الاختراقات الأمنية في المؤسسات المالية

التحديات الأخلاقية والحلول الوقائية

- المقدمة
- المفاهيم الأساسية
- التحديات الاخلاقية
- تأثير التحديات الأخلاقية على الفرد والمجتمع
- أمثلة لحالات اختراق
- تحليل الاختراقات الامنية
- الحلول الممكنة للاختراقات الأمنية
- القوانين و المعايير
- التوصيات والخاتمة

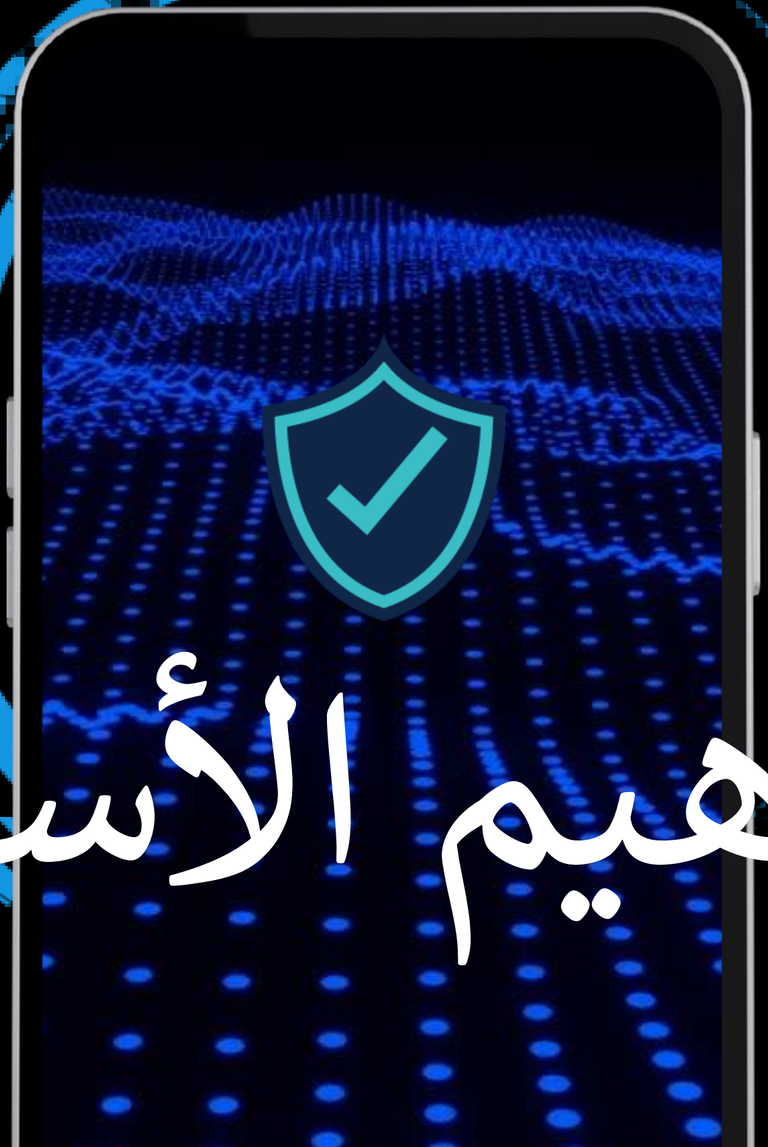
المقدمة

الاختراقات الأمنية هي هجمات سيبرانية تهدف للوصول غير المصرح به إلى الأنظمة والبيانات الحساسة في المؤسسات المالية. هذه الهجمات تتضمن سرقة المعلومات، تدمير البيانات، أو استخدامها بشكل غير قانوني، مما يهدد الأمان والخصوصية.

في عالم يعتمد بشكل متزايد على التكنولوجيا، يتحمل مهندسو البرمجيات مسؤولية كبيرة في تأمين الأنظمة وحماية البيانات الحساسة. الفشل في ذلك يمكن أن يؤدي إلى عواقب خطيرة، سواء من الناحية الأخلاقية أو القانونية، حيث أن ضمان حماية البيانات الشخصية ينعكس على الثقة العامة في الأنظمة التقنية.

الأهداف

- توضيح التحديات الأمنية والأخلاقية التي تواجه المؤسسات المالية.
- تحليل تأثير الاختراقات الأمنية على الأفراد والمجتمع.
- تقديم حلول وقائية لتعزيز الأمان السيبراني.
- استعراض القوانين والمعايير المنظمة لحماية البيانات.
- تقديم توصيات لتحسين الأمان وتقليل مخاطر الاختراقات.



