



Home



# خصوصية البيانات ومخاطر جمعها بطرق غير قانونية



created by Danya Musbah

12/12/2024

# Table of Content



01. مقدمة

02. المخاطر المرتبطة بجمع البيانات بطرق غير قانونية

03. خصوصية الذكاء الاصطناعي

04. التحديات الأخلاقية المرتبطة بخصوصية البيانات ومخاطر جمعها بطرق غير قانونية على الأفراد والمجتمع

# Table of Content



05. أمثله وحالات دراسية

06. أساليب حماية البيانات من الوصول الغير قانوني

07. أهم القوانين والمعايير المهنية في هندسة البرمجيات

08. توصيات لمهندسي البرمجيات و أهمية الالتزام بالأخلاقيات في مجال هندسة البرمجيات



في العصر الرقمي الذي نعيش فيه، أصبحت البيانات هي العملة الجديدة. مع تزايد استخدام التكنولوجيا في كل جانب من جوانب حياتنا، من الأعمال التجارية إلى الترفيه والتعليم، أصبحت حماية البيانات والخصوصية أمراً بالغ الأهمية.

خصوصية البيانات تعتبر واحدة من القضايا الأكثر أهمية في العصر الرقمي. تتعلق بحماية المعلومات الشخصية للأفراد من الوصول غير المصرح به أو الاستخدام غير القانوني.



# ماهي خصوصية البيانات

خصوصية البيانات تعني حماية المعلومات الشخصية للأفراد من الوصول غير المصرح به أو الاستخدام غير المشروع. تشمل هذه المعلومات البيانات الشخصية مثل الاسم، العنوان، رقم الهاتف، بريد الكتروني، وأي معلومات تتعلق بالحياة الشخصية. خصوصية البيانات والمعروفة أيضاً باسم خصوصية المعلومات، هي مبدأ مفاده أنه يجب على الشخص التحكم في بياناته الشخصية.







05/28



جمع البيانات بطرق غير قانونية يمكن أن يؤدي إلى مخاطر كبيرة للأفراد والمجتمعات. يمكن أن تتضمن انتهاك الخصوصية، الاحتيال الإلكتروني، و سرقة الهوية. هذه الأنشطة يمكن أن تؤدي إلى انتهاكات للخصوصية، السرية، وحقوق الأفراد، وتسبب أضراراً مالية ونفسية.

# المخاطر المرتبطة بجمع البيانات بطرق غير قانونية

سرقة الهوية

الاختيال الإلكتروني

الأضرار المالية

انتهاك الخصوصية





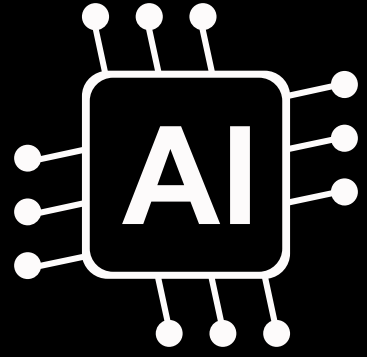
# Q خصوصية الذكاء الاصطناعي



خصوصية الذكاء الاصطناعي هي ممارسة حماية المعلومات الشخصية أو الحساسة التي يتم جمعها أو استخدامها أو مشاركتها أو تخزينها بواسطة الذكاء الاصطناعي.

ترتبط خصوصية الذكاء الاصطناعي ارتباطًا وثيقًا بخصوصية البيانات.





# مخاطر خصوصية الذكاء الاصطناعي



جمع البيانات الحساسة

جمع البيانات دون موافقة

استخدام البيانات دون إذن

تسرب البيانات

المراقبة والتحيز غير المراقب

استخلاص البيانات

## التدابير المؤقتة التي اتخذتها الصين لإدارة خدمات الذكاء الاصطناعي التوليدي

وتعد الصين من بين الدول الأولى التي سنت لوائح خاصة بالذكاء الاصطناعي. وفي عام 2023، أصدرت الصين تدابيرها المؤقتة لإدارة خدمات الذكاء الاصطناعي التوليدي. وبموجب القانون، "يجب أن يحترم توفير واستخدام خدمات الذكاء الاصطناعي التوليدي الحقوق والمصالح المشروعة للآخرين ويشترط عدم تعريض الصحة البدنية والعقلية للآخرين للخطر، وعدم التعدي على حقوق صورة الآخرين وحقوق سمعتهم. وحقوق الشرف وحقوق الخصوصية وحقوق المعلومات الشخصية".





