# الأمن السيبراني في التكنولوجيا المالية

مرحبًا بكم في هذا العرض التقديمي حول الأمن السيبراني في مجال التكنولوجيا المالية. سنستكشف معًا أهمية الأمن السيبراني في هذا القطاع الحيوي، ونتعرف على التحديات الفريدة التي تواجهها المؤسسات المالية في العصر الرقمي. سنناقش أيضًا أحدث التقنيات والأساليب المستخدمة لحماية البيانات المالية الحساسة.

**by Abdelhak Lefilef**

# ما هو الأمن السيبراني؟

### مواجهة التهديدات المتطورة

يتطور باستمرار لمواجهة التهديدات الجديدة والمتقدمة في العالم الرقمي.

### ضمان سرية البيانات

يهدف إلى الحفاظ على سرية وسلامة وتوافر البيانات ضد محاولات الاختراق أو السرقة.

### حماية الأنظمة والشبكات

مجموعة من الممارسات والتقنيات لحماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية.

# خصوصية الأمن السيبراني في التكنولوجيا المالية

### مواجهة الهجمات المالية

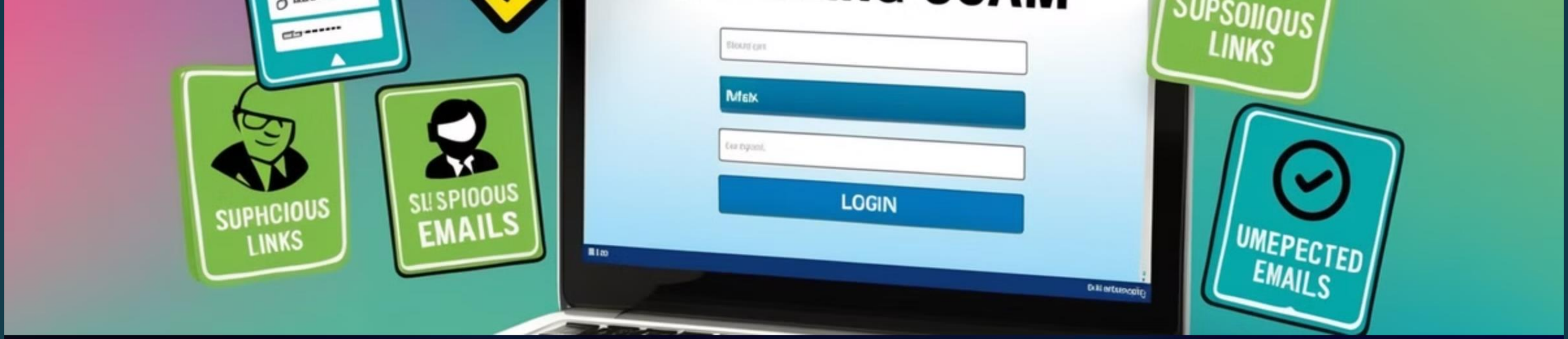
يتم تصميم أنظمة الحماية خصيصًا لمواجهة الهجمات التي تستهدف الأموال والأصول المالية الرقمية.

### حماية بيانات العملاء

تُولى أهمية قصوى لحماية البيانات الشخصية والمالية للعملاء، نظرًا لحساسيتها وقيمتها العالية.

### حماية المعاملات المالية

في قطاع التكنولوجيا المالية، ينصب التركيز الرئيسي على حماية المعاملات المالية وضمان سلامتها من أي تدخل خارجي.




