البروشور التعريفي للدورة

التوعية بالأمن السيبراني

دورة تأسيسية تعرّف الموظفين بالتهديدات السيبرانية التي يواجهونها يومياً، وتدرّبهم على سلوك آمن في البريد وكلمات المرور والتعامل مع البيانات والأجهزة.

الكود	HT-IT-101
التصنيف	تقنية المعلومات والأمن السيبراني
المدة	أسبوع واحد
المستوى	مبتدئ

مقدمة

كثير من الحوادث السيبرانية يبدأ بتصرف بسيط من موظف حسن النية: نقرة على رابط مزيّف، أو كلمة مرور مكررة، أو ملف يُرسل إلى الجهة الخطأ؛ ولهذا يبقى وعي الأفراد خط الدفاع الأول في كل مؤسسة.

الأهداف

- فهم أبرز التهديدات السيبرانية التي تستهدف الموظفين وأسباب نجاحها
- التعرف على رسائل التصيّد ومحاولات الهندسة الاجتماعية عبر القنوات المختلفة
- حماية الحسابات بكلمات مرور قوية والتحقق متعدد العوامل
- التعامل مع المعلومات والأجهزة وفق درجة حساسيتها
- الإبلاغ عن الحوادث المشتبه بها بسرعة وعبر القناة الصحيحة

لمن هذه الدورة

- موظفو الإدارات المختلفة الذين يستخدمون البريد والأنظمة يومياً
- موظفو الاستقبال وخدمة العملاء المتعاملون مع اتصالات خارجية
- المساعدون التنفيذيون ومديرو المكاتب المطلعون على معلومات حساسة
- الموظفون الجدد ضمن برامج التهيئة الوظيفية

المهارات التي ستكتسبها

- كشف رسائل التصيّد
- إدارة كلمات المرور بأمان
- تصنيف المعلومات ومشاركتها
- الإبلاغ عن الحوادث

مخرجات التعلم

- تحليل رسالة مشبوهة وتحديد ثلاث علامات على الأقل تكشف أنها تصيّد
- إعداد عبارة مرور قوية وتفعيل التحقق متعدد العوامل على حساب عمل
- تحديد درجة تصنيف مستند وطريقة مشاركته الآمنة داخل المؤسسة وخارجها
- رفع بلاغ واضح عن حادث مشتبه به يتضمن المعلومات التي يحتاجها فريق الأمن

محاور الدورة

اليوم الأول: التهديدات السيبرانية بلغة بسيطة

- لماذا يستهدف المهاجمون الأفراد وليس الأنظمة فقط
- البرمجيات الخبيثة وبرمجيات الفدية والاحتيال الإلكتروني

- قيمة البيانات التي يتعامل معها كل موظف في عمله اليومي

اليوم الثاني: التصيّد والهندسة الاجتماعية

- علامات رسائل التصيّد في البريد والرسائل النصية والمكالمات الهاتفية
- انتحال صفة المديرين وطلبات تحويل الأموال أو تعديل بيانات الموردين
- التحقق من الروابط والمرفقات قبل فتحها

اليوم الثالث: كلمات المرور وحماية الحسابات

- عبارات المرور وبرامج إدارة كلمات المرور
- التحقق متعدد العوامل وأهميته في منع الاستيلاء على الحسابات
- مشاركة الحسابات وتنبيهات تسجيل الدخول غير المعتاد

اليوم الرابع: البيانات والأجهزة وبيئة العمل

- تصنيف المعلومات وقواعد مشاركتها وإرسالها
- وسائط التخزين المحمولة والطباعة وسياسة المكتب النظيف
- الهاتف المحمول وشبكات الإنترنت العامة والعمل عن بُعد

اليوم الخامس: الإبلاغ والعادات الآمنة

- متى وكيف يُبلَّغ عن حادث مشتبه به وما الذي يجب تجنبه
- وسائل التواصل الاجتماعي والإفراط في مشاركة المعلومات الشخصية والوظيفية
- مشروع تطبيقي: قائمة سلوكيات آمنة خاصة بوظيفة المشارك مع سيناريو إبلاغ عن رسالة تصيّد

منهجية التدريب

فحص جماعي لرسائل تصيّد نموذجية تخفي علاماتها في التفاصيل
مقارنة عملية بين كلمات مرور ضعيفة وعبارات مرور قوية
جولة في مكتب افتراضي لاكتشاف مخالفات حماية المعلومات
تمرين إبلاغ يصعّد فيه المشاركون رسالة مشبوهة إلى فريق الأمن

الشهادة

يحصل المشارك على شهادة حضور من Harbor Training Center عند إتمام الدورة.

المواعيد القادمة

المدينة	الموعد	اللغة	الرسوم
لندن	7 – 11 ديسمبر 2026	AR	EUR 5,800
إسطنبول	17 – 21 مايو 2027	EN	EUR 5,400
دبي	24 – 28 مايو 2027	AR	EUR 4,800
لندن	7 – 11 يونيو 2027	EN	EUR 5,800
أمستردام	14 – 18 يونيو 2027	AR	EUR 6,100
أونلاين	21 – 25 يونيو 2027	EN	EUR 2,800

الرسوم للمشارك الواحد.

تواصل معنا

البريد info@harbor4training.com

للتسجيل والتفاصيل، امسح الرمز أو زر الرابط:

https://harbor4training.com/ar/courses/cybersecurity-awareness