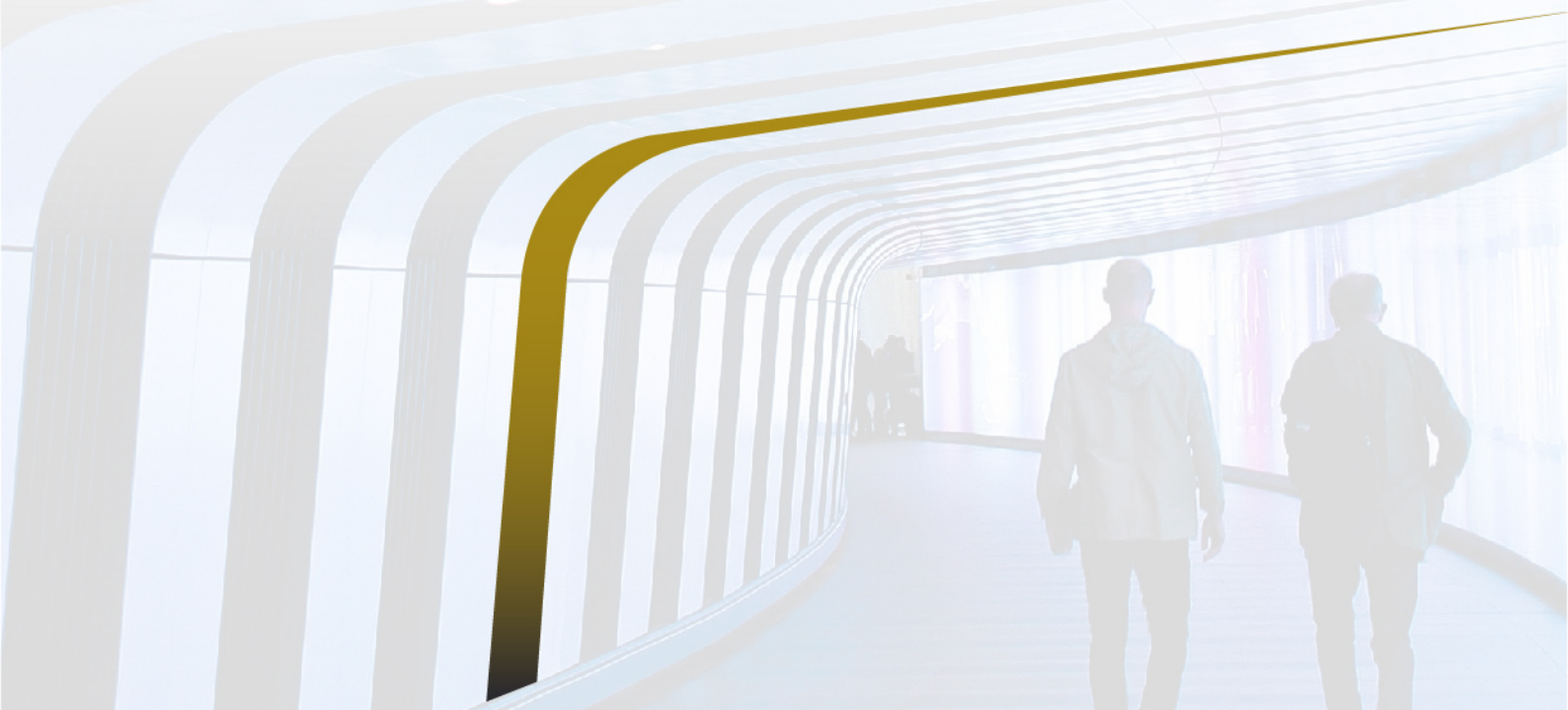
# غير التقنيين الدورة التدريبية: حماية الأصول الرقمية للمبتدئين والموظفين



