

MKT324

التسويق عبر الهاتف المحمول

**إعداد
د. كريم أحمد**

التسويق عبر الهاتف المحمول

المحاضرة التاسعة

MKT324

التسويق عبر الهاتف المحمول

إعداد
د. كريم أحمد

عنوان المحاضرة
خصوصية العملاء
في بيئة الهاتف المحمول

أهداف المحاضرة

تهدف هذه المحاضرة إلى تحقيق ما يلي:

١. توضيح أهمية الهوية والبيانات في التسويق عبر الهاتف المحمول ودورها في تخصيص التجارب وتحقيق التفاعل الفعال مع العملاء.
٢. شرح أنواع الهوية الرقمية وتصنيفات البيانات الخاصة لفهم كيفية استخدامها في الاستراتيجيات التسويقية.
٣. تحليل النهجين الرئيسيين لإدارة الهوية والبيانات (المؤسسي والمتمحور حول الأفراد) وأثرهما على الخصوصية.
٤. تعريف الخصوصية وحقوق الأفراد في البيئة الرقمية مع التركيز على القوانين والمبادئ التنظيمية مثل GDPR.
٥. استعراض الأساليب التقليدية والحديثة لإدارة الهوية والخصوصية في التسويق عبر الأجهزة المحمولة.
٦. تسليط الضوء على المخاطر والأضرار الناتجة عن إساءة استخدام البيانات الشخصية من خلال أمثلة واقعية ودراسة حالة.
٧. تأكيد أهمية الامتثال القانوني وبناء الثقة مع المستهلكين كعنصر استراتيجي في التسويق الرقمي.

موضوعات المحاضرة

تتناول المحاضرة الموضوعات التالية:

• مقدمة

• الهوية وأنواعها في البيئة الرقمية

• النهج المؤسسي والنهج المتمحور حول الأفراد في إدارة الهوية والبيانات

• الخصوصية وحقوق الأفراد

• احترام الخصوصية والامتثال القانوني

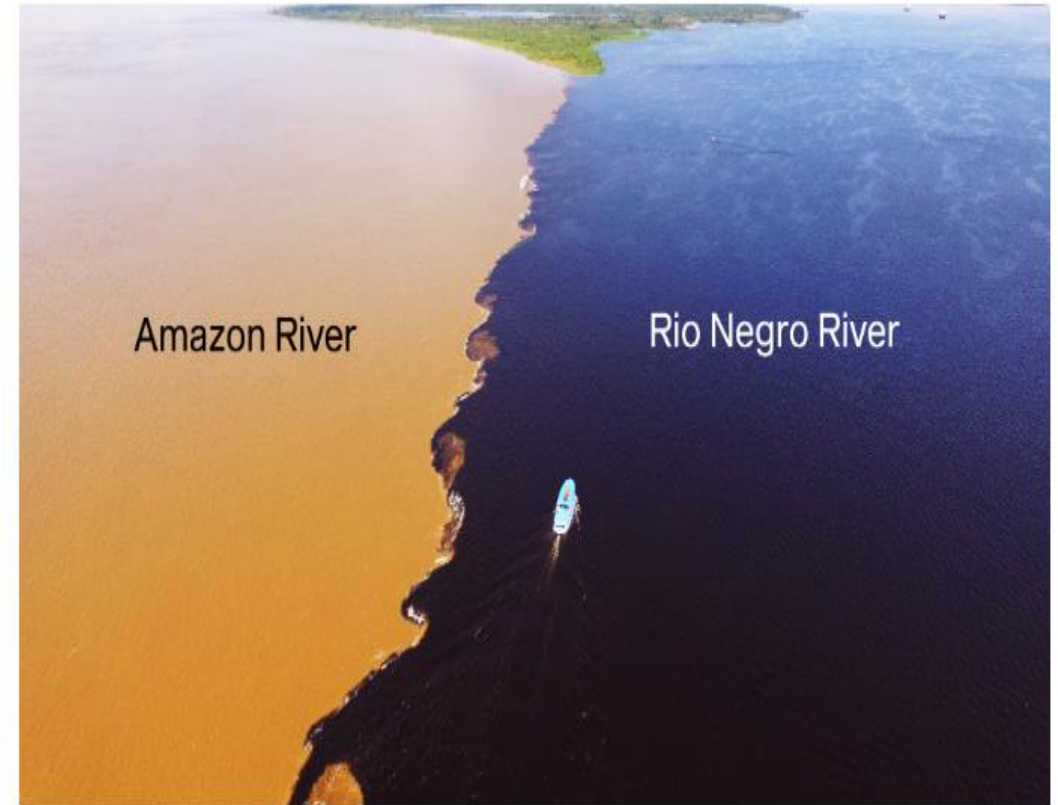
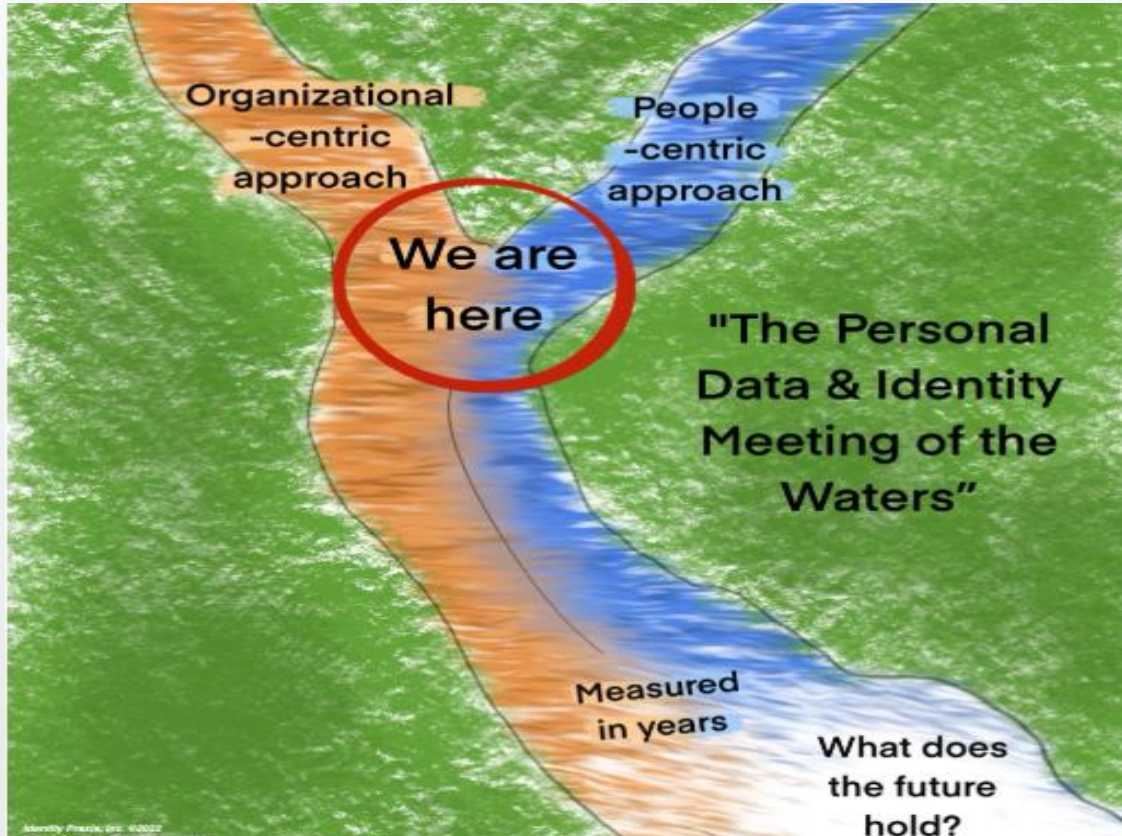
• الأضرار الناتجة عن إساءة استخدام البيانات الشخصية والهوية

• الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

• الأساليب الحديثة لإدارة الهواتف المحمولة والخصوصية

مقدمة

تظهر ظاهرة "التقاء المياه" في نهر الأمازون بالبرازيل، حيث يلتقي نهر ريو نيغرو ذو المياه الداكنة مع نهر الأمازون ذي اللون الرملي الفاتح دون اندماج بسبب اختلاف خصائصهما الفيزيائية مثل السرعة ودرجة الحرارة وكثافة الرواسب، نموذجًا تشبيهيًا لما يحدث في المجتمع المعاصر. في مجال التسويق عبر الهاتف المحمول، يشهد العالم تقاطعًا مشابهًا يتمثل في "التقاء الهوية والبيانات"، حيث يلتقي النهج التقليدي الذي يركز على المؤسسات مع النهج الحديث الذي يركز على الأفراد في إدارة الهوية والبيانات. هذا التلاقي يعكس تحولًا جوهريًا في كيفية التعامل مع الخصوصية وإدارة المعلومات، إذ يسعى إلى تحقيق توازن بين متطلبات التنظيم المؤسسي واحتياجات الأفراد، بما يضمن احترام الحقوق الشخصية ويعزز التفاعل المتمحور حول العميل في رحلته التسويقية.



مقدمة

يُعد فهم الهوية والبيانات الشخصية أساسًا جوهريًا في إدارة الهوية والبيانات ضمن ممارسات التسويق الحديث. فمعرفة الجمهور المستهدف، بما في ذلك مشاعره واحتياجاته ورغباته ونواياه، تمثل عنصرًا حاسمًا لنجاح الاستراتيجيات التسويقية، إذ تتيح للمسوقين التفاعل مع العملاء عبر جميع مراحل رحلتهم، وتقديم المحتوى والمنتجات والخدمات المناسبة في الوقت والمكان الملائم، مما يعزز تحقيق التوافق بين المنتج والسوق. ويكتسب التعامل مع الهوية والبيانات، ولا سيما البيانات الشخصية أو الخاصة، أهمية متزايدة في العصر الرقمي، حيث تُستخدم هذه المعلومات لتخصيص التجارب وإنشاء مجموعات تسويق مستهدفة وخدمة العملاء بكفاءة.

