ثقافة الأمن الدورة التدريبية: الوعي السيبراني للموظفين - تعزيز

سبتمبر ٢٠٢٦ ٢٥ - ٢١

كيب تاون - *

(للشخص الواحد) € ٦٠٠٠

Ref: #CYB4777_564694

مقدمة الدورة التدريبية / لمحة عامة:

هجمات التصيد الاحتيالي في أي استراتيجية للأمن السيبراني. مع تزايد يُعد العنصر البشري خط الدفاع الأول والأكثر أهمية
أن يكون جميع الموظفين على دراية بمخاطر ، أصبح من (Malware) والبرامج الضارة ((Phishing) التهديدات السيبرانية مثل
المعرفة الدورة التدريبية التفاعلية والشاملة لجميع موظفي الأمن السيبراني وكيفية التصرف بشكل آمن. تقدم هذه الضروري
في هذه الدورة أساسيات والمهارات الأساسية لحماية أنفسهم ومؤسساتهم من المؤسسات، بغض النظر عن مناصبهم،
لأمن كلمات المرور، والتعامل الآمن مع الأمن السيبراني، التعرف على الهجمات الشائعة، أفضل التهديدات الرقمية. سنتناول
اتخاذ قرارات آمنة في حياتهم المهنية والشخصية، مما المعلومات الحساسة. سيكتسب المشاركون القدرة على الممارسات
المحتوى إلى تهدف الدورة إلى بناء ثقافة أمنية قوية في المؤسسة، يقلل بشكل كبير من احتمالية وقوع حوادث أمنية.
بارزين مثل الدكتور جوزيف أحدث الممارسات والمعايير الأمنية، مع الاستفادة من حيث يصبح الأمن مسؤولية جماعية. يستندا
التوعية الأمنية وسلوك المستخدم. يقدم BIG BEN ، المعروف بأعماله في (Joseph Cannon) كانون (إسهامات خبراء أكاديميين
أن يصبحوا درعًا منيعًا ضد الهجمات السيبرانية. الدورة لتمكين الموظفين من هذه Training Center

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- جميع موظفي المؤسسة من مختلف الأقسام والمستويات.
- المديرون وقادة الفرق.
- موظفو الإدارة والموارد البشرية.
- الموظفون الجدد.
- فرق المبيعات وخدمة العملاء.
- الفرق التقنية وغير التقنية.

القطاعات والصناعات المستهدفة:

- جميع القطاعات والصناعات.
- القطاع المالي والمصرفي.
- الرعاية الصحية.
- القطاع الحكومي وما في حكمها.
- شركات التجزئة.
- الشركات الصغيرة والمتوسطة.

الأقسام المؤسسية المستهدفة:

- جميع الأقسام المؤسسية.
- إدارة الموارد البشرية.
- إدارة المبيعات والتسويق.
- الإدارة التنفيذية.
- إدارة تقنية المعلومات.
- إدارة العمليات.

أهداف الدورة التدريبية:

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

- فهم مفاهيم الأمن السيبراني الأساسية وأهميتها.
- البرامج الضارة). التعرف على التهديدات السيبرانية الشائعة (التصيد،
- والروابط الضارة. القدرة على تحديد رسائل البريد الإلكتروني المشبوهة
- وآمنة. تطبيق أفضل الممارسات لإنشاء كلمات مرور قوية
- حماية البيانات الحساسة والمعلومات السرية للمؤسسة.
- التعامل الآمن مع الأجهزة الشخصية وشبكات Wi-Fi
- الإبلاغ الفعال عن الحوادث الأمنية المحتملة.

منهجية الدورة التدريبية:

المتدربون من مصممة لجعل مفاهيم الأمن السيبراني سهلة الفهم تعتمد هذه الدورة التدريبية منهجية تفاعلية وجذابة،
ودراسات الحالة الواقعية لحوادث خلال ورش العمل العملية التي تتضمن محاكاة هجمات والتطبيق لجميع الموظفين. سيتمكن
مقاطع فيديو توضيحية وأنشطة جماعية لتعزيز أمنية، من فهم تأثير سلوكهم على أمن المؤسسة. تتضمن التصيد الاحتيالي،
BIG BEN الجانب السلوكي للأمن، وتشجيع الموظفين على أن الوعي وبناء ثقافة أمنية قوية. سيتم التركيز على المنهجية
تكنولوجيا المعلومات، بل هو هذه الدورة لضمان أن الأمن السيبراني ليس Center يكونوا يقظين ومسؤولين. يقدمTraining
مسؤولية مشتركة بين جميع أفراد المؤسسة. مجرد مسؤولية فريق