# التحديات الأخلاقية



# التحديات الأخلاقية الرئيسية



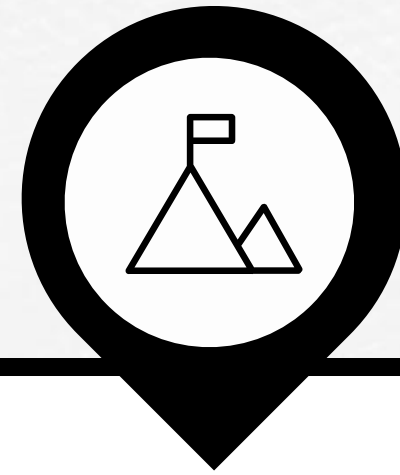
## الاستغلال التجاري

استخدام البيانات الشخصية لأغراض تجارية بطرق غير أخلاقية، مثل الاستهداف الإعلاني المضلل أو التلاعب بالرأي العام، يثير تساؤلات حول أخلاقية استخدام البيانات.



## الأمان السيرياني الضعيف

الفشل في حماية البيانات بشكل كافٍ من الهجمات السيريانية يمكن أن يؤدي إلى تسريب بيانات حساسة واستخدامها بطرق ضارة.



## عدم الشفافية

عدم وضوح السياسات والممارسات المتعلقة بجمع واستخدام البيانات يمكن أن يؤدي إلى فقدان الثقة بين الأفراد والمؤسسات.



## انتهاك الخصوصية

جمع البيانات بطرق غير قانونية ينتهك حق الأفراد في الخصوصية، حيث يتم جمع معلوماتهم الشخصية بدون موافقة صريحة.



# التحديات الأخلاقية الرئيسية



## الوصول غير المصرح

يُمنح الوصول غير المصرح به إلى البيانات الشخصية انتهاكًا صارخًا للخصوصية.



## انعدام المساءلة

غياب الآليات المناسبة للمساءلة والرقابة يمكن أن يؤدي إلى سوء استخدام البيانات بدون عواقب حقيقية على الجهات الفاعلة.



## التحيز والتمييز

جمع البيانات وتحليلها بطرق غير قانونية يمكن أن يعزز من التحيز والتمييز، خاصة إذا كانت البيانات تستخدم لاتخاذ قرارات تؤثر على مجموعات معينة من الناس بطرق غير عادلة.



## تأثيرات نفسية واجتماعية

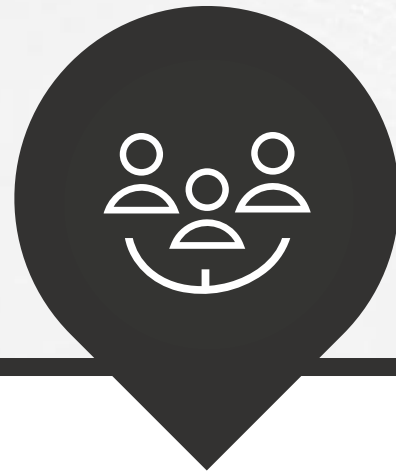
تعرض الأفراد لمخاطر جمع البيانات بطرق غير قانونية يمكن أن يؤدي إلى تأثيرات نفسية سلبية، مثل القلق، بالإضافة إلى التأثيرات الاجتماعية مثل التمييز والاستبعاد.

