المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

Security Awareness and Training Programs

فكرة الدورة

أصبحت التوعية الأمنية عاملاً أساسياً في تقليل المخاطر السيبرانية المرتبطة بالسلوك البشري، خاصة مع تزايد التصيد الاحتيالي، والهندسة الاجتماعية، وتسرب البيانات، وسوء استخدام الأنظمة. ولم تعد برامج التوعية مجرد رسائل إرشادية أو دورات سنوية، بل أصبحت جزءاً من منظومة إدارة المخاطر وبناء الثقافة الأمنية داخل المؤسسة.

يركز هذا البرنامج التدريبي من AINFCT على تمكين المشاركين من تصميم وتنفيذ وإدارة برامج توعية وتدريب أمني فعّالة، تبدأ من تحليل الجمهور والمخاطر السلوكية، مروراً ببناء الرسائل والمحتوى، وانتهاءً بقياس الأثر والتحسين المستمر. كما يتناول البرنامج أساليب التدريب حسب الأدوار، وحملات التوعية، ومحاكاة التصيد، والتواصل الأمني، ومؤشرات قياس النضج.

يوفر البرنامج قيمة تطبيقية واضحة من خلال تحويل مفاهيم الوعي الأمني إلى ممارسات قابلة للتنفيذ، بما يساعد المؤسسات على تعزيز الالتزام، وتقليل الأخطاء البشرية، وبناء سلوك أمني مستدام.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تحليل احتياجات التوعية والتدريب الأمني داخل المؤسسة.
- تصميم برامج توعية مبنية على المخاطر والسلوك.
- تطوير رسائل أمنية واضحة لجماهير مختلفة.
- إدارة حملات تدريبية وتوعوية متعددة القنوات.
- قياس أثر التوعية باستخدام مؤشرات عملية.
- تحسين السلوك الأمني عبر تدخلات مستمرة.

منهجية الدورة

- عروض تفاعلية مدعومة بأمثلة سلوكية واقعية.
- تمارين تصميم رسائل وحملات توعوية.
- مناقشات حول أخطاء بشرية وحوادث شائعة.
- تحليل سيناريوهات تصيد وهندسة اجتماعية.
- تطبيق عملي لبناء خطة توعية قابلة للتنفيذ.

أثر الدورة على المنظمة

يمكن تعزيز الثقافة الأمنية المؤسسية من خلال:

- تقليل المخاطر الناتجة عن الأخطاء البشرية.
- رفع الالتزام بالسياسات والإجراءات الأمنية.
- تحسين استجابة الموظفين للتهديدات اليومية.
- دعم نضج الأمن السيبراني المؤسسي.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- بناء برامج توعية أمنية قابلة للتطبيق.
- تحويل المفاهيم الأمنية إلى رسائل مؤثرة.
- تقييم فعالية التدريب الأمني بموضوعية.
- إدارة التغيير السلوكي المرتبط بالأمن.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المختصين والمسؤولين عن رفع الوعي الأمني، وتطوير السلوك السيبراني الآمن، ودعم الامتثال للسياسات الأمنية داخل المؤسسة. كما يفيد فرق الأمن وتقنية المعلومات والموارد البشرية والاتصال المؤسسي المشاركة في تنفيذ برامج التوعية.

- مسؤولو أمن المعلومات والأمن السيبراني.
- مختصو التوعية والتدريب الأمني.
- فرق تقنية المعلومات والدعم الفني.
- مسؤولو الحوكمة والمخاطر والامتثال.
- فرق الموارد البشرية والاتصال الداخلي.

موضوعات الدورة

اليوم الأول: مدخل إلى التوعية الأمنية والثقافة السيبرانية

- مفهوم التوعية الأمنية ودورها في تقليل المخاطر.
- العلاقة بين السلوك البشري والتهديدات السيبرانية.
- الفرق بين الوعي والتدريب والتعليم الأمني.
- مكونات الثقافة الأمنية داخل بيئة العمل.
- دور القيادة والإدارة في دعم السلوك الآمن.

اليوم الثاني: تحليل المخاطر السلوكية واحتياجات التدريب

- تحديد السلوكيات عالية المخاطر داخل المؤسسة.
- تحليل الجمهور حسب الدور ومستوى التعرض.
- استخدام الحوادث والنتائج الأمنية كمصدر احتياج.
- تحديد فجوات المعرفة والمهارة والسلوك.
- ترتيب أولويات التدريب وفق المخاطر المؤسسية.

اليوم الثالث: تصميم استراتيجية برنامج التوعية

- تحديد رؤية البرنامج وأهدافه التشغيلية.
- ربط التوعية بإدارة المخاطر والسياسات الأمنية.
- تحديد النطاق والجمهور والرسائل الرئيسية.
- بناء خارطة سنوية للأنشطة والحملات.
- توزيع الأدوار بين الأمن والاتصال والموارد البشرية.

اليوم الرابع: بناء المحتوى الأمني الفعّال

- خصائص الرسائل الأمنية الواضحة والمؤثرة.
- تحويل السياسات إلى تعليمات قابلة للفهم.
- استخدام القصص والسيناريوهات في المحتوى.

- تبسيط المفاهيم التقنية لغير المتخصصين.
- تجنب التهويل والإرهاق المعلوماتي في الرسائل.