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الوعي السيبراني للموظفين

- مقدمة إلى الأمن السيبراني وأهميته في مكان العمل.
- التهديدات السيبرانية الشائعة وكيفية عملها.
- الموظف كخط دفاع أول.
- التعامل مع المعلومات السرية والبيانات الحساسة.
- أمن الأجهزة الشخصية في بيئة العمل.
- التعرف على هجمات الهندسة الاجتماعية.
- المسؤولية الفردية في الأمن السيبراني.

والهندسة الاجتماعية الوحدة الثانية: التصيد الاحتيالي ((Phishing

- Smishing). أنواع هجمات التصيد الاحتيالي (Spear Phishing,
- المشبوهة. كيفية التعرف على رسائل البريد الإلكتروني
- التعامل مع الروابط والمرفقات الضارة.
- حماية المعلومات الشخصية من الهندسة الاجتماعية.
- محاكاة هجمات تصيد عملية.
- الإبلاغ عن رسائل التصيد الاحتيالي.
- أهمية اليقظة الدائمة.

الوحدة الثالثة: تأمين كلمات المرور والوصول

- أفضل الممارسات لإنشاء كلمات مرور قوية.
- استخدام المصادقة متعددة العوامل (MFA).
- مخاطر استخدام نفس كلمة المرور في أكثر من مكان.
- إدارة كلمات المرور بشكل آمن.
- أمن الوصول إلى أنظمة الشركة.
- حماية حسابات الموظفين من الاختراق.
- التعامل مع كلمات المرور على الأجهزة المحمولة.

العمل الوحدة الرابعة: حماية البيانات والأجهزة في مكان

- أمن البيانات والخصوصية في مكان العمل.
- التعامل مع البيانات السرية وفقًا لسياسات المؤسسة.
- أمن الأجهزة المحمولة (الهواتف، الأجهزة اللوحية).
- أمن الشبكات اللاسلكية (Wi-Fi).
- التعامل الآمن مع الأجهزة الخارجية (USB).
- مخاطر استخدام شبكات Wi-Fi العامة.
- إجراءات الأمن عند العمل عن بعد.

أمنية الوحدة الخامسة: الاستجابة للحوادث وبناء ثقافة

- ماذا تفعل عند وقوع حادث أمني؟
- الإبلاغ الفوري عن الحوادث الأمنية.
- دور الموظف في الاستجابة للحوادث.
- بناء ثقافة أمنية إيجابية في المؤسسة.
- أهمية التدريب المستمر.
- التحديات في التوعية الأمنية.
- مكافآت السلوك الأمني الإيجابي.

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:

التدريب، السيبراني، كيف يمكن للمؤسسات أن تبتكر استراتيجيات بما أن العنصر البشري هو أضعف حلقة في سلسلة الأمن موظف من أن يكون درعًا بل تحول الوعي الأمني إلى سلوك طبيعي، وتُنشئ ثقافة توعية أمنية مستدامة لا تقتصر على مجرد استباقيًا ضد التهديدات الرقمية المتزايدة؟ أمنية قوية تُمكن كل

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

الخبرة في المؤسسة. الوعي السيبراني للموظفين، مما يوفر محتوى مصممًا تتميز هذه الدورة بتركيزها الشامل والعملي على الأمن من خلال محاكاة هجمات واقعية بدلاً من مجرد سرد المعلومات، نغوص في التطبيق خصيصًا ليناسب جميع مستويات قابلة للتطبيق الفوري، مما يضمن أن المشاركين ودراسات حالة تفاعلية. نقدم أمثلة عملية ونصائح العملي لمفاهيم والمشاركة في حماية نركز على بناء ثقافة أمنية إيجابية، حيث يُشجع سيخرجون بمهارات عملية لحماية أنفسهم ومؤسساتهم. مصممة لتغيير السلوك وبناء مجتمع الأصول الرقمية. إنها ليست مجرد دورة نظرية، بل هي الموظفون على تحمل المسؤولية مؤسسي واعٍ أمنيًا. تجربة تعليمية