BLACKBIRD FOR TRAINING

الاستخدام الآمن والمسؤول للذكاء الاصطناعي التوليدي

UK Traininig

PARTNER

www.blackbird-training.com

الاستخدام الآمن والمسؤول للذكاء الاصطناعي التوليدي

مقدمة

مع الانتشار السريع للذكاء الاصطناعي التوليدي في بيئات العمل المختلفة، أصبح من الضروري فهم المخاطر والتحديات المرتبطة باستخدام هذه التقنيات المتطورة. يواجه الموظفون اليوم تحديات جديدة تتعلق بأمن المعلومات، حماية البيانات، والتعامل مع المحتوى المولد آلياً. أصبح الوعي بالأمان والاستخدام المسؤول للذكاء الاصطناعي التوليدي ضرورة ملحة وليس مجرد خيار.

تم تصميم دورة "الاستخدام الآمن والمسؤول للذكاء الاصطناعي التوليدي" لتوعية جميع الموظفين، بغض النظر عن مستوياتهم الوظيفية، بالمخاطر الأمنية والأخلاقية المرتبطة باستخدام أدوات الذكاء الاصطناعي التوليدي مثل Gemini. تهدف الدورة إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لاستخدام هذه الأدوات بأمان، حماية البيانات السرية، التعرف على المعلومات المضللة، والالتزام بالسياسات المؤسسية والأطر الأخلاقية.

هذه الدورة ليست مجرد تدريب تقني، بل هي استثمار في الثقافة الأمنية للمؤسسة، وبناء وعي جماعي حول الاستخدام المسؤول للتكنولوجيا، مما يساهم في حماية سمعة المؤسسة، بياناتها، وموظفيها من المخاطر المتزايدة في العصر الرقمي.

أهداف الدورة

تهدف هذه الدورة إلى تمكين جميع الموظفين من مجموعة متكاملة من المعارف والمهارات الأمنية والأخلاقية، يمكن تلخيصها في الأهداف التالية:

1. فهم المخاطر الأمنية للذكاء الاصطناعي التوليدي: التعرف على مخاطر استخدام أدوات الذكاء الاصطناعي التوليدي، بما في ذلك تسرب البيانات، الاختراقات، وسوء الاستخدام.
2. الإلمام بسياسات الأمان المؤسسية: فهم سياسات SPH Media المتعلقة باستخدام الذكاء الاصطناعي، وحماية البيانات السرية، والامتثال للمعايير التنظيمية.
3. الاستخدام الآمن لأدوات الذكاء الاصطناعي: تعلم كيفية استخدام Gemini وغيرها من أدوات الذكاء الاصطناعي بأمان، بما في ذلك التعامل مع المعلومات الحساسة وتجنب المخاطر الشائعة.
4. اكتشاف المعلومات المضللة: تطوير القدرة على التمييز بين المحتوى البشري والمحتوى المولد بالذكاء الاصطناعي، واستخدام أدوات التحقق من المصادر.
5. فهم الأخلاقيات المرتبطة بالذكاء الاصطناعي: استيعاب مبادئ الشفافية، العدالة، والمسؤولية في استخدام الذكاء الاصطناعي وتطبيقها في بيئة العمل.

بناء ثقافة أمنية مؤسسية: المساهمة في خلق بيئة عمل آمنة ومسؤولة من خلال تبادل الخبرات والتحديات الأمنية مع الزملاء.

مخطط الدورة

المستوى: توعوي جميع المستويات

المدة: يومان 8 ساعات تدريبية

الفئة المستهدفة: جميع الموظفين All Employees

اليوم الأول: أساسيات الأمان والاستخدام المسؤول

1.1 افتتاح الدورة وتعريفها

الموضوعات التي سيتم شرحها:

- الترحيب بالمشاركين وأنشطة كسر الجليد
- استعراض أهداف الدورة والنتائج المتوقعة لجميع الموظفين
- تعريف الذكاء الاصطناعي التوليدي وأهميته في بيئة العمل الحديثة
- أهمية الأمان في عصر الذكاء الاصطناعي التوليدي
- نظرة عامة على المخاطر الأمنية المتزايدة
- تحديد التوقعات والقواعد الأساسية للمشاركة
- استطلاع آراء المشاركين حول تجاربهم السابقة مع أدوات الذكاء الاصطناعي

