النشرة الفنية لورشة عمل،

الأمن السيبراني والهندسة الإجتماعية

يوم، 3 ساعات

تبدأ بتاريخ 2023/02/25م

تدريب إلكتروني... Live

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

بطاقة معلومات الورشة:

مدة التدريب	:	يوم واحد، (3) ساعات
نمط التدريب	:	تدريب إلكتروني - **Live**
تاريخ الانعقاد	:	2023/02/25م
توقيت التدريب	:	12:00 ظهراً لغاية 03:00 مساءً
شهادة التدريب	:	شهادة الكترونية صادرة من مجموعة الجهود المشتركة
لغة التدريب	:	اللغة العربية مع بعض المصطلحات الفنية باللغة الإنجليزية

أساليب التدريب	:	– إسلوب العصف الذهني. – إسلوب السيناريوهات والحلول. – إسلوب حالات من واقع عمل المشاركين.

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.

الامن السيبراني والثورة التكنولوجية:

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.

يتطور التهديد السيبراني العالمي بوتيرة سريعة مع تزايد عدد خروقات البيانات كل عام؛ حيث قُدرت سرقة بيانات 7.9 مليار سجل عن طريق خروقات البيانات في الأشهر التسعة الأولى من عام 2019 وحده، وهو أكثر من ضعف عدد السجلات التي تم الكشف عنها في نفس الفترة من عام 2018، وتتوقع مؤسسة البيانات الدولية أن الإنفاق العالمي على حلول الأمن السيبراني سيصل إلى 133.7 مليار دولار بحلول عام 2022م.

كما 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 التحتية لتكنولوجيا المعلومات بالكامل، هذا يعني نقل إستراتيجية أمن تكنولوجيا المعلومات الخاصة بالمنظمة إلى مستوى جديد.

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com

الهندسة الإجتماعية:

نعيش الان في عصر التطور التكنولوجي حيث تدخل التكنولوجيا في جميع مجالات حياتنا، فالتقنية أصبحت جزءاً هاماً لا يستغنى عنه في نسيج الحياة، لما تقدمه من تسيير وتيسير مهام ووظائف حياتنا اليومية، ويشهد هذا العصر ثورة تكنولوجية تحمل معها العديد من السلبيات والإيجابيات للفرد والمجتمع، لقد أصبحت الهندسة الإجتماعية مفهوم منتشر نظراً للنمو الهائل لشبكات التواصل الإجتماعي، وأصبح هذا المصطلح مستخدماً على نطاق واسع في مجال أمن المعلومات للإشارة الى مجموعة من الأساليب التي يتم إستخدامها في الحصول على المعلومات الدقيقة والحساسة أو اقناع الضحايا المستهدفة بتنفيذ بعض الإجراءات التي تساعد على إختراق انظمتهم والإضرار بها.

الهندسة الاجتماعية، وكما يسميها الكثير "فن اختراق العقول"، وهي مجموعة من العمليات الاحتيالية التي تقتضي بتوجيه بعض التقنيات الهجومية لدفع الضحية إلى البوح بمعلومات سرية، وبالتالي اختراق الخصوصيات والمعلومات التي يفترض أنها محمية، أو يجب عدم الإفصاح عنها لأشخاص غرباء قد يكونوا منافسين أو عابثين، والإفصاح عنها أو تعرضها للسرقة أو الاختراق بطرق احتيالية يعد خطراً وتهديداً على أمن معلومات الأفراد والمؤسسات والشركات، وهذا النمط من الاحتيال يقوم على مبدأ استغلال نقاط الضعف في ذهن الضحية بالهندسة الاجتماعية، والتي تجعل من الأشخاص ومستخدمي الشبكة العنكبوتية وتطبيقاتها يقعون بشكل لا إرادي في فخها.

وهي مهارة استخدام الأساليب الكلامية أو النفسية الإيحائية أو الإعلانية لتوجيه عقل وتفكير الضحية إلى ما يريد الجاني والاستفادة أكبر قدر منه والحصول على معلومات وبيانات سرية دون أن يشعر وبرضا تام منه. أما في عالم التقنية والحواسيب، فالهندسة الاجتماعية تعرف بأنها عبارة عن مجموعة من التقنيات المستخدمة لجعل المستخدم يقوم بعمل ما أو الإفصاح عن معلومات سرية عن حساباته الإلكترونية، أو البيانات المتعلقة بحساباته البنكية لتحقيق الغرض المنشود من الضحية.