اليوم الخامس: التوعية بالتصيد والهندسة الاجتماعية

- أنواع التصيد الاحتيالي وأساليب الخداع الشائعة.
- مؤشرات الرسائل والروابط والمرفقات المشبوهة.
- الهندسة الاجتماعية عبر الهاتف والمنصات الرقمية.
- سلوك الإبلاغ الآمن عن محاولات الاحتيال.
- تصميم رسائل توعوية ضد أساليب الخداع.

اليوم السادس: حماية البيانات والخصوصية

- مبادئ التعامل الآمن مع البيانات الحساسة.
- تصنيف المعلومات ومتطلبات مشاركتها.
- مخاطر التخزين والنقل غير الآمن للبيانات.
- الخصوصية في العمل عن بُعد والمنصات السحابية.
- توعية الموظفين بمسؤوليات حماية البيانات.

اليوم السابع: كلمات المرور والهوية الرقمية

- مخاطر كلمات المرور الضعيفة والمعاد استخدامها.
- مبادئ إدارة كلمات المرور والعبارات السرية.
- المصادقة متعددة العوامل وتجربة المستخدم.
- حماية الحسابات الشخصية والمهنية.
- رسائل تدريبية لتعزيز ممارسات الهوية الآمنة.

اليوم الثامن: أمن الأجهزة والعمل المتنقل

- الاستخدام الآمن للحواسيب والأجهزة المحمولة.
- مخاطر الشبكات العامة والوسائط القابلة للإزالة.
- تحديث الأنظمة والتطبيقات وأثره الأمني.

- الإبلاغ عن فقدان الأجهزة أو الاشتباه باختراقها.
- سلوكيات العمل الآمن خارج مقر المؤسسة.

اليوم التاسع: استخدام البريد والإنترنت والتطبيقات

- السلوك الآمن عند استخدام البريد الإلكتروني.
- مخاطر التنزيلات والمواقع غير الموثوقة.
- استخدام التطبيقات المعتمدة وتجنب القنوات غير الرسمية.
- التعامل مع الملفات والمرفقات والروابط.
- الممارسات الآمنة في التعاون الرقمي اليومي.

اليوم العاشر: التدريب حسب الأدوار والمسؤوليات

- التدريب العام لجميع الموظفين.
- التدريب المتخصص للمستخدمين ذوي الصلاحيات العالية.
- احتياجات فرق تقنية المعلومات والأمن.
- توعية الإدارة العليا وملاك العمليات.
- تصميم مسارات تدريبية حسب مستوى المخاطر.

اليوم الحادي عشر: الحملات والقنوات وأساليب التواصل

- اختيار القنوات المناسبة للرسائل الأمنية.
- إدارة الحملات الشهرية والموسمية.
- استخدام الملصقات والنشرات والرسائل القصيرة.
- التعلم المصغر والرسائل المتكررة.
- تنسيق التواصل بين الأمن والاتصال المؤسسي.

اليوم الثاني عشر: محاكاة التصيد والتمارين السلوكية

- أهداف محاكاة التصيد وحدود استخدامها.
- تصميم سيناريوهات واقعية وغير عقابية.
- إدارة النتائج والتغذية الراجعة للموظفين.

- تحليل الأنماط السلوكية بعد التمارين.
- تحويل نتائج المحاكاة إلى خطة تحسين.

اليوم الثالث عشر: قياس الفعالية ومؤشرات الأداء

- مؤشرات الحضور والإكمال والمشاركة.
- مؤشرات التغيير السلوكي والإبلاغ.
- قياس خفض المخاطر المرتبطة بالسلوك.
- استخدام الاستبيانات والاختبارات القصيرة.
- بناء لوحة متابعة لبرنامج التوعية.

اليوم الرابع عشر: حوكمة البرنامج والتحسين المستمر

- إدارة السياسات والاعتمادات المرتبطة بالتوعية.
- توثيق الخطة والأنشطة والنتائج.
- دمج التوعية في دورة إدارة المخاطر.
- مراجعة البرنامج بناءً على الحوادث والملاحظات.
- تحسين النضج الثقافي عبر دورات منتظمة.

اليوم الخامس عشر: التطبيق العملي وبناء خطة برنامج

- تحليل حالة تدريبية لبرنامج توعية مؤسسي.
- تصميم خارطة حملة توعوية لمدة عام.
- تحديد الرسائل والجماهير والقنوات.
- اختيار مؤشرات قياس مناسبة للبرنامج.
- مناقشة خطط التحسين والاستدامة.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة للموضوع السابق، ثم عرض للمحور الرئيسي، يتبعه نقاش تطبيقي أو تمرين قصير، وينتهي اليوم بخلاصة عملية تربط المفاهيم بسلوكيات العمل اليومية. يتم توزيع الوقت بما يوازن بين الشرح، والتفاعل، والتطبيق، والمراجعة المعرفية.

course_assessment

يعتمد التقييم على المشاركة الفعالة، والتمارين التطبيقية، وتحليل السيناريوهات، وإعداد عناصر من خطة توعية أمنية قابلة للتنفيذ. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- تصميم برامج التوعية الأمنية.
- تحليل المخاطر السلوكية.
- التواصل الأمني المؤثر.
- إدارة حملات التوعية.
- قياس فعالية التدريب.
- بناء الثقافة الأمنية.

مكتب القاهرة الرئيسي
القاهرة، جمهورية مصر العربية
7 شارع وهران، الطيران، مدينة نصر
+201152466358
info@ainfct.com
ainfct.com
رقم التسجيل الضريبي: 472920235
مكتب مدريد الفرعي
مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد
training@ainfct.com
ainfct.com