# التصيد الاحتيالي: تهديد رئيسي

### ما هو التصيد الاحتيالي؟

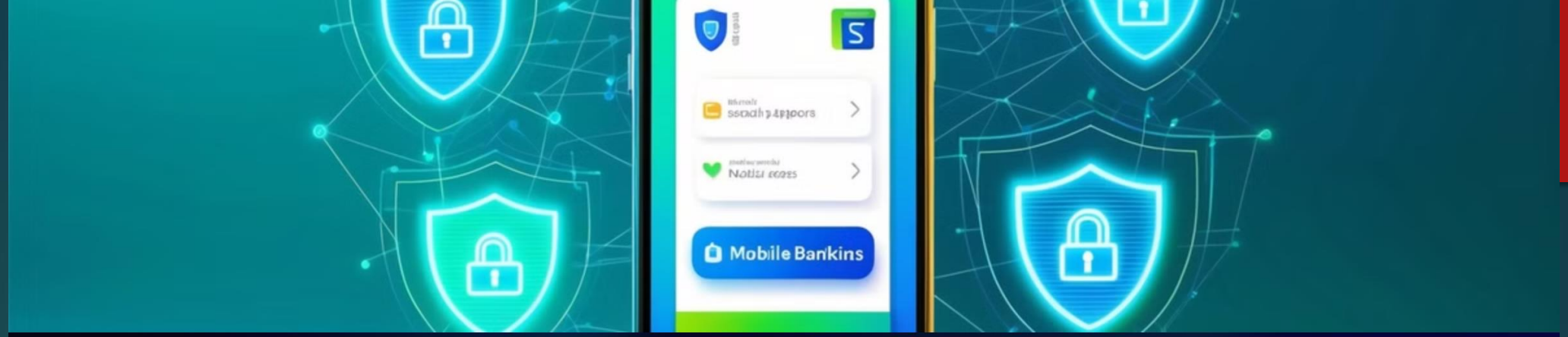
محاولة خداع المستخدمين للحصول على معلوماتهم الحساسة من خلال رسائل بريد إلكتروني مزيفة تبدو وكأنها مرسلة من جهات رسمية.

### كيف يحدث؟

عادة ما يتم إرسال رسائل تحمل شعارات بنوك أو مؤسسات مالية معروفة، تطلب من المستخدم تحديث بياناته عبر رابط مزيف.

### الحماية منه

التوعية المستمرة للمستخدمين وتطبيق تقنيات متقدمة لفلترة البريد الإلكتروني والتحقق من مصدر الرسائل.




# الهجمات على تطبيقات الهواتف الذكية

1

## استهداف التطبيقات المالية

تطبيقات الهواتف الذكية في مجال التكنولوجيا المالية هدف رئيسي للهجمات السيبرانية.

2

## استغلال الثغرات البرمجية

يسعى المهاجمون لاكتشاف واستغلال الثغرات في التطبيقات للوصول إلى بيانات المستخدمين المالية.

3

## تحديثات الأمان المستمرة

يجب على الشركات إصدار تحديثات أمان دورية لسد الثغرات وتعزيز حماية التطبيقات.

# برامج الفدية: تهديد متزايد

1

**الاختراق**

يخترق المهاجم النظام ويثبت برنامج الفدية.

2

**التشفير**

يقوم البرنامج بتشفير البيانات المهمة في النظام.

3

**المطالبة بالفدية**

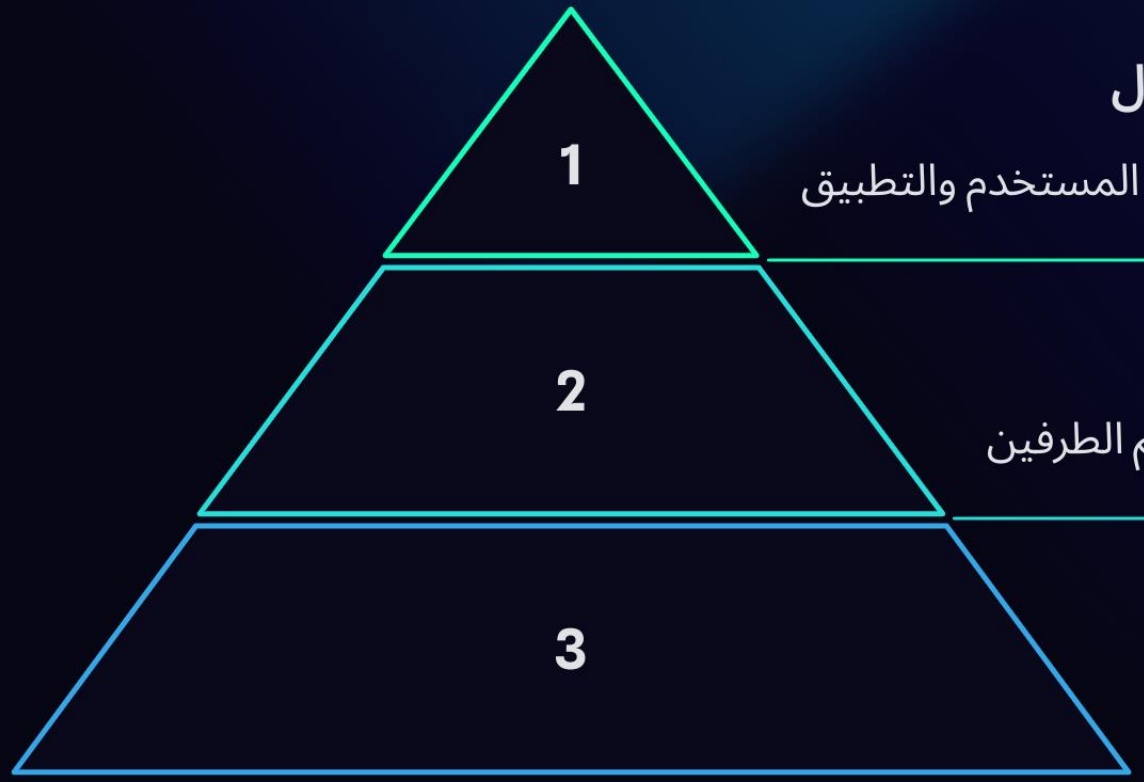
يطالب المهاجم بدفع فدية مقابل فك تشفير البيانات.