هناك العديد من أساليب الهندسة الاجتماعية (الاحتيال) التي يعتمد عليها المهاجمون لإيقاع ضحاياهم، ولا يمكن حصرها لأن المهاجمون يفكرون أيضاً بشكل مستمر بأساليب جديدة ومبتكرة لخداع الضحايا. ومن ابرز الأساليب الشائعة؛ استغلال العواطف، فضول المستهدف، بحث المستهدف عن علاقات مشروعة أو غير مشروعة إلى غيرها من الأساليب المبتكرة التي تهدف إلى استدراج الضحية للقيام بما يريد منه المهاجم كتنزيل برمجيات خبيثة أو إعطاء بيانات شخصية كاسمه وموقع سكنه وحتى صورته أو بيانات حسابات تطبيقات التواصل الاجتماعي ورقم هاتفه...وغيرها، وقد يؤدي ذلك إلى ابتزازه إلكترونيا في وقت لاحق، خاصة إذا ما تم تهديده بفضح بياناته أو نشرها.

ملخص ورشة العمل:

في ظل التحول الرقمي وارتفاع نسبة الاعتماد على الإنترنت في حياتنا، أصبح من الضروري الانتباه للأمن السيبراني وكيفية حماية أنفسنا من الاختراق في الفضاء الرقمي، لذا تعقد الجهود ورشة عمل حول الأمن السيبراني والهندسة الإجتماعية، إذ تهدف الورشة إلى توعية المشاركين بمهارات حماية الأنظمة وتقنيات الاختراق وكيفية تصديها، ويتم ذلك من خلال عرض الأفكار ومناقشتها وإعطاء الفرصة للمشاركين بذكر آرائهم الخاصة.

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com

حيث ستركز ورشة العمل على استخدامات الهندسة الاجتماعية بالأنشطة والهجمات الإجرامية أو الاحتيالية على شبكة الانترنت، بما في ذلك انتحال الهوية كنتيجة شائعة لهذه الأنواع من الهجمات وفي كثير من الحالات يؤدي إلى خسائر مالية كبيرة،كما ستناقش الورشة كيف تعتمد جميع أنواع تقنيات الهندسة الاجتماعية على نقاط ضعف علم النفس البشري من خلال استغلال المحتالين لعواطف الناس مثل الخوف والجشع والفضول، ودفعهم للتصرف وفق أهواء المخترقين من خلال رسائل البريد الإلكتروني، والبرامج الخبيثة، واستبيانات الرأي واختبارات الترفيه وغيرها من أساليب إغراء المستخدمين للكشف عن معلوماتهم الخاصة.

ومن خلال ورشة العمل سيتم تعريف المشاركين بأهمية الامن السيبراني والهندسة الاجتماعية والياتها وأساليبها والإختراق وأساليبه وبالتالي تزويدهم بالمهارات اللازمة التي تحميهم من الإختراق وعدم الوقوع في براثن شباكه الخبيثة، إضافة إلى معرفة الدور الأخلاقي والمدونات السلوكية ذات الصلة وتفعيل العمل وفق منظومة قيم العمل الأخلاقي.

لذا تنبع أهمية عقد ورشة الأمن السيبراني والهندسة الإجتماعية من أهمية موضوع الأمن السيبراني على المستويين المحلي والدولي، من خلال متطلبات الحماية والضوابط الواجب توفيرها على المستوى الفردي من خلال حماية البيانات الشخصية والصور والملفات الخاصة بالأفراد والمنظمات، وعلى مستوى الشركات والمؤسسات، من خلال حماية الأصول الإلكترونية والبيانات والمعلومات وبيانات الموظفين والمواقع الإلكترونية والبرمجيات والبنية التحتية الإلكترونية العاملة لديها، وعلى مستوى الدولة عن طريق حماية أمنها الإلكتروني وحماية الأنظمة المالية والإقتصادية والعسكرية من الهجمات الإلكترونية والقرصنة والتعطيل.

المواضيع الرئيسية لورشة العمل:

الموضوع (1): نهج ومفهوم الأمن السيبراني.

الموضوع (2): أدوات و تقنيات الاختراق وطرق تصديها.

الموضوع (3): طبيعة الهجمات والتهديدات السيبرانية وأنواعها .

الموضوع (4): مفهوم وأهمية الهندسة الإجتماعية والية عملها.

الموضوع (5): سيكولوجية المهندس الإجتماعي.

الموضوع (6): مراحل الهجوم في الهندسة الاجتماعية وانواعها.

الموضوع (7): الأساليب التي يتم استخدامها في الهندسة الاجتماعية.

الموضوع (8): كيفية الحماية من الوقوع في فخ الهندسة الاجتماعية.

الموضوع (9): النماذج الفعالة في الامن السيبراني والهندسة الاجتماعية.

الموضوع (10): أساليب إكتشاف التهديدات والتحقيق فيها باسلوب الهندسة الإجتماعية.

إنتهت النشرة الفنية،

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com