1.2 أمن المعلومات والخصوصية

الموضوعات التي سيتم شرحها:

- تعريف أمن المعلومات: فهم المفاهيم الأساسية لأمن المعلومات في سياق الذكاء الاصطناعي
- مخاطر استخدام أدوات الذكاء الاصطناعي التوليدي:
  - تسرب البيانات الحساسة بيانات العملاء، المعلومات المالية، الأسرار التجارية
  - مشاركة معلومات سرية دون وعي
  - تخزين البيانات على خوادم خارجية
  - مخاطر الخصوصية للموظفين والعملاء
  - استخدام البيانات لأغراض تدريب النماذج
- أمثلة واقعية على اختراقات وحوادث أمنية:
  - حالات تسرب بيانات من شركات كبرى
  - أمثلة على موظفين شاركوا معلومات سرية مع أدوات الذكاء الاصطناعي
  - عواقب الاختراقات على السمعة والثقة
  - دروس مستفادة من الحوادث السابقة
- أنواع البيانات الحساسة في بيئة العمل:
  - البيانات الشخصية للموظفين والعملاء
  - المعلومات المالية والميزانيات
  - المستندات السرية والعقود
  - الملكية الفكرية والتصاميم
  - استراتيجيات المؤسسة وخططها
- أفضل الممارسات لحماية المعلومات:
  - تصنيف البيانات حسب مستوى الحساسية
  - تحديد ما يمكن مشاركته مع الذكاء الاصطناعي
  - استخدام أدوات آمنة ومعتمدة
  - الالتزام بسياسات الخصوصية
- مسؤولية الموظف في حماية المعلومات:
  - كل موظف هو خط الدفاع الأول
  - الإبلاغ عن الحوادث الأمنية المشتبه بها
  - المشاركة في بناء ثقافة أمنية قوية

1.3 سياسات الأمان في SPH Media

الموضوعات التي سيتم شرحها:

- سياسات استخدام الذكاء الاصطناعي في المؤسسة:
  - الأدوات المسموح باستخدامها
  - الأدوات المحظورة أو المقيدة
  - إجراءات الحصول على الموافقة لاستخدام أدوات جديدة
  - تحديثات السياسات والتغييرات
- حماية البيانات السرية:
  - تعريف البيانات السرية في سياق المؤسسة
  - إجراءات التعامل مع البيانات السرية
  - عقوبات مخالفة سياسات حماية البيانات
  - دور الموظف في حماية السرية
- الامتثال للمعايير التنظيمية:
  - قوانين حماية البيانات المحلية والدولية
  - معايير الأمان في قطاع الطباعة والإعلام
  - متطلبات الامتثال للعملاء والشركاء
- إجراءات الإبلاغ عن الحوادث:
  - كيفية الإبلاغ عن حادث أمني
  - قنوات الإبلاغ المعتمدة
  - الإطار الزمني للإبلاغ
  - سرية الإبلاغ وحماية المبلغين
- تحديثات السياسات والتدريب المستمر:
  - أهمية التحديث الدوري للسياسات
  - التدريب المستمر للموظفين
  - قنوات التواصل للتوعية الأمنية
- أسئلة وأجوبة حول السياسات:
  - فتح النقاش لتوضيح أي غموض في السياسات
  - مشاركة أمثلة عملية لتوضيح التطبيق

1.4 الاستخدام المسؤول لـ Gemini

الموضوعات التي سيتم شرحها:

UK Traininig
PARTNER

- ما هو Gemini؟ نظرة عامة مختصرة على أداة Gemini وقدراتها
- كيفية استخدام Gemini بأمان:
  - عدم مشاركة معلومات شخصية أو سرية
  - عدم تحميل مستندات حساسة
  - استخدام النسخة المؤسسية الآمنة إن وجدت
  - تسجيل الخروج بعد الاستخدام
  - استخدام كلمات مرور قوية
- التعامل مع المعلومات الحساسة:
  - تحديد المعلومات التي لا يجب مشاركتها مع Gemini
  - تقنيات إخفاء الهوية عند الحاجة لمشاركة البيانات
  - استخدام البيانات الاصطناعية في الاختبارات
  - توثيق ما تم مشاركته مع الذكاء الاصطناعي
- أخطاء شائعة يجب تجنبها:
  - مشاركة معلومات تعريفية شخصية
  - تحميل مستندات داخلية حساسة
  - استخدام Gemini في المهام غير المسموح بها
  - الاعتماد على المخرجات دون التحقق
- إعدادات الخصوصية والأمان:
  - ضبط إعدادات الخصوصية في حساب Gemini
  - فهم سياسات الاحتفاظ بالبيانات
  - خيارات حذف المحادثات والبيانات
- إرشادات عملية للاستخدام اليومي:
  - قائمة مراجعة قبل استخدام Gemini
  - خطوات للاستخدام الآمن في المهام اليومية
  - التعامل مع المخرجات بحذر
- دراسات حالة:
  - أمثلة على استخدام آمن لـ Gemini
  - أمثلة على استخدام غير آمن والعواقب

1.5 تمارين عملية - سيناريوهات أمنية

الموضوعات التي سيتم شرحها:

- التمرين 1: سيناريو تسرب بيانات محتمل:
  - قراءة سيناريو حول موظف شارك معلومات سرية مع Gemini
  - تحليل الموقف: ما الخطأ الذي حدث؟
  - تحديد العواقب المحتملة
  - اقتراح الإجراءات التصحيحية
- التمرين 2: سيناريو بريد إلكتروني مشبوه:
  - تحليل بريد إلكتروني يدعي أنه من Gemini
  - تحديد علامات الاحتيال والتصيد
  - الإجراءات الصحيحة للتعامل مع البريد
- التمرين 3: سيناريو مشاركة مستند:
  - تقييم ما إذا كان مستند معين آمناً للمشاركة مع Gemini
  - تحديد المعلومات الحساسة في المستند
  - اقتراح بدائل آمنة للمشاركة
- التمرين 4: سيناريو اختراق:
  - ماذا تفعل إذا اكتشفت أن حساب Gemini الخاص بك قد تم اختراقه؟
  - خطوات الاستجابة للحوادث
  - قنوات الإبلاغ والإجراءات
- التمرين 5: سيناريو سياسة جديدة:
  - تطبيق سياسة أمان جديدة على سيناريو عمل واقعي
  - تحديد التحديات في التطبيق
  - اقتراح تحسينات للسياسة
- مناقشة مخرجات التمارين:
  - مشاركة الحلول مع المجموعة
  - تغذية راجعة من المدرب والزملاء
  - استخلاص الدروس المستفادة

1.6 مناقشة جماعية - تبادل الخبرات والتحديات الأمنية

الموضوعات التي سيتم شرحها:

- تبادل الخبرات الشخصية:
  - مشاركة تجارب المشاركين مع أدوات الذكاء الاصطناعي
  - التحديات الأمنية التي واجهوها
  - الحلول التي استخدموها
- التحديات الأمنية الشائعة في بيئة العمل:
  - تحديد التحديات المتكررة
  - تحليل الأسباب الجذرية
  - اقتراح حلول مشتركة
- أفضل الممارسات من المشاركين:
  - نصائح وتجارب ناجحة
  - إجراءات وقائية فعالة
  - أدوات وتقنيات مفيدة
- سيناريوهات افتراضية للنقاش:
  - ماذا لو واجهت موقفاً أمنياً معيناً؟
  - كيف ستتعامل معه؟
  - ما هي الدروس المستفادة؟
- بناء شبكة أمان داخلية:
  - تشجيع التعاون بين الزملاء في القضايا الأمنية
  - إنشاء قنوات لمشاركة المعلومات الأمنية
  - دعم بعضهم البعض في التحديات الأمنية
- توصيات جماعية:
  - اقتراح تحسينات للسياسات والإجراءات
  - مبادرات لتعزيز الثقافة الأمنية
  - خطوات عملية للتحسين

1.7 ملخص اليوم الأول وجلسة أسئلة وأجوبة

الموضوعات التي سيتم شرحها:

UK Traininig
PARTNER

- مراجعة شاملة لمفاهيم اليوم الأول:
  - مخاطر أمن المعلومات والخصوصية
  - سياسات الأمان في SPH Media
  - الاستخدام المسؤول لـ Gemini
  - السيناريوهات الأمنية والتحديات
- تلخيص النقاط الرئيسية:
  - كل موظف هو خط الدفاع الأول
  - الوعي الأمني هو أفضل حماية
  - الإبلاغ الفوري عن الحوادث
- الإجابة على أسئلة واستفسارات المشاركين
- معاينة محتوى اليوم الثاني المعلومات المضللة والأخلاقيات
- مهام تحضيرية لليوم التالي إن وجدت