# التحديات الأخلاقية الرئيسية



## الاستغلال والتلاعب

يمكن أن تُستخدم المعلومات الشخصية للتأثير على قرارات الأفراد وأفعالهم بطرق غير أخلاقية



## المسؤولية الاجتماعية

يتحمل مهندسو البرمجيات مسؤولية اجتماعية كبيرة في ضمان استخدام التقنيات التي طورونها بطرق أخلاقية.



## انتهاك الثقة

يؤدي جمع البيانات بطرق غير قانونية إلى فقدان الثقة بين الأفراد والمؤسسات



## استخدام البيانات لأغراض غير مشروعة

مثل الاحتيال والابتزاز والتلاعب بالرأي العام.



تؤثر التحديات الأخلاقية المرتبطة بخصوصية البيانات ومخاطر جمعها بطرق غير قانونية على الأفراد والمجتمع بطرق متعددة. بعض الآثار المحتملة

## على الفرد

04

### التمييز والتحيز

استخدام البيانات الشخصية بطرق غير مشروعة يمكن أن يعزز من التحيز والتمييز، حيث يمكن أن تُستخدم هذه البيانات لاتخاذ قرارات تمييزية في مجالات مثل التوظيف، التأمين، أو الخدمات الصحية.

03

### التأثير النفسي

الشعور بفقدان السيطرة على البيانات الشخصية يمكن أن يسبب قلقًا نفسيًا واكتئابًا لدى الأفراد، خاصة إذا تعرضوا للاختراق أو التهديد بنشر معلوماتهم.

02

### الأضرار المالية

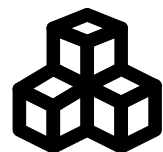
قد يتعرض الأفراد لخسائر مالية نتيجة للاحتيال باستخدام بياناتهم المسروقة، مثل سحب الأموال من حساباتهم أو استخدام بطاقاتهم الائتمانية دون إذن.

01

### سرقة الهوية

يمكن أن يؤدي تسريب البيانات الشخصية إلى سرقة الهوية، مما قد يؤدي إلى استخدام المعلومات الشخصية بشكل غير قانوني لفتح حسابات بنكية، طلب قروض، أو تنفيذ عمليات احتيالية باسم الفرد.

## انعدام الثقة



عندما تتعرض المؤسسات لاختراقات بيانات أو تُكتشف أنها تجمع البيانات بطرق غير قانونية، فإن ذلك يضعف الثقة بين المواطنين والحكومات أو الشركات، مما يؤثر سلبًا على التعاون المجتمعي.

## التلاعب بالمعلومات



يمكن استخدام البيانات المجمعة بطرق غير قانونية للتلاعب بالرأي العام أو التأثير على الانتخابات، مما يهدد الأسس الديمقراطية للمجتمع.

## الأمن الوطني



تسريب البيانات الشخصية يمكن أن يشكل تهديدًا للأمن الوطني، خاصة إذا استخدمت جهات خارجية هذه البيانات لتحقيق أهداف عدائية.

## الفجوة الرقمية



بعض الأفراد أو المجتمعات قد يكونون أكثر عرضة لجمع البيانات بطرق غير قانونية بسبب قلة الوعي أو قلة الموارد المتاحة لحمايتهم، مما يعزز الفجوة الرقمية بين الأفراد والمجتمعات.



# أمثلة وحالات دراسية

# اختراق شركة إكويفاكس (Equifax)

The Equifax logo is centered within a dark red rounded square. The word "EQUIFAX" is written in a bold, white, sans-serif font. A registered trademark symbol (®) is located to the upper right of the word.