المفاهيم الأساسية

الأمن السيبراني: حماية الأنظمة والشبكات من الهجمات الإلكترونية التي تستهدف سرقة البيانات أو إتلافها

التشفير: تقنية لتحويل البيانات إلى صيغة غير قابلة للقراءة إلا بواسطة الأطراف المصرح لها، مما يحمي البيانات من الاختراق

جدران الحماية (FIREWALLS): أدوات أمان تتحكم في حركة البيانات بين الشبكات الموثوقة وغير الموثوقة

المصادقة الثنائية (TWO-FACTOR AUTHENTICATION): إجراء أمني يضيف طبقة إضافية من الحماية بتأكيد هوية المستخدم عبر طريقتين مستقلتين

الهجمات الإلكترونية (CYBER ATTACKS): تشمل أنواعًا متعددة مثل التصيد الاحتيالي، البرمجيات الخبيثة، وهجمات الفدية التي تستهدف سرقة أو تعطيل البيانات

تزداد أهمية حماية المعلومات في المؤسسات المالية مع التوسع الكبير في استخدام التكنولوجيا، حيث تحتفظ هذه المؤسسات بكميات هائلة من البيانات الشخصية والمالية. هذا التطور يجعلها أكثر عرضة للتحديات الأمنية ويعزز الحاجة إلى إجراءات قوية للحماية من الاختراقات.

التحديات الأخلاقية

تتعدد التحديات الأخلاقية التي ترتبط بالاختراقات الأمنية في المؤسسات المالية، ويمكن أن تؤثر سلبًا على الأفراد والمجتمع ككل. من أبرز هذه التحديات:

1.الخصوصية وحماية البيانات

يعد انتهاك خصوصية العملاء من أخطر التحديات الأخلاقية. عند اختراق الأنظمة المالية، قد يتم سرقة المعلومات الشخصية الحساسة مثل الأرقام السرية، الحسابات المصرفية، وأرقام الهوية، مما يعرض الأفراد للخطر

2. المسؤولية في حالة الفشل

أحد التحديات الأخلاقية التي تواجهها المؤسسات هو تحمل المسؤولية عن الفشل في تأمين البيانات. هل تقع المسؤولية فقط على المتسللين، أم أن المؤسسة التي لم تتخذ التدابير اللازمة يجب أن تُحاسب أيضًا؟

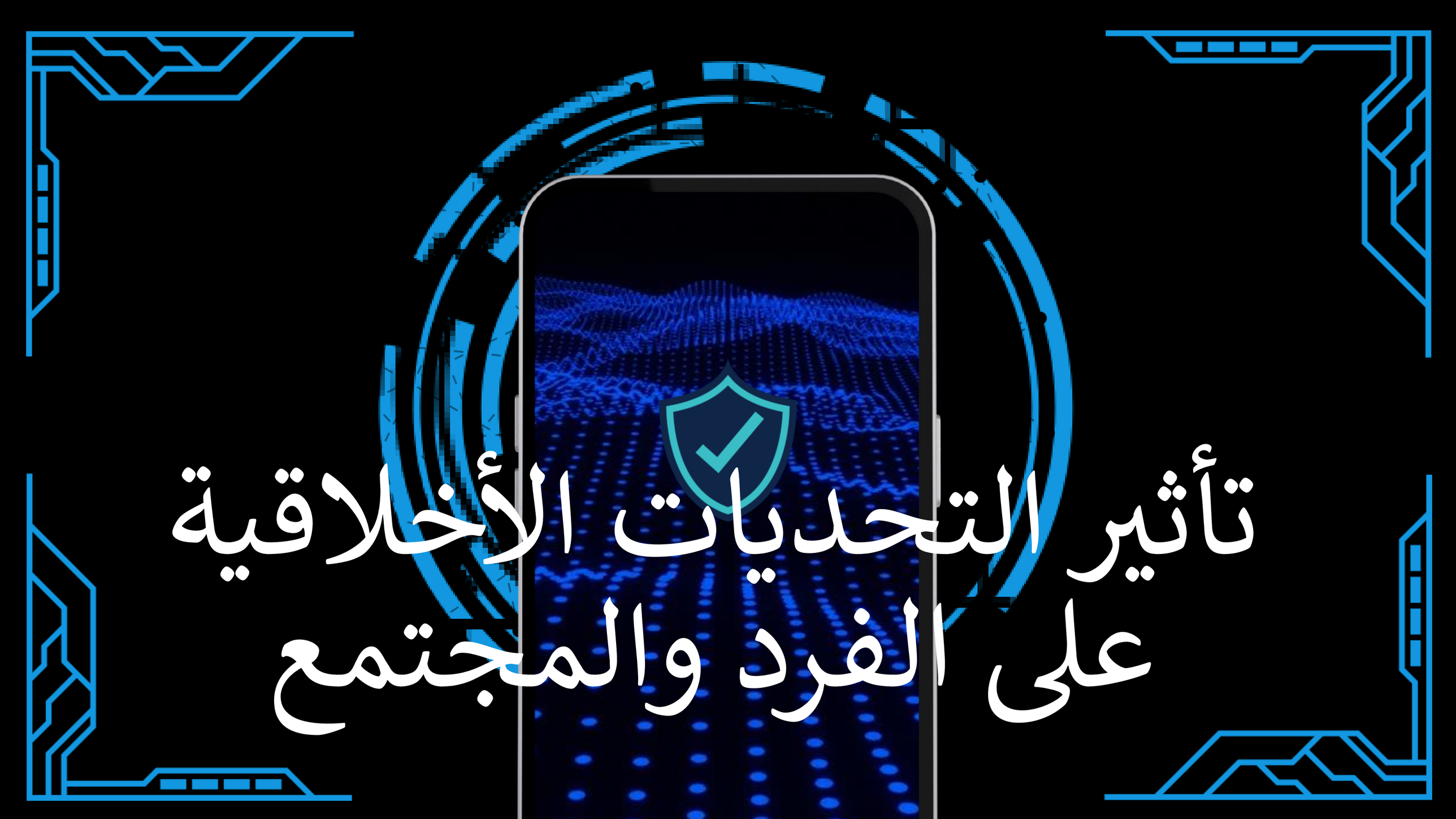
المسؤولية تقع على المؤسسة إذا قصرت في تأمين الأنظمة، حيث يجب عليها أخلاقيًا حماية بيانات العملاء

