المهارات الاساسية في الامن السيبراني

وصف البرنامج التدريبية (الدورة التدريبية)

- تم تصميم البرنامج التدريبي (الأمن السيبراني) وفقاً لتوجه العالم نحو زيادة الأمان الالكتروني للمستخدمين والدول وحفظ البيانات ويشتمل هذا البرنامج على تطوير المتدرب في تأمين شبكة الانترنت من الاختراقات بالإضافة إلى تأمين كافة الأجهزة الالكترونية المستخدمة بأنظمة حماية من البرامج الخبيثة وانتشاراتها، كما يخلق البرنامج الطرق المتبعة في تأمين المستخدمين وأجهزتهم بالإضافة إلى استخدام البروتوكولات الآمنة في عمليات التواصل، كما يستعرض البرنامج أهم طرق تأمين المدفوعات وتشفيرها بما يحقق حمايتها من أي أخطار ناتجة عن الهجمات الالكترونية المقرصنة.

الهدف العام من البرنامج التدريبي

- تعليم أفضل ممارسات الأمن السيبراني، بما في ذلك إنشاء كلمات مرور قوية، واستخدام برامج مكافحة الفيروسات، وتصفح الإنترنت بأمان، وحماية البيانات الشخصية.
- بناء مهارات التعافي من الحوادث السيبرانية، بما في ذلك إنشاء خطة استجابة للحوادث، واستعادة البيانات، والإبلاغ عن الحوادث.

الأهداف التفصيلية للبرنامج التدريبي:

المعرفة الكاملة بـ:-

- **أن يعرفوا أفضل المعاييروالتطبيقات المستخدمة في مجال الأمن السيبراني.**
- **أن يعرفوا كافة الضوابط الأمنية التي تستخدم من أجل حماية المعلومات والحفاظ على أجهزة الحاسب الآلي.**
- **أن يعرفوا كافة طرق تأمين المدفوعات وحماية الخدمات الرقمية المصرفية المختلفة.**
- **أن يتعرفوعلى عناصرأمن المعلومات التي تعمل على الأنظمة والبروتوكولات السرية**
- **أن يفهموا معاييرومتطلبات PCI DSS لتأمين المدفوعات الالكترونية.**

- **مخطط الدورة التدريبية:**

اليوم الأول:

- **مقدمة عن الأمن السيبراني:**
  - تعريف الأمن السيبراني وأهميته.
  - أنواع التهديدات السيبرانية الشائعة.
  - تأثير الهجمات السيبرانية على الأفراد والمنظمات.
- **مبادئ الأمن السيبراني الأساسية:**
  - أفضل ممارسات إنشاء كلمات المرور.
  - استخدام برامج مكافحة الفيروسات وتحديثها بانتظام.
  - تصفح الإنترنت بأمان وتجنب المواقع المشبوهة.
  - حماية البيانات الشخصية والمعلومات الحساسة.

اليوم الثاني:

- **الأمان على الإنترنت:**
  - مخاطر التصيد الاحتيالي والهندسة الاجتماعية.
  - كيفية التعرف على رسائل البريد الإلكتروني والبريد العشوائي الضارة.
  - استخدام VPN عند الاتصال بشبكات Wi-Fi العامة.
  - حماية خصوصيتك على الإنترنت.

اليوم الثالث:

- **أمان الأجهزة:**
  - حماية أجهزة الكمبيوتر والهواتف الذكية من البرامج الضارة.
  - تحديث أنظمة التشغيل والبرامج بانتظام.
  - استخدام برامج النسخ الاحتياطي لحماية البيانات.
  - تكوين جدار حماية قوي.

اليوم الرابع:

- **أمن الشبكات:**

- أنواع الشبكات الشائعة ومخاطرها.
- حماية الشبكات المنزلية والشركات.
- استخدام تقنيات التشفير لحماية البيانات.
- التعرف على برامج التجسس وبرامج الفدية.

اليوم الخامس:

- **التعافي من الحوادث السيبرانية:**
  - إنشاء خطة استجابة للحوادث السيبرانية.
  - استعادة البيانات في حال فقدانها أو سرقتها.
  - الإبلاغ عن الحوادث السيبرانية.
  - تعلم من أخطاء الماضي لمنع تكرار الحوادث.

1. **مزايا تطبيق برنامج التفكير الابداعي وتقنيات الابتكار**

- تجنب سرقة المعلومات الحساسة مثل كلمات المرور، والبيانات المالية، والمعلومات الطبية من السرقة أو الوصول غير المصرح به.
- تقليل مخاطر الاحتيال المالي، مثل سرقة بطاقات الائتمان أو المعلومات المصرفية.
- منع الفيروسات، وبرامج التجسس، وبرامج الفدية، وغيرها من البرامج الضارة من إلحاق الضرر بالأجهزة والبيانات.
- تجنب فقدان البيانات أو تلفها أو تشفيرها.
- منع الفيروسات، وبرامج التجسس، وبرامج الفدية، وغيرها من البرامج الضارة من إلحاق الضرر بالأجهزة والبيانات.
- تجنب فقدان البيانات أو تلفها أو تشفيرها.
- منع الفيروسات، وبرامج التجسس، وبرامج الفدية، وغيرها من البرامج الضارة من إلحاق الضرر بالأجهزة والبيانات.
- تجنب فقدان البيانات أو تلفها أو تشفيرها.

الفئات المستهدفة

حاصل على درجة البكالوريوس في احد تخصصات تقنية المعلومات المناسبة–
دراسات المعلومات، تقنية المعلومات، علوم الحاسب، هندسة الحاسب الآلي، نظم المعلومات، هندسة البرمجيات، هندسة الشبكات

المهارات الشخصية:

- مهارات التفكير النقدي وحل المشكلات.

- مهارات التواصل والعمل الجماعي.
- مهارات التعلم المستمر والإبداع.
- مهارات أخلاقيات المهنة والثقة بالنفس.

مهارات تقنية:

- اختبار الاختراق وتحليل التهديدات.
- الاستجابة للحوادث والطب الشرعي الرقمي.
- أمن الشبكات وأمن التطبيقات.
- تشفير البيانات.

الاستفادة المؤسسية:

- تجنب سرقة البيانات الحساسة للمؤسسة من السرقة أو الخسارة أو الوصول غير المصرح به.
- ضمان الامتثال للقوانين واللوائح المتعلقة بحماية البيانات، مثل قانون حماية البيانات الشخصية (GDPR) في الاتحاد الأوروبي.
- تجنب الغرامات والعقوبات القانونية التي قد تُفرض على المؤسسة في حال عدم الامتثال للقوانين.
- تقليل مخاطر تسريب البيانات أو اختراقها، مما قد يُلحق الضرر بسمعة المؤسسة ويُعرضها للمساءلة القانونية.
- إظهار التزام المؤسسة بالأمان كعامل تمييز في السوق.
- جذب العملاء والشركاء الذين يُقدرون أهمية الأمن السيبراني.
- تقليل مخاطر انقطاع الأعمال الناجم عن الهجمات السيبرانية، مثل هجمات رفض الخدمة (DDoS) أو هجمات البرامج الضارة.
- ضمان سير العمليات بسلاسة دون تباطؤ أو انقطاع، مما يُحافظ على الإنتاجية ويُقلل من الخسائر المالية.