This sucks: dev finds backdoor in his robot vacuum, potentially giving full control to spies

Published: 30 October 2025 · Last updated: 31 October 2025



Ernestas Naprys, Senior Journalist



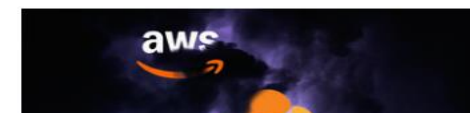
Partner content



SECON & eGISEC 2026: Asia's Leading Integrated Security Exhibition

by Hailey Kim · 19 November 2025

Editor's choice



[Developer discovers his vacuum has a secret backdoor | Cybernews](#)



<https://www.youtube.com/watch?v=FbRUQRmvC4U>

الهوية وأنواعها في البيئة الرقمية

تشير الهوية إلى مجموعة الخصائص ونقاط البيانات التي تحدد فردًا أو كيانًا في النظام البيئي الرقمي، مثل الاسم، العنوان، الموقع، والسلوكيات، حيث يمكن أن تصل هذه الخصائص إلى عشرات الآلاف من البيانات المحتملة. وتنقسم الهوية إلى عدة أنواع رئيسية، لكل منها دور محدد في إدارة البيانات والتسويق الرقمي:

١- الهوية الشخصية Personal Identity

هي المعلومات التي يمكن استخدامها لتحديد هوية فرد أو شيء بشكل فريد، مثل رقم الهوية الوطنية أو عنوان البريد الإلكتروني (للأشخاص) أو أكواد أجهزة إنترنت الأشياء (للأشياء).

الهوية وأنواعها في البيئة الرقمية

٢- الهوية الرقمية Digital Identity

تمثل التواجد عبر الإنترنت للفرد أو الكيان، بما في ذلك التفاعلات عبر المنصات، السلوكيات، والسمات. تُنشأ باستخدام تقنيات مثل ملفات تعريف الارتباط، ومعرّفات الأجهزة، وسجلات الشراء.

مثال: ملف تعريف المستخدم على فيسبوك الذي يحتوي على بياناته وسلوكياته وتفضيلاته.

٣- الهوية الاحتمالية Probabilistic Identity

تعتمد على النمذجة الإحصائية لاستنتاج من قد يكون مرتبطاً بملف رقمي، من خلال مراقبة السلوكيات وربطها ببيانات مثل الموقع والوقت.

مثال: نظام إعلانات يتوقع أن المستخدم الذي يزور مواقع السفر في الليل هو شخص يخطط لرحلة، حتى لو لم يقدم بياناته الشخصية.

الهوية وأنواعها في البيئة الرقمية

٤- الهوية الحتمية Deterministic Identity

تستخدم معرفات فريدة مثل مسح المستندات أو بيانات تسجيل الدخول للتحقق بدقة من هوية الشخص أو الشيء.
مثال: التحقق من هوية المستخدم عبر بصمة الوجه عند تسجيل الدخول إلى تطبيق مصرفي.

٥- هوية الوكيل (Agent Identity)

هي الهوية الرقمية المرتبطة بوكيل مفوض، مثل روبوت دردشة تابع لشركة أو مساعد شخصي يعمل بالذكاء الاصطناعي، مع إمكانية التحقق من صلاحياته بشكل تشفيري.
مثال: روبوت دردشة في موقع خدمة عملاء لديه صلاحية الوصول إلى بيانات الحساب لتنفيذ طلبات العميل.

الهوية وأنواعها في البيئة الرقمية

٦- البيانات الخاصة (Private Data)

هي البيانات التي يتم إنتاجها بواسطة الفرد عن نفسه أو يتم إنتاجها بواسطة الأشياء الخاصة بالفرد وعنها، مثل أجهزة إنترنت الأشياء الخاصة بالفرد.

تُصنّف البيانات الخاصة إلى خمسة مجالات رئيسية، تُجمع من مصادر متعددة، وتشمل بيانات شخصية وغير شخصية، إضافة إلى خصائص مميزة لكل نوع.

يجب أن يكون المسوق على علم بنوعية البيانات التي يتعامل معها، وذلك من الناحية التقنية والناحية القانونية.

الهوية وأنواعها في البيئة الرقمية

٦- البيانات الخاصة (Private Data)

أولاً، البيانات غير الشخصية هي بيانات مجهولة المصدر تُنتج من تفاعل الفرد مع الأجهزة أو الخدمات، مثل بيانات الكاميرا المجهولة أو بيانات التشخيص من الأجهزة الذكية، وغالبًا ما تكون محل جدل قانوني بشأن ملكيتها.

ثانيًا، البيانات الشخصية تشير إلى المعلومات التي يتم إنتاجها عن الفرد أو أشيائه، سواء من خلاله مباشرة أو بواسطة أطراف أخرى، وتُعرف غالبًا باسم المعلومات الشخصية القابلة للتحديد personally identifiable information (PII)، مع اختلاف تعريفها بين الأنظمة القانونية.

ثالثًا، المعلومات وهي بيانات محمية قانونيًا تُستخدم لتحديد هوية الأفراد أو أشيائهم بشكل احتمالي أو حتمي.