3. استخدام المعلومات المسروقة

في حال وقوع اختراق، من المحتمل أن تستخدم المعلومات المسروقة لتحقيق مكاسب غير قانونية. هذا يثير تساؤلات حول دور الشركات في حماية المعلومات حتى بعد تسريبها، وكيفية منع استخدام هذه البيانات بطريقة ضارة.

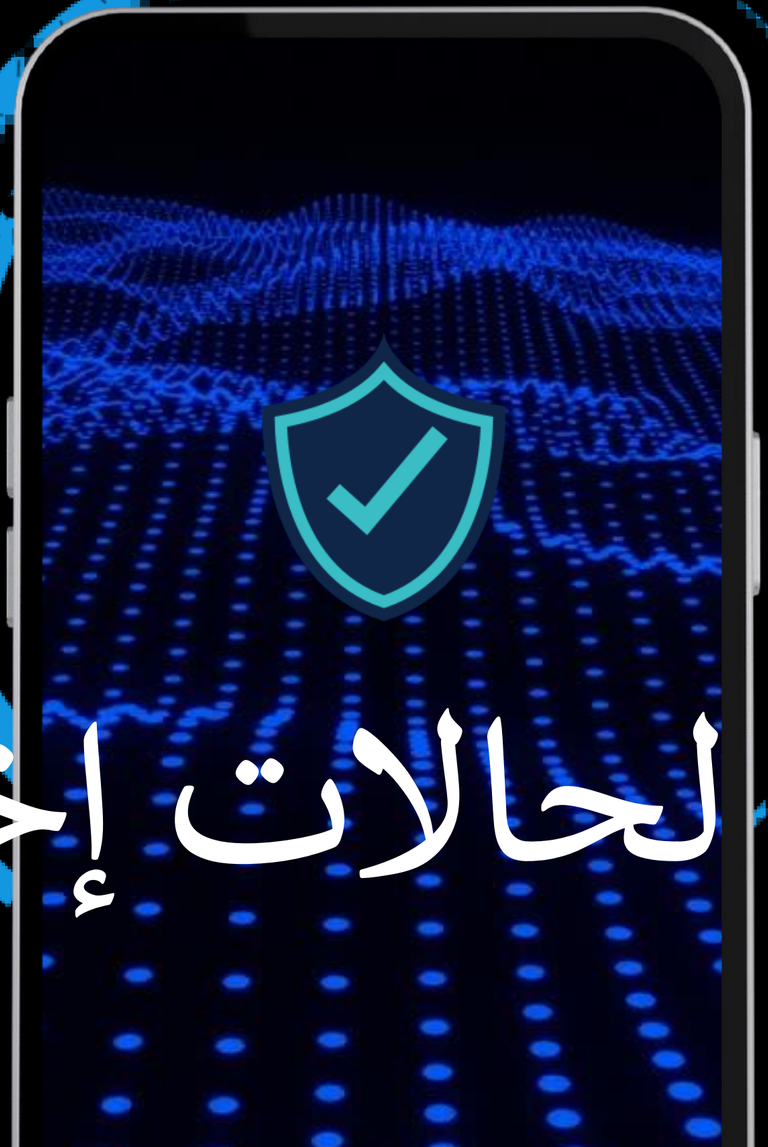
4. الثقة العامة

تؤدي مثل هذه الاختراقات إلى فقدان الثقة بين العملاء والمؤسسات المالية، مما يمكن أن يضر بالاقتصاد والمجتمع. إذا فقد العملاء الثقة في قدرتهم على الحفاظ على خصوصيتهم، قد يتجنبون استخدام الخدمات المالية الرقمية، مما يؤدي إلى تراجع الابتكار والنمو في القطاع



تأثير التحديات الأخلاقية على الفرد والمجتمع

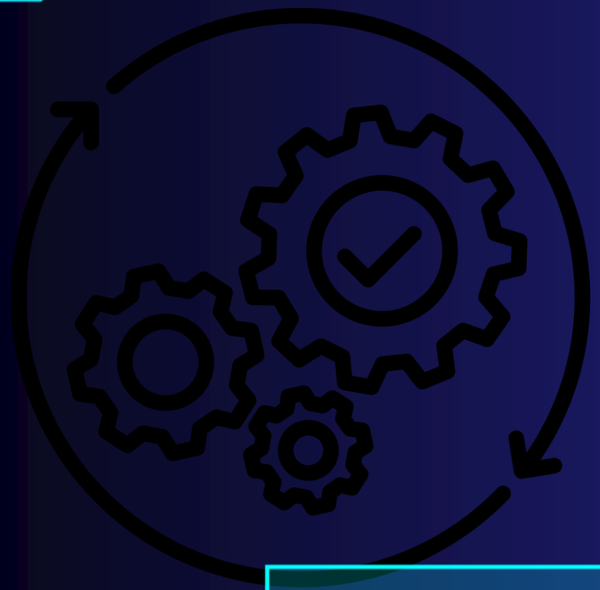