اليوم الثاني: المعلومات المضللة والأخلاقيات

2.1 مراجعة واستذكار اليوم الأول

الموضوعات التي سيتم شرحها:

- استرجاع سريع للمفاهيم الرئيسية من اليوم الأول من خلال أسئلة تفاعلية
- مراجعة سياسات الأمان والاستخدام المسؤول
- مشاركة تجارب المشاركين بعد اليوم الأول
- الإجابة على أي استفسارات متبقية
- تهيئة الأجواء لموضوعات اليوم الثاني
- ربط مفاهيم اليوم الأول بالأخلاقيات والمعلومات المضللة

2.2 التمييز بين المحتوى البشري والمولد بالذكاء الاصطناعي

الموضوعات التي سيتم شرحها:

UK Traininig
PARTNER

- فهم المحتوى المولد بالذكاء الاصطناعي:
  - كيف يعمل توليد المحتوى بالذكاء الاصطناعي
  - أنواع المحتوى المولد نصوص، صور، فيديو، صوت
  - قدرات الذكاء الاصطناعي في توليد محتوى واقعي
- المعلومات المضللة والعمق المزيف Deepfakes:
  - تعريف المعلومات المضللة
  - أمثلة على عمق مزيف صور وفيديوهات مزيفة
  - تأثير المعلومات المضللة على الأفراد والمؤسسات
  - عواقب انتشار المعلومات المضللة
- أدوات التحقق من المحتوى:
  - أدوات اكتشاف المحتوى المولد بالذكاء الاصطناعي
  - أدوات التحقق من الصور والفيديوهات
  - أدوات التحقق من المصادر والمراجع
  - أدوات تحليل الميتاداتا
- علامات التحذير للمحتوى المشبوه:
  - أخطاء لغوية أو منطقية
  - معلومات غير دقيقة أو قديمة
  - مصادر غير موثوقة
  - طلب معلومات شخصية
  - محتوى عاطفي مفرط
- استراتيجيات التحقق من المعلومات:
  - التحقق من المصادر
  - البحث العكسي عن الصور
  - مقارنة المعلومات مع مصادر موثوقة
  - استخدام أدوات التحقق المتخصصة
  - التشكيك في المعلومات غير المعتادة
- مسؤولية الموظف في نشر المعلومات:
  - التحقق قبل المشاركة
  - عدم نشر معلومات غير مؤكدة
  - الإبلاغ عن المعلومات المضللة
  - تعزيز ثقافة التحقق في بيئة العمل

UK Traininig
PARTNER

2.3 تمارين عملية - تحليل محتوى مشبوه

الموضوعات التي سيتم شرحها:

- التمرين 1: تحليل نص مشبوه:
  - قراءة نص مولد بالذكاء الاصطناعي
  - تحديد العلامات التي تشير إلى أنه مولد آلياً
  - التحقق من المصادر والمراجع المذكورة
  - تقييم موثوقية المحتوى
- التمرين 2: تحليل صورة مشبوهة:
  - فحص صورة قد تكون معدلة أو مولدة
  - استخدام أدوات البحث العكسي عن الصور
  - تحليل الميتاداتا إن وجدت
  - تحديد ما إذا كانت الصورة حقيقية أم مزيفة
- التمرين 3: تحليل فيديو قصير:
  - مشاهدة مقطع فيديو قد يكون عمقاً مزيفاً
  - تحديد علامات التلاعب
  - استخدام أدوات التحقق من الفيديو
  - تقييم مصداقية الفيديو
- التمرين 4: تحليل بريد إلكتروني مشبوه:
  - قراءة بريد إلكتروني يحتوي على معلومات مضللة
  - تحديد علامات الاحتيال
  - التحقق من عنوان المرسل والمصادر
  - الإجراءات الصحيحة للتعامل مع البريد
- التمرين 5: تحليل منشور على وسائل التواصل:
  - تحليل منشور على وسائل التواصل الاجتماعي
  - التحقق من صحة المعلومات
  - تحديد الدوافع المحتملة للمنشور
  - كيفية الرد أو التعامل مع المنشور
- مناقشة النتائج:
  - مشاركة نتائج التحليل مع المجموعة
  - مناقشة التحديات في التحقق
  - استخلاص الدروس المستفادة
  - تطوير استراتيجيات تحقق أفضل