4

**العواقب**

خسائر مالية وتضرر السمعة في حالة عدم وجود نسخ احتياطية.

# هجمات Man-in-the-middle




**اعتراض الاتصال**

المهاجم يتنصت على الاتصال بين المستخدم والتطبيق.

**جمع البيانات**

يتم جمع البيانات المتبادلة دون علم الطرفين.

**استغلال المعلومات**

استخدام البيانات المسروقة لأغراض احتيالية.

لمنع هذه الهجمات، يجب استخدام بروتوكولات تشفير قوية وشبكات آمنة.

# أهمية حماية البيانات المالية الحساسة

### حماية الأصول

ضمان سلامة الأموال والأصول المالية للعملاء والمؤسسات.

### خصوصية العملاء

الحفاظ على سرية المعلومات الشخصية والمالية للمستخدمين.

### ثقة العملاء

بناء وتعزيز الثقة بين المؤسسات المالية وعملائها.

# تعزيز الثقة بين العملاء والمؤسسات المالية

1 **الشفافية في ممارسات الأمان**

إطلاع العملاء على إجراءات الأمان المتبعة لحماية بياناتهم.

2 **الاستجابة السريعة للحوادث**

وضع خطط فعالة للتعامل مع الحوادث الأمنية وإبلاغ العملاء بشكل فوري.

3 **التحديثات المستمرة**

تحديث أنظمة الأمان بشكل دوري وإعلام العملاء بالتحسينات.

# الالتزام بالقوانين والتشريعات الدولية والمحلية

| القانون | النطاق | العقوبات |
| --- | --- | --- |
| GDPR | الاتحاد الأوروبي | غرامات تصل إلى 20 مليون يورو |
| CCPA | كاليفورنيا، الولايات المتحدة | غرامات تصل إلى 7,500 دولار لكل انتهاك |

# التشفير: حجر الأساس في الأمن السيبراني

## ما هو التشفير؟

التشفير هو عملية تحويل البيانات إلى صيغة غير مفهومة إلا باستخدام مفتاح خاص. يعد أساسيًا في حماية المعلومات الحساسة أثناء نقلها أو تخزينها.

## أنواع التشفير

- التشفير المتماثل
- التشفير غير المتماثل
- التشفير الهجين

# المصادقة الثنائية (2FA)

1

### كلمة المرور

الخطوة الأولى: إدخال كلمة المرور المعتادة.

2

### رمز إضافي

الخطوة الثانية: إدخال رمز مؤقت يتم إرساله إلى الهاتف.

3

### تأكيد الهوية

الخطوة الثالثة: التحقق من صحة المعلومات والسماح بالدخول.

المصادقة الثنائية تضيف طبقة إضافية من الأمان، مما يجعل من الصعب على المهاجمين اختراق الحسابات حتى لو حصلوا على كلمة المرور.

# أنظمة الكشف عن الاختراقات (IDS)

### تحليل السلوك

تحليل أنماط الاستخدام وتحديد الانحرافات عن السلوك الطبيعي.

### المراقبة المستمرة

تقوم أنظمة IDS بمراقبة الشبكات والأنظمة بشكل مستمر بحثًا عن أي نشاط مشبوه.

### الإنذار الفوري

إرسال تنبيهات فورية للمسؤولين عند اكتشاف أي نشاط مشبوه.

Ap

# جدران الحماية (Firewalls)

1

### فحص حركة المرور

تقوم جدران الحماية بفحص جميع البيانات الداخلة والخارجة من الشبكة.

2

### تطبيق القواعد

يتم تطبيق مجموعة من القواعد المحددة مسبقًا لتحديد ما يُسمح به وما يُمنع.

