الدورة التدريبية: حماية الهوية الرقمية والخصوصية على الإنترنت للأفراد والمؤسسات

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

كوالالمبور

(للشخص الواحد) € ٥٢٠٠

Ref: #CYB4913_270943

مقدمة الدورة التدريبية / لمحة عامة:

مع تزايد التهديدات والخصوصية على الإنترنت من أهم القضايا التي تواجه في عصر الرقمنة المتسارع، أصبحت الهوية الرقمية الدورة أصبح من الضروري فهم كيفية حماية المعلومات السيبرانية، مثل سرقة الهوية وانتهاك البيانات، الأفراد والمؤسسات. لـتأمين هويتهم الرقمية التدريبية الشاملة لجميع الأفراد وموظفي المؤسسات، الشخصية والبيانات الحساسة. تقدم هذه مفاهيم الهوية الرقمية، التهديدات الشائعة، وحماية خصوصيتهم على الإنترنت. سنتناول في هذه المعرفة والمهارات اللازمة وتطبيق ضوابط الخصوصية. سيكتسب المشاركون القدرة على تحديد أفضل الممارسات لـأمن الحسابات، واستخدام أدوات الدورة قوي يمكن أن يقي من الكثير من حماية فعالة في حياتهم الرقمية. تهدف الدورة إلى المخاطر الأمنية، اتخاذ قرارات آمنة، تشا الممارسات الدولية، مع الاستفادة من إسهامات خبراء المخاطر. يستند المحتوى إلى أحدث المعايير وأفضل بناء وعي أمني والعملات المشفرة. يقدم BIG BEN ، المعروف بأعماله الرائدة في (David Chaum) أكاديميين بارزين مثل البروفيسور ديفيد والمؤسسات من التحكم في بصمتهم الرقمية وحماية هذه الدورة لتمكين الأفراد Training Center الخصوصية الرقمية أصولهم الشخصية والمعلوماتية.

لـ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- جميع مستخدمي الإنترنت من الأفراد.
- موظفو المؤسسات من جميع المستويات.
- مديرو الأمن السيبراني والمخاطر.
- المسؤولون عن حماية البيانات والخصوصية.
- القانونية.المحترفون في مجالات الموارد البشرية والشؤون
- الآباء والأمهات الراغبين في حماية أسرهم.

القطاعات والصناعات المستهدفة:

- جميع القطاعات والصناعات.
- القطاع المالي والمصرفي.
- شركات التكنولوجيا.
- الرعاية الصحية.
- القطاع الحكومي وما في حكمها.
- قطاع التعليم.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة الموارد البشرية.
- إدارة الشؤون القانونية والامتثال.
- إدارة الاتصالات.
- إدارة تكنولوجيا المعلومات.

أهداف الدورة التدريبية:

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

- الإنترنت. فهم مفاهيم الهوية الرقمية وأهمية الخصوصية على
- الهوية والاحتيال. القدرة على تحديد التهديدات الشائعة مثل سرقة
- المرور. تطبيق أفضل الممارسات لـتأمين الحسابات وكلمات
- التواصل الاجتماعي. التعامل الآمن مع البيانات الشخصية على منصات
- استخدام أدوات وتقنيات الخصوصية مثل VPNs
- حماية الأجهزة الشخصية من البرامج الضارة.
- التعرف على حقوق الخصوصية والالتزامات القانونية.

منهجية الدورة التدريبية:

الحالة مصممة لجعل مفاهيم حماية الهوية الرقمية سهلة الفهم تعتمد هذه الدورة التدريبية منهجية عملية وتشاركية، فهم تأثير سلوكهم الرقمي الواقعية لحوادث سرقة الهوية وانتهاك البيانات، والتطبيق. سيتمكن المتدربون من خلال دراسات وأنشطة جماعية لتعزيز الوعي وبناء على أمنهم الشخصي والمؤسسي. تتضمن المنهجية مقاطع وورش العمل التفاعلية، من BIG BEN التطبيقي للحماية، من تأمين الحسابات إلى استخدام عادات رقمية آمنة. سيتم التركيز على الجانب فيديو توضيحية وحماية أصولهم الأكثر قيمة. هذه الدورة لتمكين الأفراد والمؤسسات من التحكم في أدوات التشفير. يقدم Training Center مصيرهم الرقمي

