MERCURY

دورة الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

دورة الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات

مقدمة:

في ظل التحول الرقمي المتسارع، أصبحت الحاجة إلى حماية المعلومات والأنظمة من التهديدات السيبرانية أمرًا بالغ الأهمية. تقدم هذه الدورة التدريبية في الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات، أساسًا متينًا في مفاهيم الأمن السيبراني للمبتدئين الراغبين في دخول هذا المجال الحيوي.

تهدف دورة الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات، إلى تعريف المشاركين بمخاطر التهديدات الإلكترونية وسبل الوقاية منها، مع التركيز على حماية الأنظمة والشبكات من الهجمات الشائعة. يتعرف المشاركون على المبادئ الأساسية في أمن المعلومات، وإدارة الوصول، وتقييم الثغرات الأمنية.

كما تتناول الدورة التدريبية في الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات، استراتيجيات بناء بيئة آمنة داخل المؤسسات الصغيرة والمتوسطة. تم تصميم الدورة بأسلوب عملي مبسط، يشمل أمثلة واقعية وتطبيقات مباشرة. سيكون لدى المتدربين القدرة على اتخاذ خطوات عملية لحماية بياناتهم ومؤسساتهم من المخاطر السيبرانية المتزايدة.

الفئات المستهدفة:

تستهدف دورة الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات، الفئات والمحترفين الذين يسعون للاكتساب المعرفة والمهارات:

- الراغبون في بدء مسار مهني في مجال الأمن السيبراني.
- موظفو الدعم الفني وتقنية المعلومات المبتدئون.
- طلاب وخريجو تخصصات الحاسب الآلي والشبكات.
- موظفو المؤسسات الصغيرة والمتوسطة.
- العاملون في إدارات تكنولوجيا المعلومات بدون خلفية أمنية.
- من يسعون لفهم أساسيات أمن المعلومات.
- مسؤولو قواعد البيانات الجدد.
- الأفراد المهتمون بحماية أجهزتهم الشخصية من الاختراقات.
- المستخدمون الراغبون في تعزيز وعيهم الرقمي.
- مسؤولو نظم يبدؤون في تطوير مهاراتهم الأمنية.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات:

- المعرفة بأساسيات أمن المعلومات والخصوصية.
- القدرة على التعرف على التهديدات السيبرانية.
- مهارة استخدام أدوات الحماية البسيطة.
- فهم كيفية تأمين الشبكات المحلية.
- تحليل بيانات الحوادث الأمنية البسيطة.
- تنفيذ سياسات أمنية مبدئية.
- توثيق الإجراءات الأمنية.
- التعاون ضمن فرق العمل لتطبيق الأمان.
- التفكير النقدي في مواجهة الحوادث السيبرانية.
- المساهمة في التوعية الأمنية بالمؤسسة.
- إعداد خطط استجابة مبدئية للطوارئ.
- الالتزام بالمعايير الأخلاقية في الأمن الرقمي.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

أهداف الدورة التدريبية:

في نهاية هذا البرنامج التدريبي في الأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات، سيكون المشاركون قادرين على:

- التعرف على مفاهيم الأمن السيبراني الأساسية.
- تحديد أنواع التهديدات الأمنية الرقمية الشائعة.
- التمييز بين مستويات التهديدات وأنواع الهجمات.
- تطبيق تقنيات الحماية الأساسية على الأجهزة والشبكات.
- تحليل نقاط الضعف والثغرات الشائعة في الأنظمة.
- إعداد سياسات أمنية بسيطة لحماية البيانات.
- تقييم الاحتياجات الأمنية داخل بيئات العمل الصغيرة.
- استخدام أدوات فحص الثغرات المجانية للمبتدئين.
- تطوير خطط استجابة أولية للحوادث الأمنية.
- تنفيذ بروتوكولات حماية كلمات المرور والمصادقة.
- بناء فهم شامل لتقنيات الجدران النارية والمضادات.
- مراجعة أفضل ممارسات استخدام البريد الإلكتروني الآمن.
- تعزيز مهارات التوعية الأمنية الشخصية والمهنية.
- اكتساب القدرة على دعم المستخدمين في بيئة العمل.
- توظيف معايير الأمان عند تثبيت البرامج والتطبيقات.
- تنظيم البيانات الحساسة داخل الأجهزة المكتبية والمحمولة.
- فهم مسؤوليات الأفراد في حماية بيانات المؤسسة.
- إعداد تقارير مبسطة حول المخاطر الأمنية المكتشفة.
- تطوير سلوكيات رقمية آمنة في بيئة الإنترنت.