تؤثر التحديات الأخلاقية المرتبطة بالاختراقات الأمنية على الأفراد والمجتمع بشكل كبير. على مستوى الأفراد، تؤدي الاختراقات إلى فقدان الخصوصية وسرقة البيانات الشخصية، مما يزيد من مخاوف الأمان الشخصي والنفسي. أما على مستوى المجتمع، فهي تدفع لتطوير تشريعات وسياسات لحماية البيانات وتعزيز الأمان السيبراني، مما يعزز ثقة الجمهور في المؤسسات ويحمي البنية التحتية الحيوية



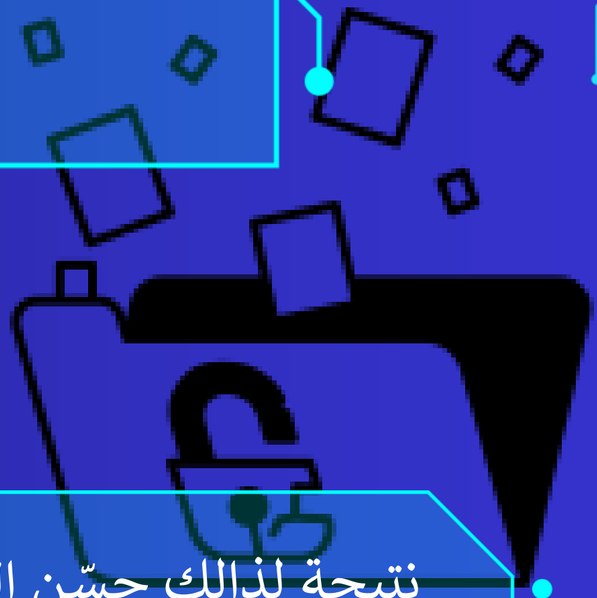
أمثلة لحالات إختراق

- بنك أوف أميركا (2023) :

تعرضت شركة خارجية متعاقدة مع البنك لخرق، مما أدى إلى تسريب بيانات حساسة كأرقام الحسابات والضمان الاجتماعي، وكشف عن مخاطر الاعتماد على الشركات الخارجية.