الهوية وأنواعها في البيئة الرقمية

٦- البيانات الخاصة (Private Data)

رابعًا، **البيانات الموثوقة** وهي بيانات شخصية تم التحقق منها تشفيرًا بواسطة جهة موثوقة مثل الحكومة أو المؤسسات التعليمية أو الصحية، مما يتيح إمكانية تتبع مصدرها.

خامسًا، **البيانات الحساسة** التي تشمل فئات محمية قانونيًا مثل الجنس والمنطقة الجغرافية.

هذه التصنيفات تمثل أساسًا لفهم إدارة الهوية والخصوصية في البيئة الرقمية، وتبرز أهمية الامتثال للمعايير القانونية والأخلاقية عند التعامل مع البيانات.

النهج المؤسسي والنهج المتمحور حول الأفراد في إدارة الهوية والبيانات

يعتمد النهج التقليدي في الاقتصاد الصناعي والمعلوماتي لإدارة البيانات الشخصية والهوية، المعروف باسم "النهج المؤسسي"، على سيطرة المؤسسات (سواء كانت شركات خاصة أو عامة، منظمات غير ربحية وغير حكومية) والهيئات العامة (المكاتب الحكومية، الجامعات، الكليات، المدارس، والمجموعات الدينية) بشكل كامل على البيانات الشخصية والهوية، وتحديد شروط استخدامها ومتى يتم ذلك. تقوم هذه المؤسسات باستخراج وجمع البيانات الشخصية والهويات من المصادر العامة والخاصة، ثم تحليلها وإدارتها وبيعها، لتحقيق النصيب الأكبر من القيمة التجارية الناتجة عن تلك البيانات والهويات.

النهج المؤسسي والنهج المتمحور حول الأفراد في إدارة الهوية والبيانات

ظل هذا النهج مهيمنًا طوال حقبتَي الاقتصاد الصناعي والمعلوماتي لأكثر من مئة عام، ولا يزال قائمًا حتى الآن، كما يتضح من دراسة منتدى النظام البيئي للهاتف المحمول (MEF) Mobile Ecosystem Forum بعنوان البيانات الشخصية، الهوية الرقمية، التحقق والمصادقة في المؤسسات لعام ٢٠٢١: التحليل والفرص. أظهرت الدراسة أن معظم المؤسسات التي شملها الاستطلاع في تسعة أسواق ترى نفسها مالكة للبيانات الشخصية والهوية، والمعروفة أيضًا باسم "بيانات العملاء". ومن المهم الإشارة إلى أن هذه النتائج تعكس ما يشعر به التنفيذيون في الشركات، وليس بالضرورة ما يفرضه القانون. وكما سنرى في بقية هذا الفصل، فإن هذا التصور لملكية البيانات والسيطرة عليها يواجه تحديات كبيرة على عدة جبهات.

النهج المؤسسي والنهج المتمحور حول الأفراد في إدارة الهوية والبيانات

يعكس النهج المتمحور حول الأفراد في إدارة الهوية والبيانات تحولاً جوهرياً في اقتصاد البيانات، حيث يقوم على منح الأفراد، بصفاتهم أصحاب البيانات، حق الملكية والسيطرة على بياناتهم الشخصية وهوياتهم الرقمية. ينبع هذا التوجه من إدراك متزايد لقيمة البيانات التي يمكن للأفراد تحقيقها من خلال جمعها وإدارتها بأنفسهم، بما يتيح لهم حرية تحديد كيفية استخدامها ومشاركتها. ويرتكز هذا النهج على ثلاثة مفاهيم أساسية: الوكالة التي تعني قدرة الفرد على التصرف بشكل مستقل واتخاذ القرارات بحرية، والاستقلالية التي تشير إلى القدرة على إدارة الذات، والسيادة التي تمنح الفرد السلطة العليا على بياناته وهويته. ويهدف هذا النموذج إلى تعزيز التحكم الفردي في عمليات جمع البيانات وإدارتها ومشاركتها، بما يحد من الاعتماد على الأنظمة المؤسسية التقليدية التي تركز على احتكار البيانات.

النهج المؤسسي والنهج المتمحور حول الأفراد في إدارة الهوية والبيانات

يتميز النهج المتمحور حول الأفراد في إدارة الهوية والبيانات بتمكين الأشخاص، أصحاب البيانات، من التحكم في بياناتهم وهوياتهم الرقمية، وإتاحة إمكانية تبادلها وفقاً لشروطهم الخاصة بدلاً من شروط مؤسسات معينة. لا يعني ذلك أن المؤسسات لن تحتفظ ببيانات الأفراد أو أن البيانات المخصصة للمساحات العامة لن تكون متاحة، بل يشير إلى أن الأفراد سيصبحون أكثر وعياً وقادرين على التغيير السلوكي، والحصول على خدمات مهنية وتأمين للبيانات، وممارسة حقوقهم المتعلقة بالبيانات. كما سيعتمدون على تقنيات معينة للتحكم في بياناتهم وحماية أنفسهم، بما يتيح لهم المشاركة الفاعلة في صناعة القرارات بدلاً من أن يكونوا مجرد أطراف خاضعة للشركات والمنظمات.