3

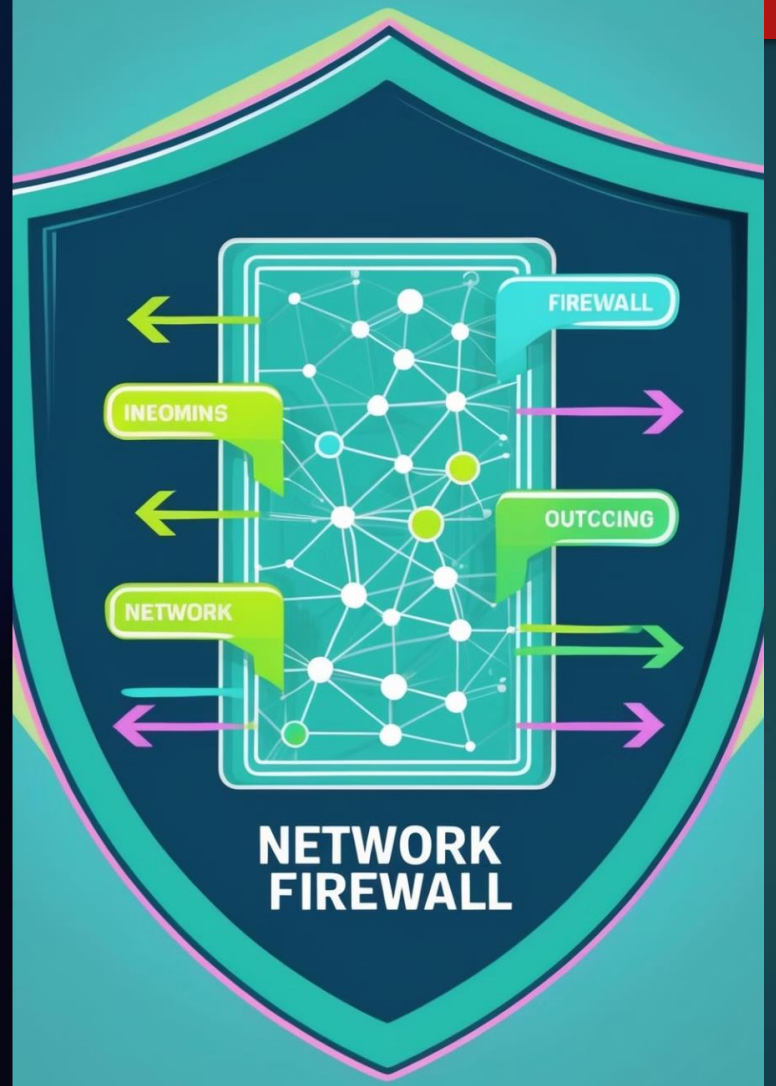
### منع الوصول غير المصرح

منع الوصول غير المصرح به إلى الشبكة من مصادر خارجية غير موثوقة.

4

### تسجيل النشاطات

تسجيل جميع محاولات الوصول للمراجعة والتحليل اللاحق.



# تحديات الأمن السيبراني في التكنولوجيا المالية

### تزايد نقاط الضعف

مع زيادة الأجهزة المتصلة والخدمات السحابية، تزداد نقاط الضعف المحتملة.

### التطور السريع للتهديدات

تتطور التهديدات السيبرانية بسرعة كبيرة، مما يتطلب تحديثًا مستمرًا لأنظمة الحماية.

### الموازنة بين الأمان وسهولة الاستخدام

تحقيق التوازن بين توفير أمان قوي وتجربة مستخدم سلسة.

Bus

# استراتيجيات الأمن السيبراني الفعالة

1. **التقييم المستمر للمخاطر**

   إجراء تقييمات دورية لتحديد نقاط الضعف الجديدة والمحتملة.

2. **التدريب والتوعية**

   تدريب الموظفين والعملاء على أفضل ممارسات الأمن السيبراني.