UK Traininig
PARTNER

2.4 أخلاقيات الذكاء الاصطناعي التوليدي

الموضوعات التي سيتم شرحها:

- مبادئ الأخلاقيات الأساسية:
  - الشفافية: الكشف عن استخدام الذكاء الاصطناعي
  - العدالة: تجنب التحيز والتمييز
  - المسؤولية: تحمل مسؤولية المخرجات
  - الخصوصية: احترام خصوصية الأفراد
  - الأمان: حماية البيانات والأنظمة
- الشفافية في استخدام الذكاء الاصطناعي:
  - الإفصاح عن استخدام المحتوى المولد بالذكاء الاصطناعي
  - توضيح دور الذكاء الاصطناعي في القرارات
  - شرح كيفية عمل النماذج للمستخدمين
  - الشفافية مع الزملاء والعملاء
- العدالة وتجنب التحيز:
  - فهم التحيز في نماذج الذكاء الاصطناعي
  - كيفية اكتشاف التحيز في المخرجات
  - تأثير التحيز على القرارات والموظفين
  - استراتيجيات تقليل التحيز
- المسؤولية تجاه الزملاء والشركة:
  - التأكد من دقة مخرجات الذكاء الاصطناعي
  - عدم الاعتماد الأعمى على الذكاء الاصطناعي
  - الإبلاغ عن الأخطاء والمشاكل
  - حماية سمعة المؤسسة
- المسؤولية تجاه العملاء والمجتمع:
  - حماية بيانات العملاء
  - تقديم معلومات دقيقة وموثوقة
  - الشفافية مع العملاء حول استخدام الذكاء الاصطناعي
  - المساهمة في الاستخدام الإيجابي للتكنولوجيا
- الأطر الأخلاقية في المؤسسة:
  - سياسات الأخلاقيات للذكاء الاصطناعي
  - لجان الأخلاقيات والرقابة
  - إجراءات المراجعة الأخلاقية للمشاريع
  - التدريب المستمر على الأخلاقيات

UK Traininig
PARTNER

- دراسات حالة أخلاقية:
  - أمثلة على معضلات أخلاقية في بيئة العمل
  - تحليل القرارات الأخلاقية
  - العواقب المحتملة للقرارات غير الأخلاقية
  - الدروس المستفادة من الحالات السابقة

2.5 ورشة عمل تفاعلية - حالات أخلاقية معقدة

الموضوعات التي سيتم شرحها:

- هيكل ورشة العمل:
  - تقسيم المشاركين إلى مجموعات صغيرة
  - تخصيص حالة أخلاقية معقدة لكل مجموعة
  - وقت للتحليل والمناقشة الجماعية
  - عرض النتائج والتوصيات
- حالات أخلاقية نموذجية:
  - الحالة 1: استخدام الذكاء الاصطناعي في التوظيف:
    - استخدام الذكاء الاصطناعي لتصفية المتقدمين للوظائف
    - مخاطر التحيز في عملية التوظيف
    - كيفية ضمان العدالة في التوظيف المدعوم بالذكاء الاصطناعي
  - الحالة 2: المحتوى المولد بالذكاء الاصطناعي في التسويق:
    - استخدام الذكاء الاصطناعي لتوليد محتوى تسويقي
    - الشفافية مع العملاء حول المحتوى المولد
    - مخاطر التضليل في التسويق
  - الحالة 3: خصوصية الموظفين:
    - استخدام الذكاء الاصطناعي لمراقبة أداء الموظفين
    - التوازن بين المراقبة والخصوصية
    - سياسات واضحة للخصوصية في مكان العمل
  - الحالة 4: أمان البيانات في المشاريع المشتركة:
    - مشاركة بيانات مع شركاء خارجيين باستخدام الذكاء الاصطناعي
    - حماية البيانات السرية في التعاونات
    - الاتفاقيات الأمنية والأخلاقية
  - الحالة 5: المسؤولية عن أخطاء الذكاء الاصطناعي:
    - من يتحمل المسؤولية عندما يخطئ الذكاء الاصطناعي؟
    - إجراءات التعامل مع الأخطاء
    - التعلم من الأخطاء وتحسين النماذج
- منهجية التحليل الأخلاقي:
  - تحديد القيم الأخلاقية المتضاربة
  - تحليل الخيارات المتاحة
  - تقييم العواقب المحتملة لكل خيار
  - اختيار الحل الأكثر أخلاقية
  - وضع خطة لتنفيذ الحل