الخصوصية وحقوق الأفراد

تُعد الخصوصية مفهومًا أساسيًا في التسويق عبر الهاتف المحمول، حيث ترتبط ارتباطًا وثيقًا بالهوية والبيانات وحقوق الأفراد، إضافة إلى الآثار الاجتماعية والتجارية والقانونية المترتبة على التعامل السليم أو الخاطئ مع هذه الجوانب. غالبًا ما يُنظر إلى الخصوصية باعتبارها حالة أو وضعًا يتيح التحرر من المراقبة أو الإزعاج من الآخرين، إلا أن هذا التعريف التقليدي لا يعكس الواقع المعاصر الذي يجمع بين البيئة الرقمية والمادية. في السياق الحديث، ينبغي النظر إلى الخصوصية باعتبارها فعلًا يتمثل في قدرة الفرد على تحديد من يمكنه الوصول إليه، ومتى وأين ولأي غرض ولمدة زمنية محددة، سواء كان الوصول ماديًا أو رقميًا عبر الأجهزة المتصلة بالإنترنت الأشياء. وبذلك تصبح الخصوصية مجموعة من الخيارات والسلوكيات السياقية وليست مجرد حالة ثابتة.

الخصوصية وحقوق الأفراد

في عام ١٩٧٤، وضعت الولايات المتحدة مبادئ الممارسات العادلة للمعلومات **FIPPs**، وهي مبادئ أساسية تهدف إلى توجيه كيفية التعامل مع الخصوصية في الصناعة وفي إطار القوانين واللوائح. وكانت المبادئ الرئيسية لـ FIPPs كما يلي:

الشفافية (أو الوعي): يجب إبلاغ الأفراد عند جمع بياناتهم وكيفية استخدامها.

الموافقة (أو الاختيار): يجب أن يستند استخدام البيانات الشخصية خارج الغرض الأصلي إلى موافقة مستنيرة من الفرد.



الوصول والمشاركة (أو التحكم): يحق للأفراد الوصول إلى بياناتهم وتصحيح الأخطاء فيها.

الأمان: يجب على المؤسسات ضمان سلامة البيانات وحمايتها من الاستخدام غير المصرح به.

المساءلة: يجب أن تكون هناك آليات لتطبيق هذه الضمانات ومعالجة أي انتهاكات.

الخصوصية وحقوق الأفراد

اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، تركز على:

١. حق الوصول: يمكن للأفراد طلب الوصول إلى بياناتهم الشخصية والحصول على معلومات حول كيفية معالجتها.

٢. حق التصحيح: يمكن للمستخدمين تصحيح الأخطاء في بياناتهم الشخصية.

٣. حق المسح ("الحق في النسيان"): يمكن للأفراد طلب حذف بياناتهم الشخصية في ظروف معينة.

٤. حق تقييد المعالجة: يمكن للأفراد الحد من كيفية معالجة بياناتهم في حالات محددة.

٥. حق قابلية نقل البيانات: يمكن للمستخدمين طلب توفير بياناتهم في صيغة قابلة للقراءة آلياً لنقلها إلى خدمة أخرى.

٦. حق الاعتراض: يمكن للأفراد الاعتراض على معالجة البيانات لأغراض معينة، مثل التسويق المباشر.

٧. الحقوق المتعلقة باتخاذ القرار الآلي: الحماية من القرارات التي تُتخذ بناءً على المعالجة الآلية فقط والتي تؤثر بشكل كبير على الأفراد.



احترام الخصوصية والامتثال القانوني

في سياق التسويق عبر الأجهزة المحمولة، يتخذ الأفراد قرارات مستمرة تتعلق بخصوصيتهم عند التفاعل مع العلامات التجارية والمسوقين. وتشمل هذه القرارات المشاركة في الإعلانات عبر الهاتف المحمول، والاشتراك أو إلغاء الاشتراك في البرامج التسويقية مثل الرسائل النصية القصيرة SMS، والبريد الإلكتروني، وإشعارات الدفع. كما يقرر الأفراد ما إذا كانوا يرغبون في تتبع نشاطهم داخل التطبيقات والمتصفحات، وإنشاء حسابات، والموافقة على سياسات الخصوصية وشروط الاستخدام، وتقديم التوصيات وتقييم الخدمات، بالإضافة إلى إحالة المنتجات والخدمات إلى شبكاتهم الاجتماعية، ومشاركة البيانات أو الامتناع عن ذلك.

احترام الخصوصية والامتثال القانوني

يُعد احترام الخصوصية من الركائز الأساسية في التسويق عبر الأجهزة المحمولة، حيث يساهم في ترسيخ العلاقة بين العلامة التجارية والمستهلكين. إن الالتزام بهذه المبادئ يحقق مزايا استراتيجية، منها تعزيز سمعة العلامة التجارية، وزيادة التفاعل والمبيعات، وتحقيق الإحالات، وبناء الثقة. أما تجاهل الخصوصية، فيؤدي إلى مخاطر متعددة، مثل التعرض لهجمات إلكترونية وتسريبات بيانات، وتراجع السمعة، وخسارة المبيعات، وتآكل الثقة لدى المستهلكين، فضلاً عن العواقب القانونية والتنظيمية.