اغسطس ٢٠٢٦ ٢٨ - ٢٤

كوالالمبور

(للشخص الواحد) € ٥٢٠٠

Ref: #CYB7548_274897

## مقدمة الدورة التدريبية / لمحة عامة:

التعقيد. فمع أساسية لكل من يرغب في فهم أساسيات الأمن السيبراني تُعد هذه الدورة التدريبية الشاملة نقطة انطلاق أصبح التهديد السيبراني يمثل تحديًا تزايد الاعتماد على التكنولوجيا في حياتنا اليومية وحماية البيانات في عالم رقمي متزايد اللازمة مصممة خصيصًا لتمكين المبتدئين والموظفين غير كبيرًا للأفراد والمؤسسات على حد سواء. هذه الدورة والمهنية، مسؤولية الخبراء التقنيين فقط، للتعامل مع هذه التحديات بفعالية. نحن نؤمن بأن التقنيين من اكتساب المعرفة والمهارات الجميع. سيتمكن المشاركون من التعرف على مفاهيم بل هو مسؤولية جماعية تتطلب وعيًا وفهمًا من الأمن السيبراني ليس المحتوى إلى أحدث المعلومات الأساسي، حماية الخصوصية الرقمية، وأفضل رئيسية مثل التهديدات السيبرانية الشائعة، أمن المستنيرة من أعمال خبراء مثل الأبحاث والممارسات الموصي بها في هذا المجال، بما ممارسات الأمن السيبراني. يستند BIG BEN يُعد مرجعًا عالميًا في مجال أمن الكمبيوتر البروفيسور روس أندرسون (Ross Anderson)، الذي في ذلك الأفكار من التعرف على المخاطر واتخاذ خطوات هذه الدورة بهدف بناء ثقافة أمنية قوية، Center والأنظمة الموثوقة. يقدم Training المنزلية، هذه الدورة فهمًا عميقًا لكيفية تجنب الاحتيال استباقية لحماية أنفسهم وبياناتهم الحساسة. ستوفر تمكّن الأفراد وإدارة كلمات المرور القوية. الإلكتروني، تأمين الشبكات اللاسلكية

## لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- الموظفون الإداريون في مختلف الأقسام.
- البيانات الرقمية. الموظفون الجدد في أي بيئة عمل تتطلب التعامل مع
- الأفراد المهتمون بتعزيز أمنهم الرقمي الشخصي.
- سيبراني متخصصة. أصحاب الأعمال الصغيرة الذين لا يملكون فرق أمن
- يرغبون في فهم أساسيات الأمن السيبراني. طلاب الجامعات من التخصصات غير التقنية الذين
- حماية الأجهزة. أي شخص يسعى لزيادة وعيه بمخاطر الإنترنت وكيفية

## القطاعات والصناعات المستهدفة:

- البيانات. قطاع الخدمات المالية والبنوك نظرًا لحساسية
- السرية. القطاع الصحي والمستشفيات لحماية بيانات المرضى
- للمؤسسات التعليمية. القطاع التعليمي والجامعات لتعزيز الأمن السيبراني
- لأهمية أمن المعلومات الحكومية. القطاع الحكومي والهيئات العامة وما في حكمها نظرًا
- العملاء المالية. قطاع التجزئة والتجارة الإلكترونية لحماية بيانات
- التحتية الحيوية. قطاع الصناعات التحويلية والطاقة لتعزيز أمن البنية

## الأقسام المؤسسية المستهدفة:

- السيبراني. إدارة الموارد البشرية لضمان وعي الموظفين بالأمن
- التسويقية. إدارة التسويق والمبيعات لحماية بيانات العملاء
- التشغيلي. إدارة العمليات والإدارة العامة لتعزيز الأمن
- لقوانين حماية البيانات. إدارة الشؤون القانونية والامتثال لضمان الامتثال
- الأمني للمؤسسة. إدارة العلاقات العامة والإعلام لتعزيز الوعي

## أهداف الدورة التدريبية:

أتقن المهارات التالية: بنهاية هذه الدورة التدريبية، سيكون المتدرب قد

- الرئيسية. فهم المفاهيم الأساسية للأمن السيبراني ومكوناته
- وكيفية اكتشاف هجمات التصيد الاحتيالي. التعرف على أنواع التهديدات السيبرانية الشائعة
- والمعلومات الحساسة. تطبيق أفضل الممارسات لحماية البيانات الشخصية
- عبر الإنترنت. القدرة على إنشاء كلمات مرور قوية وإدارة الحسابات
- المحمولة. فهم أهمية النسخ الاحتياطي للبيانات وتأمين الأجهزة
- الوعي بأمن الشبكات المنزلية وحماية الواي فاي.
- تجنبها. التعرف على مخاطر الهندسة الاجتماعية وكيفية

## منهجية الدورة التدريبية:

النظرية مصممة لضمان أقصى استفادة للمشاركين، بغض النظر عن تتبع هذه الدورة التدريبية منهجية تفاعلية وشاملة عملية. سيتم تشجيع بأسلوب مبسط ومفهوم، يليه تطبيق عملي مكثف من خلال خلفيتهم التقنية. نركز على تقديم المفاهيم الأمنية المشتركة وتطوير حلول مبتكرة. المشاركين على العمل في مجموعات صغيرة لمناقشة دراسات حالة واقعية وتمارين الاحتيالية أو للمتدربين ممارسة المهارات المكتسبة مباشرة، مثل تتضمن الجلسات التفاعلية ورش عمل تطبيقية تتيح التحديات تغذية راجعة مستمرة لضمان فهم إعداد إعدادات الخصوصية في التطبيقات. بالإضافة إلى التعرف على رسائل البريد الإلكتروني المشاركون من طرح الأسئلة ومناقشة التحديات عميق للمفاهيم وتطبيق الممارسات الأمنية الفعالة. ذلك، سيتم توفير ومشجعة Center تجربة التعلم الشاملة. يلتزم BIG BEN Training التي يواجهونها في بيئاتهم الخاصة، مما يعزز من سيتمكن الشخصي والمؤسسي. في بناء قدرات المشاركين في مجال الأمن السيبراني تساهم بتقديم بيئة تعليمية داعمة