محتوى الدورة التدريبية:

الوحدة الأولى: مقدمة في الأمن السيبراني:

- تعريف الأمن السيبراني وأهميته في العصر الرقمي.
- الفرق بين أمن المعلومات والأمن السيبراني.
- أنواع التهديدات السيبرانية الشائعة.
- مفاهيم الخصوصية والسرية والتوافر والنزاهة.
- دورة حياة التهديدات الأمنية.
- مفاهيم المصادقة وتحديد الهوية.
- نظرة عامة على الأدوار والمسؤوليات في أمن المعلومات.
- الاتجاهات العالمية في الأمن السيبراني.
- أهمية الوعي الأمني للمستخدمين النهائيين.

الوحدة الثانية: حماية الأنظمة والتطبيقات:

- مكونات النظام التي يجب تأمينها.
- إعدادات الأمان الأساسية لنظام التشغيل.
- حماية التطبيقات والبرمجيات من الاستغلال.
- التحديثات الأمنية ودورها في الحماية.
- إدارة صلاحيات المستخدمين على الأنظمة.
- تشفير البيانات المخزنة والمحولة.
- استخدام برامج مكافحة الفيروسات والجدران النارية.
- إعداد النسخ الاحتياطية المنتظمة.
- الحماية من البرمجيات الخبيثة والفيروسات.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

الوحدة الثالثة: أمن الشبكات والاتصالات:

- التعرف على مكونات الشبكة ومخاطرها.
- فهم البروتوكولات الآمنة مثل HTTPS وSSL.
- تأمين الشبكات اللاسلكية المنزلية والمكتبية.
- إعداد الشبكة باستخدام الجدران النارية.
- تقنيات رصد حركة الشبكة واكتشاف الاختراقات.
- حماية الشبكات من هجمات DoS وMITM.
- أدوات المراقبة الشبكية للمبتدئين.
- إعداد الشبكات الافتراضية الخاصة VPN.
- إدارة كلمات مرور الشبكات والأجهزة.

الوحدة الرابعة: التهديدات والهجمات السيبرانية:

- أنواع الهجمات: فيشينج، سبام، فايروسات.
- هجمات القوة الغاشمة وسرقة كلمات المرور.
- هجمات الهندسة الاجتماعية وطرق التصدي لها.
- تحليل رسائل البريد الإلكتروني الاحتيالية.
- أدوات المهاجمين واليات العمل بها.
- كيفية التعرف على سلوك غير طبيعي في الأنظمة.
- بناء قواعد للسلوك الآمن على الإنترنت.
- تقنيات التوعية بالحيل والتهديدات الحديثة.
- تطبيق إجراءات الاستجابة للحوادث البسيطة.

الوحدة الخامسة: تطبيقات عملية ونماذج حماية:

- إعداد نظام تشغيل آمن خطوة بخطوة.
- محاكاة هجوم بسيط وتحليله.
- استخدام برامج مفتوحة المصدر في الحماية.
- إنشاء خطط استجابة أولية للحوادث.
- إعداد وتطبيق سياسة كلمات المرور القوية.
- إدارة صلاحيات المستخدمين بفعالية.
- مراجعة إعدادات الأمان في الشبكة المحلية.
- تنفيذ اختبارات بسيطة لفحص الثغرات.
- إنشاء دليل توعوي أمني للمستخدمين.

خلاصة وتوصيات الدورة التدريبية:

تُعد دورة لأمن السيبراني للمبتدئين: حماية الأنظمة والشبكات، بوابة أساسية لفهم الأمن السيبراني للمبتدئين وتطبيق مبادئ الحماية بشكل عملي. تساعد الدورة المشاركين على تطوير ممارسات رقمية آمنة وتحسين جاهزيتهم لمواجهة التهديدات السيبرانية. من الضروري الاستمرار في متابعة التطورات الأمنية والمشاركة في دورات متقدمة مستقبلًا. نوصي المتدربين بتطبيق ما تعلموه في بيناتهم الشخصية والمهنية على الفور.