تم التعامل مع المشكلة عن طريق إجراء مراجعة للأمان مع الشركات المتعاقدة، وأخطر العملاء المتضررين، وقدم لهم خدمات مراقبة مجانية لحمايتهم



نتيجة لذالك حسّن البنك معايير الأمان مع الشركاء الخارجيين، مما ساعد في حماية العملاء وزيادة الثقة.

- بنك أبو ظبي (2023) :

في مايو 2023، تعرض البنك لهجوم DDoS من قبل مجموعة قراصنة ، حيث استهدفت البنك بزيادة الطلبات إلى 4.5 مليون طلب في الثانية. أدى الهجوم إلى إبطاء خدمات البنك بشكل كبير.

استجاب البنك من خلال استخدام جدران الحماية وتقنيات حماية متقدمة، مما ساعد في تقليل تأثير الهجوم. بفضل هذه الإجراءات، تمكن البنك من الحفاظ على استمرارية خدماته وتقليل الأضرار.

بشكل عام، أسهمت الاستجابة السريعة في حماية سمعة البنك وتعزيز ثقة العملاء

تحليل الاختراقات الأمنية

تحليل الاختراقات الأمنية في المؤسسات المالية لعام 2023

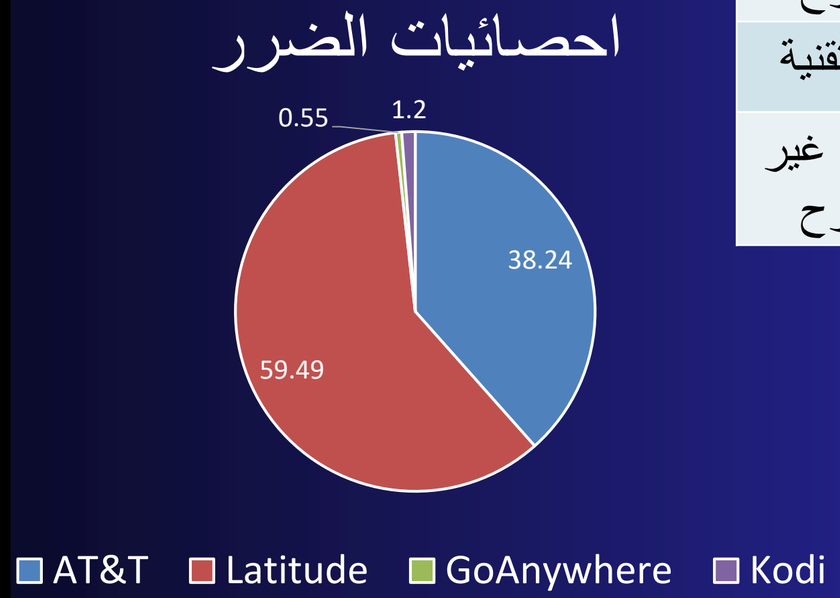
الأهداف

- معرفة أنواع الاختراقات الشائعة.
- دراسة العلاقة بين حجم المؤسسة وعدد الاختراقات.
- تقدير التأثير المالي لكل حادثة.

الأسئلة البحثية

- ما هي البيانات المستهدفة في الهجمات؟
- هل المؤسسات الكبيرة أكثر عرضة للاختراق؟
- كيف تؤثر الاختراقات على ثقة العملاء؟

المؤسسة	العام	السجلات المتأثرة	نوع البيانات المستهدفة	أسلوب الهجوم
AT&T	2023	9 مليون	بيانات شخصية	ثغرة تقنية
Latitude Financial	2023	14 مليون	أرقام رخص القيادة	وصول غير مصرح
GoAnywhere	2023	+130 منظمة	بيانات متنوعة	ثغرة تقنية
Kodi	2023	400 ألف	حسابات المستخدمين	وصول غير مصرح



التحليل الإحصائي

التحليل الوصفي :

- المتوسط: حوالي 6 ملايين سجل متأثر لكل حادثة.
- التوزيع البياني: البيانات الشخصية هي الأكثر استهدافًا.

اختبار الفرضيات :

- المؤسسات الكبيرة تتعرض للاختراقات بشكل أكبر بسبب كمية البيانات.

تقدير التداعيات المالية

- التكاليف المباشرة: مثل تكاليف استعادة الأنظمة.
- التكاليف غير المباشرة: خسائر الإيرادات وفقدان العملاء.
- التكاليف القانونية: الغرامات والتسويات.