**EQUIFAX®**



كيف تم التعامل مع  
الحالة

غرامات كبيرة  
إعادة بناء الثقة  
التوعية

**EQUIFAX®**

وافقت وكالة الائتمان Equifax على دفع غرامات تصل إلى 700 مليون دولار كتسوية مع السلطات الفدرالية الأمريكية (FTC) بسبب خرق تعرض له بيانات مستخدميها في مايو عام 2017, كان قد تم الكشف عن الاختراق في سبتمبر عام 2019, بعد فشل الوكالة في إغلاق الثغرة الأمنية التي أدت إلى الاختراق, التي كانت على علم بها في مارس 2017, ويعتبر ذلك الاختراق الأسوأ في تاريخ الولايات المتحدة. حيث كشفت الوكالة عن معلومات شخصية لأكثر من 147 مليون شخص, بما في ذلك الأسماء وتواريخ الميلاد والعناوين وأرقام الضمان الاجتماعي. وذكرت الشركة أنها وافقت على تقديم خدمات مراقبة الائتمان مجانًا لمدة 10 سنوات, للمستهلكين المتضررين من هذا الخرق, وبالإضافة إلى مدفوعات نقدية تصل إلى 20 ألف دولار للشخص الواحد.



### التحديات الأخلاقية

الأمان السيبراني الضعيف  
انتهاك الخصوصية  
عدم الشفافية  
الأضرار المالية والنفسية