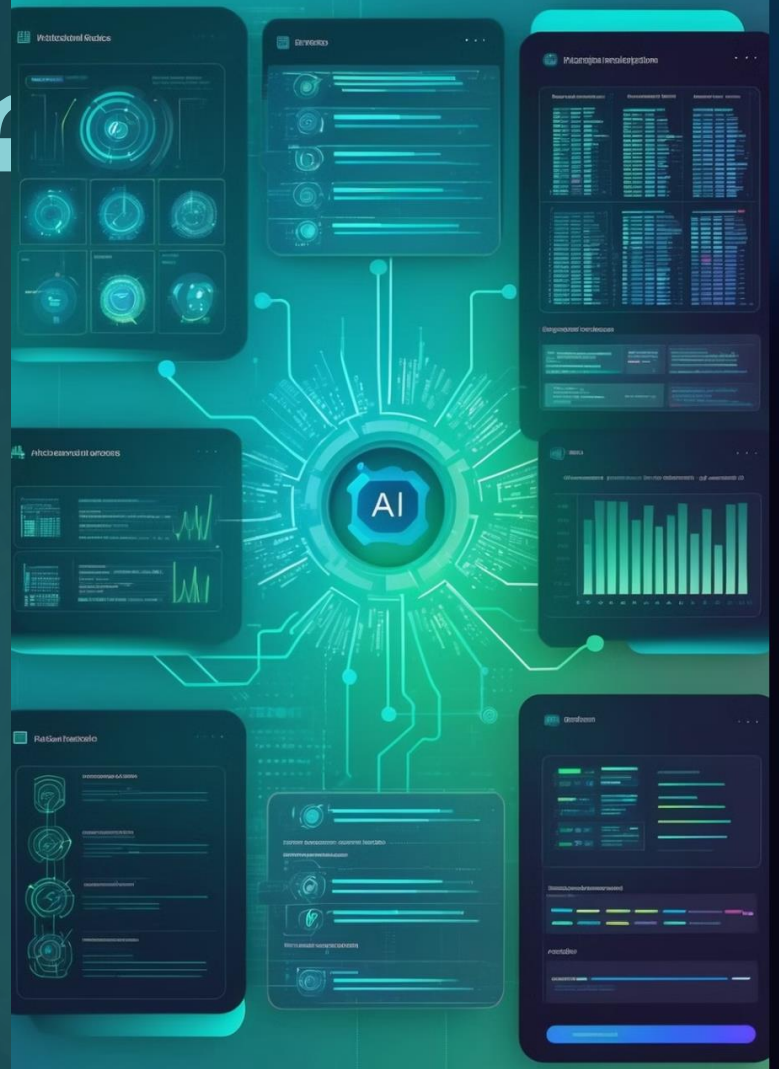
3. **التحديث المستمر**

   تحديث الأنظمة والبرامج بانتظام لسد الثغرات الأمنية.

4. **خطط الاستجابة للحوادث**

   وضع وتحديث خطط فعالة للاستجابة السريعة للحوادث الأمنية.

# دور الذكاء الاصطناعي في الأمن السيبراني




### تحليل السلوك

استخدام الذكاء الاصطناعي لتحليل أنماط السلوك وتحديد الانحرافات بدقة أكبر.

### الاستجابة التلقائية

تمكين الأنظمة من الاستجابة تلقائيًا للتهديدات المحتملة بسرعة أكبر.

### اكتشاف التهديدات الجديدة

استخدام تقنيات التعلم الآلي لاكتشاف أنواع جديدة من التهديدات السيبرانية.

# مستقبل الأمن السيبراني في التكنولوجيا المالية

### الأمن السيبراني كخدمة

توفير حلول أمنية متكاملة كخدمة للشركات الصغيرة والمتوسطة.

### الأمن الكمي

استكشاف تقنيات التشفير الكمي لمواجهة التهديدات المستقبلية.

### التكامل مع Blockchain

استخدام تقنية البلوكتشين لتعزيز أمان وشفافية المعاملات المالية.

# الخلاصة: أهمية الأمن السيبراني في التكنولوجيا المالية

### بناء الثقة

يعزز الأمن القوي ثقة العملاء في الخدمات المالية الرقمية.

### حماية الأصول والبيانات

الأمن السيبراني ضروري لحماية الأصول المالية والبيانات الشخصية في العصر الرقمي.

### دعم الابتكار

يمكّن الأمن القوي من تطوير وتقديم خدمات مالية مبتكرة بثقة.

### الامتثال للوائح

يضمن الالتزام بالقوانين والتشريعات المحلية والدولية.

# الخطوات القادمة: تعزيز الأمن السيبراني في مؤسستك

1

### تقييم المخاطر

إجراء تقييم شامل للمخاطر السيبرانية في مؤسستك.

2

### تطوير استراتيجية

وضع استراتيجية أمن سيبراني شاملة تتناسب مع احتياجات مؤسستك.

3

### التنفيذ والتدريب

تنفيذ الاستراتيجية وتدريب الموظفين على أفضل الممارسات الأمنية.

4

### المراجعة المستمرة

مراجعة وتحديث الاستراتيجية بشكل دوري لمواكبة التهديدات المتطورة.