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الهوية الرقمية والخصوصية

- مفهوم الهوية الرقمية وبصمتك الرقمية.
- أهمية الخصوصية على الإنترنت.
- الاحتيال). التهديدات الشائعة للهوية الرقمية (سرقة الهوية،
- الفرق بين البيانات الشخصية والبيانات الحساسة.
- أخلاقيات استخدام الإنترنت والخصوصية.
- تأثير انتهاك البيانات على الأفراد والمؤسسات.
- حقوقك الرقمية وقوانين حماية البيانات.

الوحدة الثانية: تأمين الحسابات وكلمات المرور

- إنشاء كلمات مرور قوية وآمنة.
- استخدام المصادقة متعددة العوامل (MFA).
- إدارة كلمات المرور بشكل فعال.
- حماية الحسابات على منصات التواصل الاجتماعي والبريد الإلكتروني.
- التعامل مع رسائل التصيد الاحتيالي (Phishing).
- التعرف على علامات الاختراق.
- التعامل مع اختراق الحساب.

الوحدة الثالثة: حماية البيانات على الإنترنت

- مخاطر مشاركة المعلومات الشخصية على الإنترنت.
- تأمين البيانات أثناء التسوق الإلكتروني.
- استخدام شبكات Wi-Fi العامة بأمان.
- تشفير البيانات على الأجهزة الشخصية.
- أمان التصفح وأدوات حظر التتبع.
- التعامل الآمن مع رسائل البريد الإلكتروني والمرفقات.
- حماية الخصوصية على محركات البحث.

الوحدة الرابعة: حماية الأجهزة الشخصية والشبكات

- أمن الأجهزة المحمولة (الهواتف، الأجهزة اللوحية).
- حماية أجهزة الكمبيوتر من البرامج الضارة والفيروسات.
- تأمين الشبكة المنزلية (الراوتر).
- التعامل مع البرامج الضارة (Malware) وفيروس الفدية (Ransomware).
- أهمية تحديث البرامج وأنظمة التشغيل.
- النسخ الاحتياطي للبيانات بشكل دوري.
- استخدام أدوات الحماية الأمنية.

الحوادث الوحدة الخامسة: الخصوصية في المؤسسات والتعامل مع

- سياسات حماية البيانات في المؤسسات.
- مسؤولية الموظف في حماية البيانات.
- التعرف على حوادث انتهاك البيانات.
- وضع خطة للاستجابة للحوادث الأمنية.
- الإبلاغ الفوري عن أي انتهاك للخصوصية.
- الالتزام باللوائح القانونية لحماية البيانات.
- مستقبل الهوية الرقمية والخصوصية.

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:

لا تقتصر على الضخمة، كيف يمكن للأفراد والمؤسسات أن يبتكرون في ظل التطور المتسارع للذكاء الاصطناعي والبيانات المستقبلية، وتُنشئ درعًا رقميًا مرنًا معالجة التهديدات الحالية، بل تتوقع انتهاكات استراتيجيات لحماية هوياتهم الرقمية والحفاظ على أمنهم الشخصي؟ يُمكنهم من التحكم الكامل في بصمتهم الرقمية الخصوصية

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

المؤسسات على حماية الهوية الرقمية والخصوصية، مما يوفر محتوى تتميز هذه الدورة بتركيزها الشامل والعملي على لحماية البيانات الشخصية حد سواء. بدلاً من تناول الأمن السيبراني بشكل عام، مصممًا خصيصًا ليناسب الأفراد وموظفي سرقة الهوية، مع تحليل مفصل لنتائجها وأمن الحسابات. تقدم الدورة دراسات حالة واقعية نغوص في التطبيق العملي هي برنامج للأمن، وتشجيع المشاركين على اتخاذ قرارات واعية وكيفية بناء دفاعات قوية. نركز على الجانب السلوكي لحوادث من التهديدات المتزايدة تدريبي مكثف يهدف إلى بناء مجتمع واعٍ رقميًا قادر ومسؤولة. إنها ليست مجرد دورة نظرية بل على حماية نفسه ومؤسسته