## خريطة المحتوى التدريبي (محاور الدورة التدريبية):

## الأولية الوحدة الأولى: أساسيات الأمن السيبراني والمفاهيم

- مقدمة إلى عالم الأمن السيبراني.
- تعريفات رئيسية: التهديد، الثغرة الأمنية، المخاطر.
- أهمية حماية البيانات في العصر الرقمي.
- أنواع المعلومات الحساسة.
- مقدمة إلى الأمن السيبراني للمستخدم العادي.
- المصطلحات الشائعة في أمن المعلومات.
- الأمن السيبراني في حياتنا اليومية.

## وكيفية التعرف عليها الوحدة الثانية: التهديدات السيبرانية الشائعة

- الفدية. البرامج الضارة: الفيروسات، أحصنة طروادة، برامج
- اكتشاف رسائل البريد الإلكتروني الاحتيالية. التصيد الاحتيالي ( Phishing): أنواعه وكيفية
- الحماية منها. الهندسة الاجتماعية: التكتيكات المستخدمة وكيفية
- هجمات حجب الخدمة الموزعة ( DDoS): فهم بسيط.
- الوصول غير المصرح به وسرقة الهوية.
- تهديدات الويب الشائعة.
- أمن البيانات ضد الهجمات.

## الرقمية الوحدة الثالثة: حماية البيانات الشخصية والخصوصية

- العوامل: إدارة كلمات المرور القوية وأهمية المصادقة متعددة
- اللوحية: أمن الأجهزة المحمولة: الهواتف الذكية والأجهزة
- النسخ الاحتياطي للبيانات وأهميته:
- إعدادات الخصوصية على وسائل التواصل الاجتماعي:
- حماية الخصوصية عبر الإنترنت:
- تشفير البيانات الأساسي:
- حماية المعلومات الشخصية:

## الوحدة الرابعة: أمن الشبكات والاتصالات

- تأمين الشبكات اللاسلكية المنزلية (Wi-Fi):
- استخدام الشبكات الافتراضية الخاصة (VPN):
- أمن البريد الإلكتروني:
- تصفح الإنترنت الآمن:
- الجدران النارية (Firewalls): مفهومها الأساسي:
- الوعي بالتهديدات السيبرانية للشبكات:
- أمن نقاط النهاية:

## الممارسات الوحدة الخامسة: الاستجابة للحوادث الأمنية وأفضل

- للبيانات: ماذا تفعل في حالة التعرض لهجوم سيبراني أو انتهاك
- الإبلاغ عن التهديدات الأمنية:
- أهمية تحديث البرامج والأنظمة:
- الوعي الأمني المستمر:
- خطة الاستجابة للحوادث الأساسية:
- ثقافة الأمن السيبراني:
- الامتثال الأمني للموظفين:

## الأسئلة المتكررة:

### التسجيل في الدورة؟ ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل

لا توجد شروط مسبقة.

### الإجمالي لساعات الدورة التدريبية؟ كم تستغرق مدة الجلسة اليومية، وما هو العدد

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

### سؤال للتأمل:

الدفاع السيبراني، وتصبح أكثر تعقيداً، كيف يمكن للأفراد والمؤسسات في عالم تتطور فيه التهديدات السيبرانية باستمرار

وأن يحولوا الوعي الأمني إلى ممارسة يومية فعالة؟ غير التقنية أن يظلوا في طليعة

### ما الذي يميز هذه الدورة عن غيرها من الدورات؟

في حياتهم لتمكين المبتدئين والموظفين غير التقنيين من فهم تتميز هذه الدورة بتركيزها العملي والموجه خصيصًا نركز على تقديم رؤى عملية وأمثلة اليومية والمهنية. بدلاً من الغوص في التفاصيل أساسيات الأمن السيبراني وتطبيقها الوقائية وفعالية. نبتعد عن الأدوات والبرمجيات المحددة، واقعية تتيح للمشاركين استيعاب المفاهيم بسرعة التقنية المعقدة، تشمل الدورة دراسات حالة تفاعلية التي تبقى ذات قيمة بغض النظر عن التغيرات ونركز على تنمية الوعي الأمني والمهارات الصناعية وكيفية الاستجابة لها بفعالية. يعتمد المحتوى على تُظهر سيناريوهات التهديدات السيبرانية الشائعة التكنولوجية. معلومات نظرية، بل هي دعوة الموصي بها في مجال أمن المعلومات وحماية البيانات. أحدث الأبحاث الأكاديمية والممارسات خط الدفاع الأول ضد المخاطر السيبرانية. لتبني عقلية أمنية استباقية، تمكن المشاركين من أن هذه الدورة ليست مجرد يصبحوا