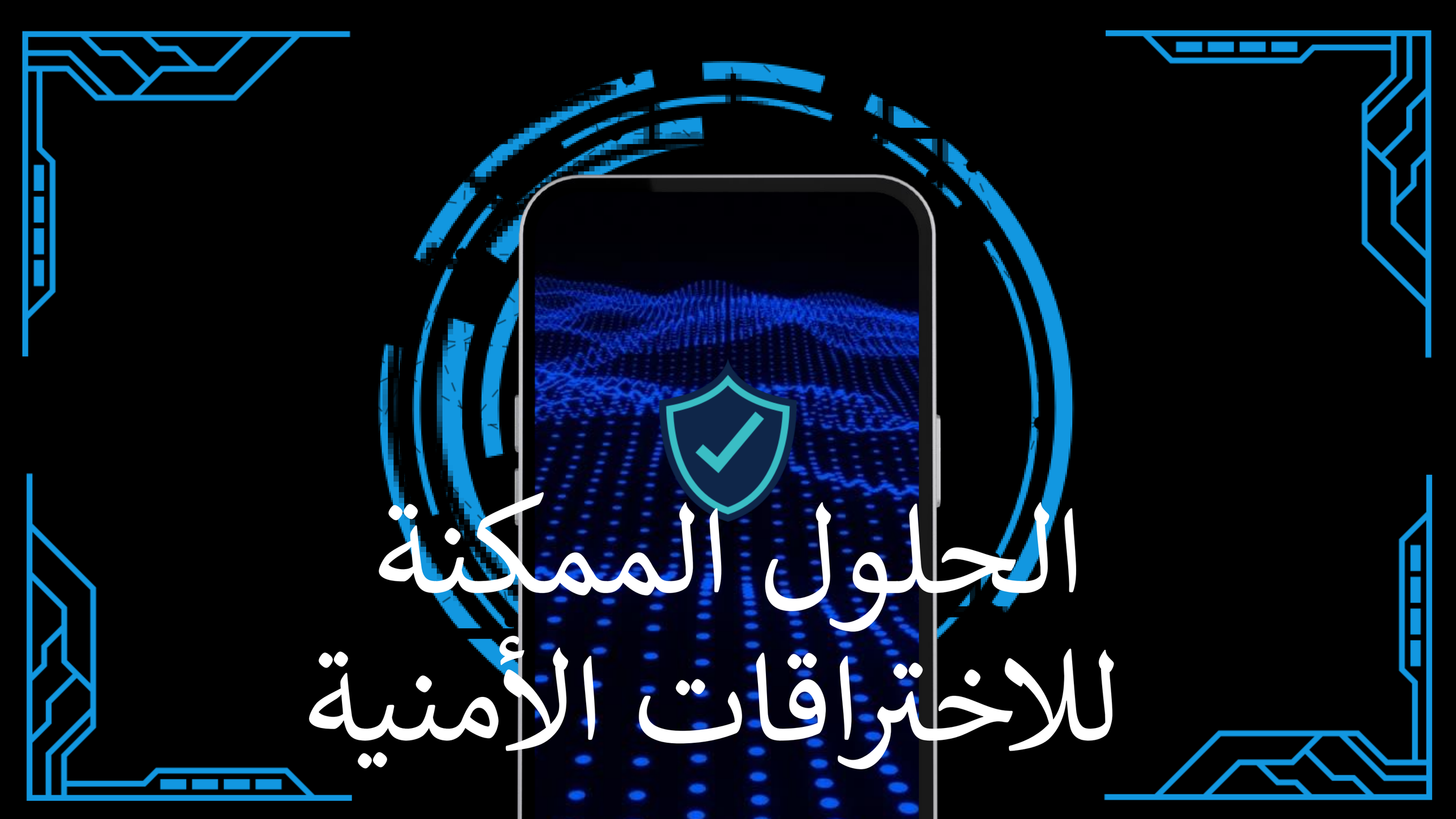
النتائج والتوصيات

النتائج:

- المؤسسات الكبيرة أكثر عرضة للاختراق.
- البيانات الشخصية هي الهدف الرئيسي.

