النشرة الفنية لورشة عمل،

الأمن السيبراني :مفتاحك لمستقبل آمن

Cybersecurity: You're Key to a Secure Future

يوم، 4 ساعات

تبدأ بتاريخ 2024/5/18م

تدريب إلكتروني

06 - 5522807
info@aljhood.com
www.aljhood.com
jordan amman queen rania st building.155

بطاقة معلومات الورشة :

مدة التدريب	:	يوم واحد، (4) ساعات
نمط التدريب	:	تدريب إلكتروني - **Live**
تاريخ الانعقاد	:	2024/05/18م
توقيت التدريب	:	pm 12:00 - pm 04:00
شهادة التدريب	:	شهادة الكترونية صادرة من مجموعة الجهود المشتركة "بنسبة الحضور لاتقل عن 90%"
لغة التدريب	:	اللغة العربية مع بعض المصطلحات الفنية باللغة الإنجليزية
أساليب التدريب	:	– إسلوب العصف الذهني. – إسلوب السيناريوهات والحلول. – إسلوب تقديم الحلول والممارسات. – أسلوب تبادل الأفكار والتجارب في العمل.
الفئة المستهدفة	:	– العاملين في إدارة تكنولوجيا المعلومات . – مدراء ومشرفين ادارة امن المعلومات. – العاملين في إدارة مراقبة أمن المعلومات. – العاملين في إدارات تدقيق الأمن السيبراني . – جميع العاملين في المؤسسات الذين يستخدمون التكنولوجيا.

الأمن السيبراني : مفتاحك للمستقبل

الأمن المعلوماتي أصبح أمراً ضرورياً في جميع دول العالم لاسيما في ظل ما يشهده العالم حالياً من نمو سريع ومتزايد في أعداد مستخدمي الأجهزة والنظم الذكية، وتزايد الهجمات الإلكترونية المتعددة، وهو ما يفرض علينا جميعاً ضرورة التعامل معها ومواجهتها، في وقت أن دول المنطقة أجمع تتسابق لإحتلال مكانة متقدمة في مؤشرات الأمن السيبراني والعديد من المؤشرات الأخرى المرتبطة بصورة مباشرة أو غير مباشرة بالأمن المعلوماتي.

وحيث يعد الأمن السيبراني جزءًا مهمًا من الأمن في البلدان اليوم وهو يقوم على حماية البنية التحتية المعلوماتية لدولة ما ، والتي تشمل مرافق مهمة وأنظمة مهمة تدير مؤسسات الدولة المهمة ، مثل الحكومة. وحيث يمكن أن تشكل تهديدات الأمن السيبراني تهديدًا للأمن القومي لأي بلد ، لذلك أعدت العديد من الدول هيئات للتخصص في الأمن السيبراني تم تسخير جميع القدرات للأمن السيبراني ، وهو أحد المعايير المستخدمة لقياس مستوى الجاهزية السيبرانية لدولة ما مثل الاتحاد الدولي للاتصالات (ITU) لديها مؤشر يقيس مدى استعداد الدولة للتعامل مع التهديدات السيبرانية.

وحيث يزيد التحول الرقمي من مخاطر أمن تكنولوجيا المعلومات، ولتحقيق مزايا تنافسية والحفاظ على ولاء العملاء والشركاء يجب على المنظمة حماية استمرارية الأعمال وتنفيذ حماية موثوقة للأصول الهامة وبيانات المنظمة والبنية

المملكة العربية السعودية –حي المرسلات – طريق ابو بكر الصديق –الموقع الالكتروني: www.aljhood.com

التحتية لتكنولوجيا المعلومات بالكامل، هذا يعني نقل إستراتيجية أمان تكنولوجيا المعلومات الخاصة بالمنظمة إلى مستوى جديد ، ويتطلب ذلك الوقوف في برنامج فعّال للبحث عن التهديدات موارد بشرية ماهرة مقترنة بالأدوات والبيانات المناسبة، لكن هذا ليس بالمهمة السهلة، وقد لا تكون متأكداً من كيفية البدء، ومن خلالها سيتعلم المشاركون اللبنات الأساسية للامن السيبراني والتعرف بأكثر التهديدات السيبرانية تداولا وطرق التعامل معها للحصول على مستقبل آمن.

هدف ورشة العمل:

تهدف ورشة العمل على المام المتدربين لماهية الأمن السيبراني ومحاوره، إضافة إلى الحديث حول إدارة مخاطره، وآليات المراقبة والتقييم وبناء سجلات مخاطر الأمن السيبراني، وتقييم مستوى النضوج والتدقيق والرقابة على مواضيع الأمن السيبراني، كما سيتم مناقشة الأطر التنظيمية والتشريعية والرقابية العالمية والمحلية للأمن السيبراني وحوكمة البيانات، وستطرق ورشة العمل الى أهم التعليمات والممارسات الدولية في المنطقة الخاصة بالأمن السيبراني والحماية من الهجمات أيضا استعراض بعض التشريعات في المؤسسات بهدف تطوير البيئة الإلكترونية والرقمية والمحافظة عليها وتعزيز أمن المعلومات بشكل عام والأمن السيبراني بشكل خاص.

المواضيع الرئيسية للورشة:

- الرقمنة والأمن السيبراني.
- قواعد الأمن السيبراني في المؤسسات.
- الأمن السيبراني و محاوره و الحماية القانونية له.
- الجهود الدولية و الوطنية لحماية الأمن السيبراني.
- الحروب السيبرانية و الهجمات الموجهة لنظم المعلومات.
- مهددات الأمن السيبراني في المؤسسات الصناعية و الحيوية.
- آليات المراقبة والتقييم وبناء سجلات مخاطر الأمن السيبراني.
- أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات في المؤسسة.
- حماية الأصول الرقمية وهوية المؤسسة والتكيف والمخاطر السيبرانية.
- الأطر التنظيمية والتشريعية والرقابية العالمية والمحلية للأمن السيبراني وحوكمة البيانات.
- التعليمات والممارسات الدولية في المنطقة الخاصة بالأمن السيبراني والحماية من الهجمات.

إنتهت النشرة الفنية،

المملكة العربية السعودية –حي المرسلات – طريق ابو بكر الصديق –الموقع الالكتروني: www.aljhood.com