الثورة الرقمية» في إطار مبادرة المعهد للتعلم من الحوارات والتي تهدف إلى استضافة حوارات دورية تغطي مواضيع الصيرفة والأمور المالية، سعياً إلى

التواصل مع أفراد المجتمع

شارك في الجلسة أكثر من 100 خبير في المؤسسات العالمية والإقليمية، مثل برافين فاكايل، مدير أول في «برايز ووترس هاوس كوبرز» الشرق الأوسط، وشيخ شذب نواز، مدير في شركة «كيه بي إم جي»، وجاياكاران بول، نائب في Cyberfort Digisec الرئيس الأول ومدير الأمن السيبراني في بنك أبوظبي الأول، وأدارها شاندران إس، مدير حلول الهند.

وسلط المتحدثون خلال الجلسة الضوء على التحديات الناشئة بسبب الثورة الرقمية المستمرة التي تتصف ببروز التقنيات الحديثة، مثل الحكومة الإلكترونية والتجارة الإلكترونية، والبلوكتشين، وخدمات الدفع عبر الموبايل، والصيرفة الإلكترونية، والحوسبة السحابية، وغيرها.

وقال جمال الجسمي، مدير عام معهد الإمارات للدراسات المصرفية والمالية: «نهدف من خلال هذه الندوة القيّمة إلى مساعدة المشاركين في الخدمات المالية في فهم واتخاذ خطوات استباقية لتعزيز الأمن السيبراني بما يتماشى مع استراتيجيات ومبادرات حكومة الإمارات التي تهدف إلى إنشاء بنية تحتية إلكترونية آمنة وقوية لتمكين الأفراد والشركات في الدولة

وأضاف: «سلطت الندوة الضوء على تحديات الأمن السيبراني التي تواجه مزودي الخدمات المالية حالياً، وطرق التغلب عليها. إذ يعتبر الأمن السيبراني مسؤولية مشتركة، ويساهم المعهد في تطوير عدد من البرامج التي تناقش مخاطر الأمن السيبراني في القطاع المصرفي وتتراوح بين الدورات المتوسطة إلى الدورات الأكثر تخصصاً. ونأمل أن يكون المشاركون استفادوا من المعلومات والرؤى الهامة خلال الجلسة