التوصيات:

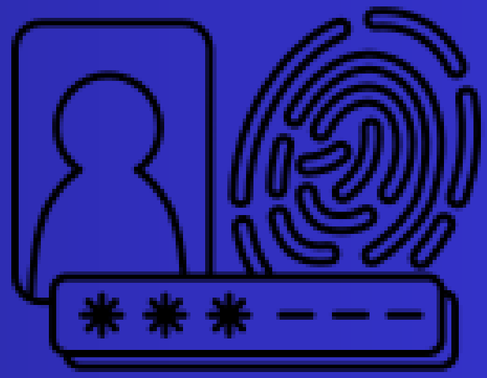
- تعزيز الأمان السيبراني باستخدام التشفير وأنظمة الكشف عن التسلل.
- زيادة الشفافية مع العملاء لرفع الثقة.
- تدريب الموظفين على الأمان السيبراني.


الحلول الممكنة
للاختراقات الأمنية

على الرغم من عدم وجود شخص او شركة او مؤسسة محصنه من اختراقات البيانات، إلا أن اتباع عادات جيدة لتأمين الاجهزة يمكن أن يقلل من خطر التعرض للاختراق ويساعدك في تقليل الأضرار. تهدف هذه النصائح إلى المساعدة في حماية الأجهزة الأخرى من القراصنة

1 . تطبيق تقنيات الحماية المتقدمة

يجب على المؤسسات المالية الاستثمار في تقنيات الأمان الحديثة مثل التشفير متعدد الطبقات، والتعرف على التهديدات في الوقت الحقيقي، وتقنيات الذكاء الاصطناعي التي يمكنها اكتشاف الأنماط غير الطبيعية ومنع الاختراقات



2 . التوعية والتدريب

يتعين على المؤسسات الاستثمار في تدريب موظفيها حول أهمية الحفاظ على أمن البيانات. يمكن أن يكون للخطأ البشري دور كبير في تسهيل عمليات الاختراق

3 . الشفافية والمسؤولية

يجب أن تكون المؤسسات المالية شفافة مع عملائها عند وقوع اختراقات، وأن تتحمل المسؤولية من خلال اتخاذ إجراءات إصلاحية سريعة، مثل تعويض المتضررين وتعزيز الإجراءات الأمنية

4 . تعزيز التعاون بين القطاعين الخاص والعام

يمكن أن يساعد التعاون بين الشركات المالية والحكومات في تطوير استراتيجيات وقائية أقوى ضد الهجمات الإلكترونية


القوانين و المعايير

للتصدي للاختراقات الأمنية، تم تطوير العديد من القوانين والمعايير المهنية التي تنظم السلوك في هذا المجال. من أبرز هذه القوانين:

- قانون حماية البيانات العامة (GDPR): هذا القانون الأوروبي يفرض على المؤسسات حماية بيانات الأفراد بصرامة، ويضع غرامات مالية كبيرة على منتهكيه

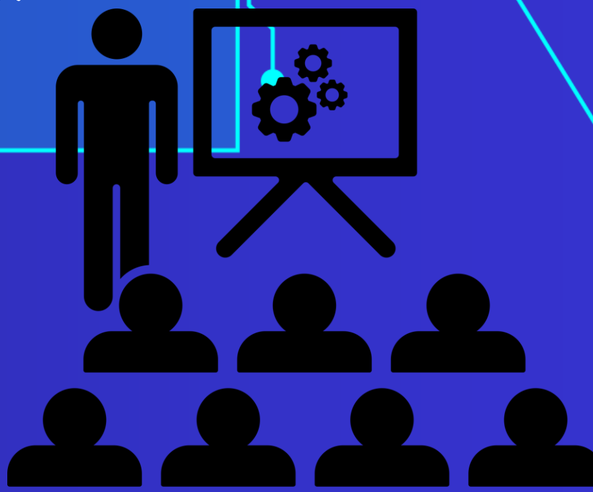
- قانون Gramm-Leach-Bliley (GLBA): يفرض على المؤسسات المالية في الولايات المتحدة اتخاذ إجراءات لحماية المعلومات الشخصية للعملاء.

- قانون PCI DSS : يوفر حماية لبيانات بطاقات الائتمان ويلزم المؤسسات المالية مثل البنوك وشركات الدفع بتشفير وتأمين بيانات الدفع لتقليل الاحتيال وسرقة المعلومات.

