مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

التوعية الأمنية للموظفين الحكوميين: بناء ثقافة الأمن السيبراني

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 20 – 24 / 4 / 2025.

مقدمة :

في ظل التطور التكنولوجي المتسارع والاعتماد المتزايد على الأنظمة الرقمية في العمل الحكومي، أصبحت التوعية الأمنية للموظفين ضرورة حتمية لحماية البيانات الحساسة والمعلومات السرية من الهجمات السيبرانية. لا يقتصر الأمن السيبراني على التقنيات والأدوات فحسب، بل يعتمد بشكل كبير على وعي وسلوك الموظفين، فهم يشكلون خط الدفاع الأول ضد التهديدات السيبرانية.

يهدف هذا البرنامج التدريبي إلى تعزيز الوعي الأمني لدى الموظفين الحكوميين وبناء ثقافة الأمن السيبراني في المؤسسات الحكومية. سيتم التركيز على تعريف الموظفين بالمخاطر والتهديدات السيبرانية، وتزويدهم بالمعرفة والمهارات اللازمة للتعامل معها، وتشجيعهم على تبني ممارسات أمنية سليمة في حياتهم اليومية وبيئة العمل.

أهداف الورشة:

- زيادة وعي الموظفين الحكوميين بالمخاطر والتهديدات السيبرانية.
- تعريف الموظفين بأنواع الهجمات السيبرانية الشائعة وكيفية التعرف عليها.
- تطوير مهارات الموظفين في حماية كلمات المرور والمعلومات الشخصية.
- تعزيز ممارسات الأمن السيبراني السليمة في استخدام البريد الإلكتروني ووسائل التواصل الاجتماعي.
- التعرف على أهمية تحديث البرامج والتطبيقات والأجهزة بانتظام.
- بناء ثقافة الأمن السيبراني في المؤسسات الحكومية.
- تشجيع الموظفين على الإبلاغ عن أي حوادث أو أنشطة مشبوهة

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى الأمن السيبراني

- مفهوم الأمن السيبراني وأهميته في حماية المؤسسات الحكومية.
- أنواع التهديدات السيبرانية الشائعة (مثل الفيروسات، البرمجيات الخبيثة، التصيد الاحتيالي، هجمات الفدية).
- تأثير الهجمات السيبرانية على الأفراد والمؤسسات.
- ورشة عمل: تحليل حالات واقعية لهجمات سيبرانية وتأثيرها.

اليوم التدريبي الثاني:

حماية كلمات المرور والمعلومات الشخصية

- أهمية استخدام كلمات مرور قوية وفريدة لكل حساب.
- طرق إنشاء وتذكر كلمات المرور القوية.
- أدوات إدارة كلمات المرور.
- حماية المعلومات الشخصية من السرقة وسوء الاستخدام.
- ورشة عمل: إنشاء كلمات مرور قوية وتطبيق أدوات إدارة كلمات المرور.

اليوم التدريبي الثالث:

الأمن السيبراني في البريد الإلكتروني ووسائل التواصل الاجتماعي

- التعرف على هجمات التصيد الاحتيالي (Phishing) وكيفية تجنبها.
- أفضل الممارسات في استخدام البريد الإلكتروني بشكل آمن.
- حماية الخصوصية على وسائل التواصل الاجتماعي.
- ورشة عمل: تحليل رسائل بريد إلكتروني مشبوهة وتطبيق ممارسات أمنية سليمة.

اليوم التدريبي الرابع:

تحديث البرامج والأجهزة

- أهمية تحديث البرامج والتطبيقات والأجهزة بانتظام.
- كيفية التحقق من وجود تحديثات وتثبيتها.
- مخاطر استخدام برامج وتطبيقات غير مُرخصة.
- ورشة عمل: التحقق من وجود تحديثات وتثبيتها على الأجهزة والبرامج.

اليوم التدريبي الخامس:

بناء ثقافة الأمن السيبراني

- أهمية بناء ثقافة الأمن السيبراني في المؤسسات الحكومية.
- دور القيادة في تعزيز الوعي الأمني.
- تشجيع الموظفين على الإبلاغ عن أي حوادث أو أنشطة مشبوهة.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.
- إعداد خطط عمل لتعزيز الأمن السيبراني في بيئة العمل.

أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.