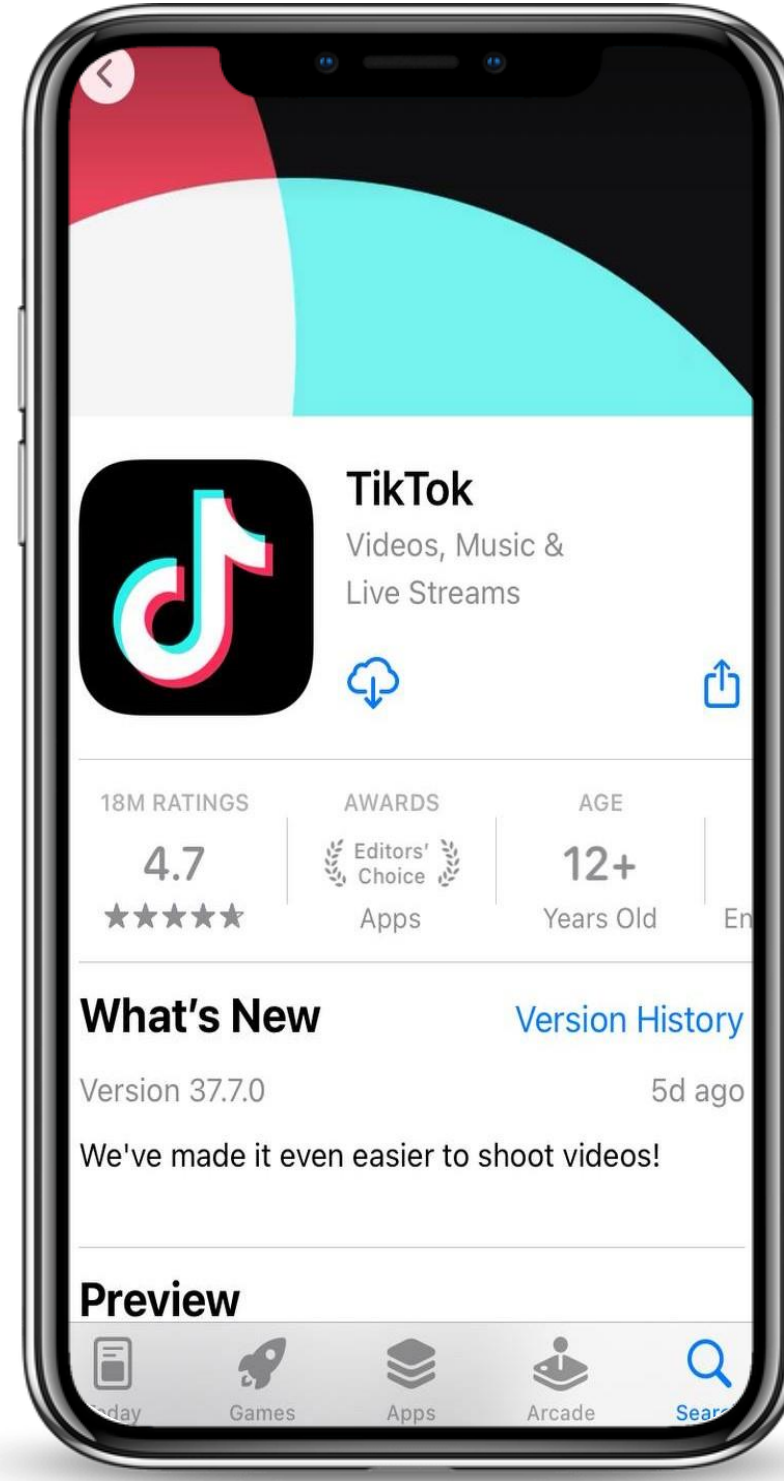
### كيفية جمع البيانات

قامت "إكويفاكس" بجمع البيانات الائتمانية والمعلومات الشخصية للأفراد من خلال مصادر متعددة مثل البنوك, شركات بطاقات الائتمان, والمقرضين. الغرض من جمع هذه البيانات هو تقديم تقارير ائتمانية للشركات التي تحتاج إلى تقييم الجدارة الائتمانية للأفراد.





# انتهاك الخصوصية في شركة TikTok



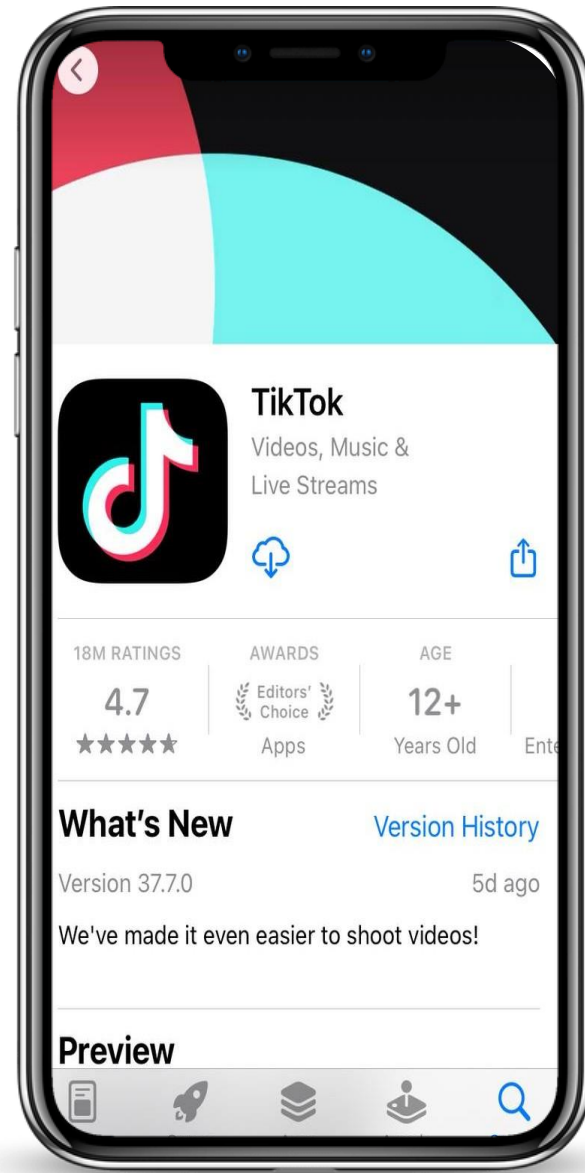
كيف تم التعامل مع الحالة

الغرامات والتنظيم

القيود والحظر

تعزيز سياسات الخصوصية

التعاون مع السلطات



في عام 2020، واجهت الشركة تحقيقات متعددة بخصوص كيفية جمعها واستخدامها لبيانات المستخدمين، وخاصة الأطفال.