UK Traininig
PARTNER

- عروض المجموعات ومناقشتها:
  - عرض تحليل كل مجموعة للحالة
  - مناقشة وجهات النظر المختلفة
  - تغذية راجعة من المدرب والزملاء
  - استخلاص الدروس الأخلاقية الرئيسية
- تطوير سياسات أخلاقية:
  - اقتراح سياسات أخلاقية للتعامل مع الحالات المماثلة
  - توصيات لتحسين الممارسات الحالية
  - خطوات لتعزيز الثقافة الأخلاقية في المؤسسة

2.6 ملخص الدورة والتقييم والاختتام

الموضوعات التي سيتم شرحها:

- مراجعة شاملة:
  - تلخيص مفاهيم اليوم الأول أساسيات الأمان
  - تلخيص مفاهيم اليوم الثاني المعلومات المضللة والأخلاقيات
  - ربط جميع المفاهيم في إطار متكامل
  - إعادة التأكيد على النقاط الرئيسية
- الوجبات الرئيسية من الدورة:
  - الأمان هو مسؤولية الجميع
  - التحقق من المعلومات قبل المشاركة
  - الشفافية والأخلاقيات في استخدام الذكاء الاصطناعي
  - الإبلاغ عن الحوادث والمخاوف الأمنية
- اختبار قصير:
  - تقييم المعرفة والمفاهيم الأمنية والأخلاقية
  - أسئلة حول سياسات الأمان
  - أسئلة حول اكتشاف المعلومات المضللة
  - أسئلة حول الأخلاقيات والاستخدام المسؤول
  - تغذية راجعة فورية وشرح للإجابات
- استبيان تقييم الدورة:
  - جمع آراء المشاركين حول جودة المحتوى، أداء المدرب، والمواد التدريبية
  - تقييم مدى فائدة الدورة للمشاركين
  - اقتراحات للتحسين
  - تحديد احتياجات تدريبية إضافية
- توصيات واستمرارية:
  - خطوات عملية لتطبيق ما تم تعلمه
  - موارد للتعلم المستمر حول الأمان والأخلاقيات
  - قنوات للإبلاغ عن المخاوف الأمنية والأخلاقية
  - تشجيع المشاركة في المبادرات الأمنية
- توزيع الشهادات:
  - منح شهادات إتمام الدورة للمشاركين
  - تقدير التزامهم وجهودهم في تعزيز الأمان والمسؤولية

الخاتمة

في ختام هذه الدورة، سيكون المشاركون قد اكتسبوا فهماً عميقاً للمخاطر الأمنية والأخلاقية المرتبطة باستخدام الذكاء الاصطناعي التوليدي، وأصبحوا مجهزين بالمعرفة والمهارات اللازمة لاستخدام هذه الأدوات بأمان ومسؤولية في بيئة العمل.

UK Training
PARTNER

من خلال فهم مخاطر أمن المعلومات، سياسات الأمان المؤسسية، والتعامل الآمن مع Gemini، أصبح المشاركون قادرين على حماية أنفسهم ومؤسستهم من التهديدات المتزايدة. كما أن قدرتهم على التمييز بين المحتوى البشري والمولد بالذكاء الاصطناعي، والالتزام بالمبادئ الأخلاقية، تجعلهم جزءاً من الحل في مواجهة تحديات العصر الرقمي.

إن بناء ثقافة أمنية وأخلاقية قوية هو استثمار في مستقبل المؤسسة. كل موظف هو خط دفاع أساسي في حماية البيانات، السمعة، والثقة التي بنتها المؤسسة مع عملائها وشركائها. هذه الدورة هي خطوة مهمة في تعزيز هذه الثقافة وضمان استخدام الذكاء الاصطناعي كأداة إيجابية وآمنة في تحقيق أهداف المؤسسة.