احترام الخصوصية والامتثال القانوني

على سبيل المثال:

شركة **Meta Platforms** وافقت على دفع غرامة بقيمة ١,٤ مليار دولار في ولاية تكساس لجمع بيانات بيومترية بشكل غير قانوني عبر تقنية التعرف على الوجه دون موافقة.

شركة **Meta (إنستغرام)** غُرمت بمبلغ ٤٠٥ مليون يورو من قبل لجنة حماية البيانات الأيرلندية بسبب التعامل غير السليم مع بيانات الأطفال، مما أدى إلى كشف معلومات الاتصال الخاصة بهم علنًا.

شركة **التأمين الصحي IHS** دفعت غرامة بقيمة ٥,١ مليون دولار بسبب خرق بيانات أثر على أكثر من ٩,٣ مليون شخص نتيجة تدابير أمنية غير كافية.

احترام الخصوصية والامتثال القانوني

علاوة على ذلك، يجب على المؤسسات الالتزام بواجباتها، مثل تأمين البيانات. مخاطر ضعف الأمن ليست بسيطة؛ فقد تصاعدت الجرائم الإلكترونية من حيث الحجم والنطاق والدرجة، لتصبح تحديًا عالميًا له آثار بعيدة المدى. وقد قُدرت التكلفة العالمية للجرائم الإلكترونية بأن تتجاوز ١٠,٥ تريليون دولار سنويًا بحلول عام ٢٠٢٥، مما يبرز العبء الاقتصادي الهائل الذي تفرضه على الحكومات والشركات والأفراد. كما أوضحت الاختراقات البارزة مثل تلك التي طالت Equifax (2017) و Marriott International (2018) كيف يمكن أن تُخترق البيانات الشخصية، بما في ذلك التفاصيل المالية والهوياتية لملايين الأشخاص، مما يؤدي إلى أضرار مالية وسمعية كبيرة.

اختراق أمني لبيانات أعضاء في الكونغرس عبر "شركة تأمين صحي"

10 مارس 2023 - 00:27 بتوقيت أبوظبي
أمينة اسريري - سكاى نيوز عربية - واشنطن



الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

تقليديًا، لمعالجة متطلبات الخصوصية في الهواتف المحمولة، يلجأ المسوقون ومؤسساتهم إلى أساليب تنظيمية تركز على إدارة الخصوصية، وتشمل:

- الالتزام بالمعايير،
- نهج السياسات والعمليات،
- نهج التصميم.

الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

الالتزام بالمعايير الخاصة بالصناعة والمنظمة

هناك عدة معايير تنظيمية وصناعية يجب على المؤسسات الالتزام بها، ومنها:

١. **تعيين مسؤول حماية البيانات (DPO):** يجب على المؤسسات التي تعالج كميات كبيرة من البيانات الشخصية أو تتعامل مع فئات خاصة من البيانات تعيين مسؤول حماية بيانات للإشراف على الامتثال والعمل كنقطة اتصال مع أصحاب البيانات والسلطات الرقابية.
٢. **مبادئ معالجة البيانات:** الالتزام بمبادئ مثل الشرعية، العدالة، الشفافية، تقليل البيانات، الدقة، تحديد فترة التخزين، النزاهة، السرية، والمساءلة.
٣. **الحصول على الموافقة:** يجب الحصول على موافقة واضحة ومستنيرة من الأفراد قبل جمع بياناتهم الشخصية ومعالجتها.

الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

الالتزام بالمعايير الخاصة بالصناعة والمنظمة

٤. حقوق أصحاب البيانات: يجب على المؤسسات احترام الحقوق مثل الحق في الوصول، التصحيح، الحذف ("الحق في النسيان")، تقييد المعالجة، قابلية نقل البيانات، والحق في الاعتراض.
٥. إشعارات الاختراق: يجب الإبلاغ عن أي اختراق للبيانات إلى السلطة الرقابية المختصة خلال فترة زمنية يحددها القانون، ويجب إخطار أصحاب البيانات المتأثرين دون تأخير إذا كان الاختراق يشكل خطرًا كبيرًا.

الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

نهج السياسات والعمليات المتعلقة بالخصوصية

لتلبية الالتزامات الصناعية والشركات والتنظيمية، ستعتمد المؤسسات والمسوقون عدة سياسات وعمليات، تشمل:

١. **سياسات جمع البيانات:** وضع بروتوكولات واضحة لجمع البيانات تحدد نوع البيانات التي يتم جمعها (مثل الأسماء، معرفات الأجهزة، بيانات الموقع)، وضمان توافقها مع المعايير القانونية.
٢. **آليات موافقة المستخدم:** تنفيذ إجراءات قوية للحصول على موافقة المستخدمين بشكل صريح على جمع البيانات والأنشطة التسويقية مثل الرسائل.
٣. **شفافية سياسة الخصوصية:** توفير سياسات خصوصية شاملة وسهلة الوصول تشرح كيفية جمع بيانات المستخدم وتخزينها واستخدامها.

الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

نهج السياسات والعمليات المتعلقة بالخصوصية

- لتلبية الالتزامات الصناعية والشركات والتنظيمية، ستعتمد المؤسسات والمسوقون عدة سياسات وعمليات، تشمل:
٤. **تقليل البيانات:** جمع البيانات الضرورية فقط للأغراض التسويقية المحددة لتقليل المخاطر والامتثال.
 ٥. **المراجعات الدورية وفحوصات الامتثال:** إجراء تدقيقات دورية للخصوصية لضمان توافق عمليات التعامل مع البيانات مع اللوائح الحالية وأفضل الممارسات الصناعية.
 ٦. **إتاحة الوصول والتحكم للمستخدم:** تمكين المستخدمين من الوصول إلى بياناتهم، وطلب حذفها، أو تعديل تفضيلاتهم بشأن مشاركة البيانات.
 ٧. **التدريب والتوعية:** تثقيف فرق التسويق حول معايير الخصوصية وأهمية حماية البيانات.

الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

نهج التصميم والبيانات

أخيراً، بدأت المؤسسات في تصميم منتجاتها وخدماتها بما يتوافق مع التزاماتها وسياساتها وإجراءاتها. ويُشار إلى هذه باسم نهج التصميم، وتشمل:

الخصوصية في التصميم Privacy by Design

استراتيجية أساسية يتم فيها دمج الخصوصية طوال دورة حياة المنتجات والخدمات. ويعني ذلك أخذ تدابير حماية البيانات في الاعتبار منذ البداية، بما في ذلك آليات قوية للحصول على موافقة المستخدم، وتقليل البيانات، وأمن شامل من طرف إلى طرف. يركز هذا النهج على الوقاية بدلاً من التصحيح، لضمان معالجة المخاطر المحتملة قبل أن تصبح مشكلات فعلية.

الأساليب التقليدية لإدارة الهواتف المحمولة والخصوصية

نهج التصميم والبيانات

الثقة في التصميم Trust by Design

يقوم على مفاهيم الخصوصية والأمان من خلال دمج الشفافية والمساءلة والممارسات الأخلاقية للبيانات في العمليات التجارية. تسعى الشركات إلى تعزيز ثقة المستخدمين عبر تنفيذ سياسات اتصال واضحة، وتوفير التحكم للمستخدمين في بياناتهم، واستخدام ممارسات آمنة لمعالجة البيانات. يضمن هذا النهج شعور الأطراف المعنية بالثقة في كيفية التعامل مع بياناتهم، بحيث تصبح الثقة عنصرًا أساسيًا في تجربة المستخدم.

الأساليب الحديثة لإدارة الهواتف المحمولة والخصوصية

مع استمرار تطور الأساليب التقليدية لإدارة الخصوصية في الهواتف المحمولة، يتم اعتماد حلول جديدة تركز على الهواتف لمعالجة التعقيدات المتزايدة في حماية البيانات وبناء الثقة مع المستخدمين. ومن بينها:

١- التطورات الأمنية

- بينما ركزت الأساليب التقليدية للحفاظ على الخصوصية على السياسات العامة لحماية البيانات ونماذج موافقة المستخدم، تدفع الحلول الحديثة حدود التكامل بين الأمان والخصوصية. وتشمل التطورات الأمنية تقنيات مثل:
- المصادقة البيومترية: تستخدم السمات البيولوجية الفريدة مثل بصمات الأصابع أو التعرف على الوجه للتحقق من هوية المستخدمين.

الأساليب الحديثة لإدارة الهواتف المحمولة والخصوصية

١- التطورات الأمنية

- مفاتيح الأمان المادية مثل **YubiKey**: تستخدم بروتوكولات تشفير للتحقق من الهوية، غالبًا عبر USB أو أجهزة متصلة أخرى.
- أنظمة كلمات المرور لمرة واحدة OTP: رمز مرور مؤقت يتم إرساله إلى البريد الإلكتروني أو الهاتف، ويُستخدم مرة واحدة فقط كجزء من المصادقة متعددة العوامل.

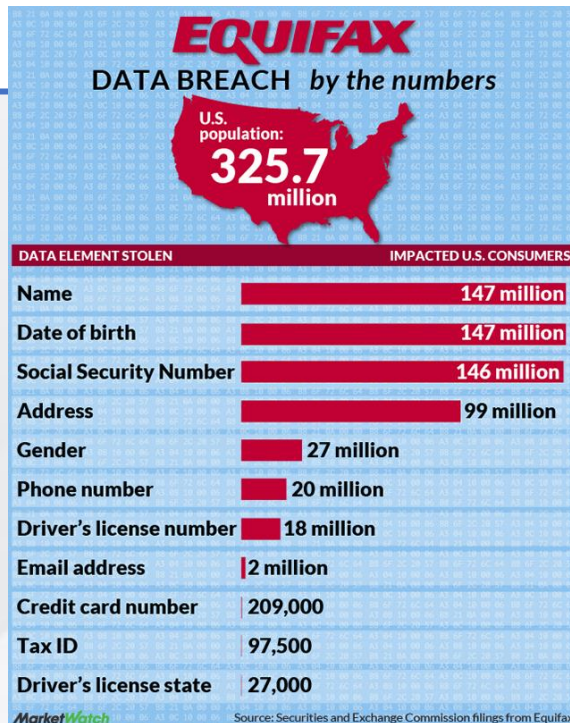
الأساليب الحديثة لإدارة الهويات المحمولة والخصوصية