صدرت لجنة حماية البيانات الأيرلندية -إحدى كبرى الهيئات الرقابية الأوروبية- قراراً بتغريم شركة «تيك توك» 345 مليون يورو (أي ما يعادل 368 مليون دولار)، بسبب فشل التطبيق في اتخاذ التدابير اللازمة لحماية المستخدمين الأطفال.

كانت اللجنة التي تراقب أنشطة التطبيق في دول الاتحاد الأوروبي قد أجرت تحقيقاً خلُص إلى أن إعدادات «تيك توك» على 2020 تيك توك» الافتراضية لم تكن كافية لحماية حسابات الأطفال خلال النصف الأخير من عام 2020. سبيل المثال، تظهر الملفات الشخصية الحديثة للأطفال للعامة بشكلٍ كامل، ما يعني أنه يمكن لأي شخص على الإنترنت مشاهدتها

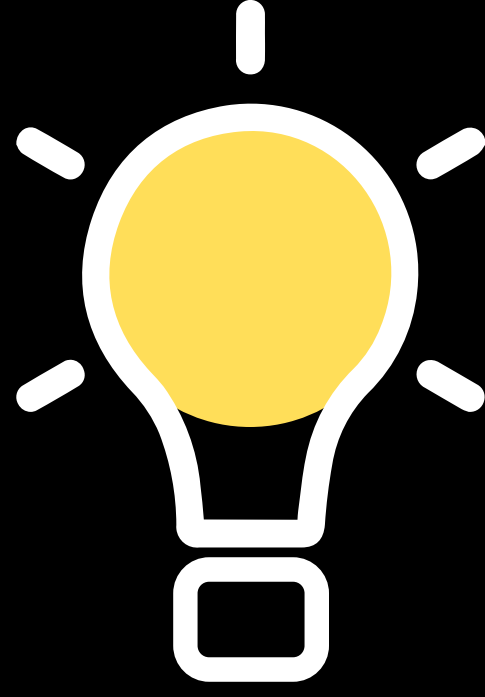
التحديات الأخلاقية

جمع البيانات من القاصرين  
الأمان السيبراني الضعيف  
انعدام الشفافية

كيفية جمع البيانات

تيكتوك يقوم بجمع مجموعة واسعة من البيانات بما في ذلك معلومات الحساب، الفيديوهات المنشورة، التفضيلات، المواقع الجغرافية، وسجل البحث. هذه البيانات تُستخدم لتحسين تجربة المستخدم وتوجيه الإعلانات المخصصة.





الحلول



# أساليب حماية البيانات من الوصول الغير قانوني

حافظ على تحديث كافة تصحيحات الأمان

كشف الاختراقات والرد عليها بسرعة

تنفيذ مبدأ الامتيازات الأقل (تقليل الوصول إلى البيانات)

استخدام المصادقة متعددة العوامل

تنفيذ القائمة البيضاء لعناوين IP

تشفير حركة مرور الشبكة داخل النظام

تشفير البيانات في حالة الراحة

استخدام جدران الحماية



More



# The Eight IEEE/ACM Codes of Ethics

---



21/28



أصبح تطبيق مدونة أخلاقيات هندسة البرمجيات الحالية أمراً صعباً للتنفيذ على أساس يومي نظراً لأنها على مستوى عالٍ.

تم إجراء دراسة بحثية من خلال شركة لتطوير مشاريع البرمجيات المعروفة باسم دراسة حالة SADAasa في المملكة العربية السعودية. بحث من قبل مطوري البرمجيات. واستخدم الباحثون المقابلات والإستبيانات ومصادر المعلومات الثانويه. وباستخدام هذه الأدوات، قام الباحثون بتحليل واقتراح تصنيفات جديدة له حسب دورات حياة تطوير البرمجيات. أخذ الباحثون المبادئ الأربعة لمدونة الأخلاقيات (العام، العميل وصاحب العمل، المنتج، والحكم) وصنفوها بناءً على المتطلبات الهندسية، والتصميم، والتعليمات والاختبار، ومرحلة صيانة واقتروا حلولاً جديدة.