خطوات للالتزام بالمعايير الأمنية في المؤسسات المالية بشكل يومي :

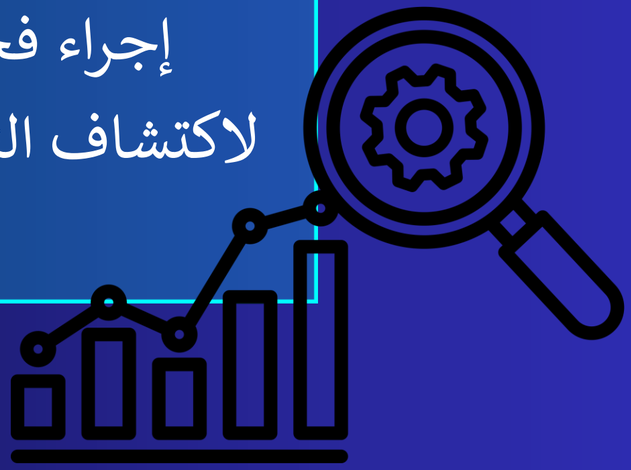
- تدريب الموظفين :

تقديم تدريبات دورية للموظفين حول أمان البيانات وكيفية حماية المعلومات الحساسة.



- مراقبة الأنظمة :

إجراء فحوصات دورية للأنظمة لاكتشاف الثغرات وتحديث الأمان عند الحاجة.

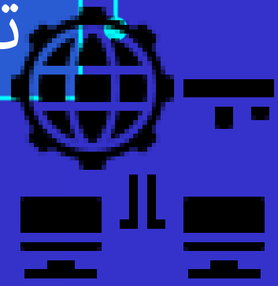


- تشفير البيانات

تشفير المعلومات الحساسة أثناء التخزين والنقل لحمايتها من الوصول غير المصرح به.

- إدارة الوصول

تحديد من يمكنه الوصول إلى المعلومات الحساسة وتطبيق أنظمة تسجيل الدخول متعددة العوامل.



- الإبلاغ عن الخروقات

تقديم تقارير فورية عن أي خروقات أمنية للحفاظ على الشفافية مع العملاء.

التوصيات والخاتمة

يُنصح مهندسو البرمجيات بما يلي:

1. الالتزام بأعلى معايير الأخلاقيات

يجب على المهندسين فهم المسؤوليات الأخلاقية المتعلقة بتطوير الأنظمة المالية، والحرص على تصميم حلول تحافظ على خصوصية وأمان المستخدمين

2. التطوير المستمر

يجب على المهندسين متابعة التهديدات الجديدة باستمرار وتحديث تقنيات الحماية

3. التواصل والشفافية

من الضروري أن يكون المهندسون على تواصل دائم مع العملاء والمؤسسات بشأن التهديدات المحتملة، وتوضيح الخطوات المتخذة لحمايتهم.

الخاتمة

يمثل الحفاظ على أمن المعلومات في المؤسسات المالية تحديًا كبيرًا يتطلب الالتزام الصارم بالأخلاقيات، والتعاون بين الأطراف المختلفة لتقليل المخاطر

المصادر :

- مجلة KASPERSKY، العنوان: ماهو الاختراق الامني
HTTPS://ME.KASPERSKY.COM/RESOURCE-CENTER/THREATS/WHAT-IS-A-SECURITY-BREACH

- العنوان: التحديات الاخلاقية في تكنولوجيا المعلومات
HTTPS://ILTIZAMERP.COM/AR/BLOG/TUTORIALS/%D8%A7%D9%84%D8%AA%D8%AD%D8%AF%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%A3%D8%AE%D9%84%D8%A7%D9%82%D9%8A%D8%A9-%D9%81%D9%8A-%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D9%85%D8%B3%D8%A7%D8%A6%D9%84-%D8%AD%D9%88%D9%84-%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D8%A3%D9%85%D8%A7%D9%86

- “CYBERSECURITY IN FINANCIAL SERVICES” - MCKINSEY & COMPANY, 2022. رابط المصدر (HTTPS://WWW.MCKINSEY.COM/BUSINESS-FUNCTIONS/RISK-AND-RESILIENCE/OUR-INSIGHTS/CYBERSECURITY-IN-FINANCIAL-SERVICES)

- MICROSOFT SECURITY INTELLIGENCE REPORT, “PHISHING AND MALWARE TRENDS” - MICROSOFT, 2023. رابط المصدر (HTTPS://WWW.MICROSOFT.COM/EN-US/SECURITY/BUSINESS/SECURITY-INTELLIGENCE-REPORT)

تقرير ZDNET وتقرير THE VERGE. ، تقرير CNBC وتقرير FORBES.

وموقع PCI SECURITY STANDARDS.

الموقع الرسمي لـ GDPR.

- CYBERSRC. (HTTPS://CYBERSRCC.COM/RECORD-BREAKING-DDOS-ATTACK-ON-UAE-FINANCIAL-INSTITUTION-BY-BLACKMETA)


THANK
YOU