٢- الهوية الذاتية السيادية والمشاركة المبدئية

يشهد السوق تحولاً كبيراً نحو نموذج الهوية الذاتية السيادية (SSI) self-sovereign identity، وإدارة الهوية والبيانات المبدئية. يُعد SSI نموذجاً للهوية الرقمية يتيح للأفراد التحكم الكامل في بياناتهم الرقمية، مثل هوياتهم، وسجلاتهم الرقمية (التعليم، الصحة، المالية، وغيرها)، والبيانات الخاصة، بالإضافة إلى تحديد كيفية ومتى ولماذا ولأي غرض يتم مشاركة هذه البيانات، ولأي مدة زمنية. وعلى عكس الأساليب التقليدية التي تُخزن فيها البيانات وتُدار بواسطة أطراف ثالثة (مثل الحكومات أو الشركات أو منصات التواصل الاجتماعي)، يضع نموذج SSI الأفراد في مركز إدارة هويتهم وبياناتهم.

دراسة حالة: Equifax Data Breach

في سبتمبر ٢٠١٧، تعرضت شركة Equifax، وهي واحدة من أكبر وكالات المعلومات الائتمانية في الولايات المتحدة، لاختراق أمني كبير أثر على حوالي ١٤٧ مليون شخص. البيانات المسروقة تضمنت معلومات شخصية حساسة مثل الأسماء الكاملة، تواريخ الميلاد، العناوين، أرقام الضمان الاجتماعي، وبيانات رخص القيادة. هذه المعلومات تم تسريبها إلى الدارك ويب، مما يزيد من خطر سرقة الهوية بشكل كبير.



دراسة حالة: Equifax Data Breach

الاختراق حدث بسبب ثغرة في برنامج Apache Struts 2 المستخدم في خوادم الشركة. رغم إصدار تحديث أمني في مارس ٢٠١٧، لم يرق فريق تقنية المعلومات في Equifax بتطبيق التصحيح، مما جعل الأنظمة معرضة للخطر من مايو حتى يوليو ٢٠١٧. هذا الإهمال في إدارة الثغرات الأمنية كان السبب الرئيسي في الكارثة.

دراسة حالة: Equifax Data Breach

النتائج والتأثيرات

الحادثة أدت إلى أضرار جسيمة، منها:

على الأفراد: زيادة خطر الاحتيال المالي وسرقة الهوية.

على الشركة: إقالة مجموعة من كبار المسؤولين في الشركة، خسارة عقد بقيمة ٧,٢ مليون دولار مع مصلحة

الضرائب، ودفع أكثر من ٢٤٢,٧ مليون دولار في غرامات ورسوم قانونية.

على المجتمع والصناعة: زيادة التدقيق على شركات الائتمان الأخرى، وتعرض ملايين الأشخاص لمخاطر

مستقبلية. تقرير Javelin لعام ٢٠١٨ أشار إلى سرقة ١٦,٨ مليار دولار من ١٦,٧ مليون مستهلك أمريكي.

دراسة حالة: Equifax Data Breach

الدروس المستفادة

أهمية إدارة الثغرات الأمنية: يجب تطبيق التحديثات فور صدورها.

الامتثال لمعايير الأمان والخصوصية: اعتماد سياسات مثل **Privacy by Design** و **Compliance by Design**.

التأثير الاستراتيجي: اختراق واحد يمكن أن يؤدي إلى خسائر مالية ضخمة وفقدان الثقة.

التوعية للمستهلكين: ضرورة تعزيز حماية الهوية الشخصية.

في هذه المحاضرة، ناقشنا الموضوعات التالية:

- مقدمة عن مفهوم الهوية والبيانات في التسويق الحديث.
- أنواع الهوية في البيئة الرقمية (الشخصية، الرقمية، الاحتمالية، الحتمية، هوية الوكيل).
- تصنيفات البيانات الخاصة (شخصية، غير شخصية، معرفات، بيانات موثوقة، بيانات حساسة).
- النهج المؤسسي مقابل النهج المتمحور حول الأفراد في إدارة الهوية والبيانات.
- الخصوصية وحقوق الأفراد، بما في ذلك مبادئ FIPPs واللائحة الأوروبية GDPR.
- الأساليب التقليدية لإدارة الخصوصية (المعايير، السياسات، التصميم).
- الأساليب الحديثة مثل الهوية الذاتية السيادية (SSI) والتطورات الأمنية.
- دراسة حالة عن اختراق بيانات شركة Equifax والدروس المستفادة.



Thank You