# القوانين والتشريعات

قوانين حماية البيانات الشخصية

GDPR: قانون حماية البيانات العامة في الاتحاد الأوروبي

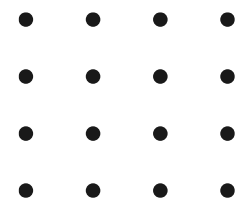
CCPA: قانون خصوصية المستهلك في كاليفورنيا

قوانين الملكية الفكرية

أكواد السلوك المهني

قانون الاتحاد الأوروبي للذكاء الاصطناعي





# معايير أمن المعلومات

01.

ISO/IEC 27001

يحدد متطلبات نظام إدارة الأمن للمعلومات

02.

PCI DSS

يركز على أمن بيانات بطاقات الدفع



# كيفية الالتزام بهذه المعايير في العمل اليومي

الابلاغ عن المخالفات



توثيق العمل



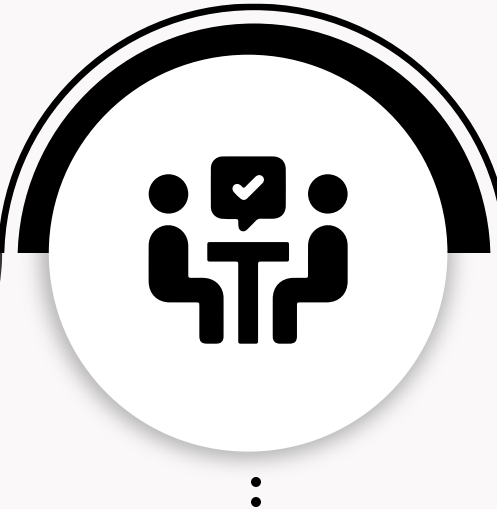
التدريب المستمر



الالتزام بأكواد السلوك  
المهني



التعاون مع فريق  
العمل



التعرف على المعايير







## تحديات الالتزام بالمعايير

الضغط لإنجاز المشاريع.  
التغيرات التكنولوجية السريعة.  
التنوع الثقافي.

## الالتزام بالمعايير في العمل اليومي



التدريب والتوعية  
التقييم الدوري.  
الاستجابة السريع.



# توصيات لمهندسي البرمجيات



1. الالتزام بالمعايير والقوانين.
2. الالتزام بالمعايير المهنية لإدارة أمن المعلومات.
3. تصميم البرامج مع مراعاة الخصوصية.
4. تقليل جمع البيانات.
5. توفير الشفافية.
6. تأكد من الحصول على موافقة صريحة من المستخدمين قبل جمع أي بيانات شخصية.
7. تطبيق أفضل ممارسات الأمان السيبراني ,استخدم تقنيات التشفير القوية لحماية البيانات أثناء النقل والتخزين ,حافظ على أنظمة البرمجيات محدثة بآخر التحديثات الأمنية لتجنب الثغرات الأمنية.
8. قدم تدريبات دورية لفريقك حول أهمية حماية البيانات وطرق التعامل الآمن معها.
9. زود المستخدمين بمعلومات حول كيفية حماية بياناتهم وأهمية الخصوصية.
10. اجري مراقبة مستمرة لأنظمة البرمجيات لاكتشاف أي نشاط غير طبيعي أو تهديدات.
11. إنشاء آليات للمسائلة تسمح للمستخدمين بالإبلاغ عن انتهاكات الخصوصية وضمان التحقيق فيها ومعالجتها.



# أهمية الالتزام بالأخلاقيات في مجال هندسة البرمجيات

1. حماية حقوق الأفراد.
2. تعزيز الثقة بين المستخدمين والمؤسسات.
3. تقليل المخاطر القانونية والمالية.
4. تحسين جودة المنتجات والخدمات.
5. الوقاية من التحيز والتمييز.
6. المساهمة في النفع العام.
7. مواجهة التحديات الأخلاقية بكفاءة.







Home



# Thank You.

We hope this presentation has  
provided useful information

---

