



دورة الأمن الذاتي المعلوماتي

برنامج تدريسي عملي يهدف إلى رفع وعي المشاركين بمفاهيم أمن المعلومات وحماية الحسابات الشخصية على منصات التواصل الاجتماعي من الاختراق والتجسس.

أتلانتس ذا بالم	الفندق :	دبي	المدينة :
2026-01-30	تاريخ النهاية :	2026-01-26	تاريخ البداية :
\$ 3950	السعر :	Week 1	الفترة :



فكرة الدورة التدريبية

إن أمن المعلومات ليس مرتبطاً فقط بحماية المعلومات من الوصول غير المرخص إنما يمتد أيضاً لمنع أي استخدام، أو كشف، أو إتلاف، أو تعديل، أو نسخ غير مصرح به للمعلومات. ويمكن للمعلومات أن تكون مادية أو رقمية، فهي تشمل معلوماتك الشخصية، وحساباتك على مواقع التواصل الاجتماعي، والبيانات على هاتفك المحمول، وغير ذلك. من خلال هذه الدورة التدريبية المميزة حول الأمن الذاتي المعلوماتي، سوف تتعزّز على المقصود بأمن المعلومات، والمخاطر التي تواجه المستخدمين في جهة العمل ومواطن تلك المخاطر. كما سيعمل المشاركون كيفية تأمين حسابات الواقع التي يستخدمونها على الإنترنت، وقواعد أمن المعلومات التي يجب إتباعها لتفادي التعرّض للاختراق الشخصي أو اختراق المنشأة التي يعملون بها.

أهداف الدورة التدريبية

تهدف هذه الدورة التدريبية حول الأمن الذاتي المعلوماتي إلى:

- تدريب المشاركون على فهم قواعد وأسس وعناصر الأمن المعلوماتي
- تعريف المشاركون بما هي المخاطر التي تحيق بمستخدمي شبكة الإنترنت ونظم المعلومات على المستوى الشخصي وفي أماكن العمل
- تدريب المشاركون على كيفية تأمين مواقعهم الشخصية
- تعريف المشاركون على الأصول الواجب إتباعها لأمن المعلومات الشخصية ومعلومات العمل لتفادي التعرض للاختراق والتسريب
- تعريف المشاركون على القواعد الأمنية للتعامل مع نظم المعلومات في أماكن العمل بشكلٍ خاص والدواسيب الشخصية وأجهزة الهاتف المحمول

الفئات المستهدفة

هذه الدورة التدريبية موجهة لـ:

- ضباط الشرطة العاملين في مجال البحث الجنائي وتحليل المعلومات
- أعضاء النيابة العامة والقضاة
- موظفي القطاع الحكومي والخاص
- ضباط أمن المعلومات في القطاع الشرطي والعسكري
- المحامين
- أعضاء هيئة التدريس بالجامعات
- مسؤولي الأمن في المؤسسات والشركات

منهجية الدورة

تعتمد الدورة على عرض مبادئ أمن المعلومات بشكل مبسط وربطها بالمخاطر الواقعية التي يواجهها مستخدمو الإنترنت ونظم المعلومات. يتم توظيف أمثلة واقعية ودراسات الحالات لخراق حقيقي لشرح أساليب الهجوم وأسبابها وطرق الوقاية منها. تركز المنهجية على التطبيق العملي من خلال شرح إعدادات الأمان والحماية للحسابات الشخصية على أشهر منصات التواصل الاجتماعي. كما يتم تدريب المشاركين على كيفية اكتشاف مؤشرات الاختراق أو التجسس والتصرف الصحيح عند حدوثها. ويعزز البرنامج التعلم التفاعلي عبر النقاش وتبادل الخبرات لضمان ترسیخ الممارسات الآمنة في الاستخدام اليومي.

محاور الدورة

اليوم الأول: بيان المقصود بأمن المعلومات وعناصره الأساسية

- التعريف بأمن المعلومات والأمن الذاتي المعلوماتي
- شرح العناصر الأساسية لأمن المعلومات
- دراسة تحليلية لأشهر حالات الاختراق المعلوماتي وأسبابها

اليوم الثاني: المخاطر التي تواجه مستخدمي الإنترنت ونظم وشبكات المعلومات

- شرح طرق عمل الفيروسات والديدان الرقمية
- شرح أساليب الاختراق والتجسس
- شرح طرق الاختراق وأشهر الحالات من الواقع العملي

اليوم الثالث: تأمين الحسابات الشخصية على موقع فيس بوك

- شرح مكونات وخصائص موقع فيس بوك
- كيفية إنشاء حساب وتأمينه من الاختراق أو التجسس
- كيف تعرف إذا كان الحساب مخترق أو يتم التجسس عليه والإجراء الممكن اتخاذه لإعادة تأمين الحساب

اليوم الرابع: تأمين الحسابات الشخصية على موقع توينتر وجوجل

- شرح مكونات وخصائص موقع توينتر
- كيفية إنشاء حساب وتأمينه من الاختراق او التجسس
- كيف تعرف إذا كان الحساب مخترق أو يتم التجسس عليه والإجراء الممكن اتخاذه لإعادة تأمين الحساب

اليوم الخامس: تأمين الحسابات الشخصية على موقع إنستغرام وواتس آب



- شرح مكونات وخصائص موقع إنستغرام وواتس اب
- كيفية إنشاء حساب وتأمينه من الاختراق او التجسس
- كيف تعرف إذا كان الحساب مخترق أو يتم التجسس عليه والإجراءات الممكن اتخاذها ل إعادة تأمين الحساب

الشهادات المُعتمدة

عند إتمام هذا البرنامج التدريبي بنجاح، سيتم منح المشاركيين شهادة هاي بوينت رسمياً، اعترافاً بمعارفهم وكفاءاتهم المثبتة في الموضوع.
يُعد هذه الشهادة دليلاً رسمياً على كفاءتهم والتزامهم بالتطور المهني.

