تعريف الخصوصية

الخصوصية هي حق الفرد في الحفاظ على معلوماته الشخصية وحياته الخاصة بطريقة اختيارية وحرة، وتتعلق بالمعلومات التي نختار مشاركتها مع آخرين أو لا نشاركها بناءً على أهميتها بالنسبة لنا أو للآخرين.

الخصوصية الرقمية

الخصوصية الرقمية تشير إلى قدرة الفرد على التحكم بالمعلومات التي يكشف عنها عبر الإنترنت، وتحديد من يمكنه الوصول إليها وأغراض استخدامها. تتضمن أيضًا حماية البيانات الشخصية والاتصالات والمراسلات عبر الإنترنت .

الهدف من خصوصية البيانات

يهدف إلى حماية البيانات من الوصول غير المصرح به أو الاستخدام غير القانوني. يتضمن ذلك التعامل السليم مع البيانات الشخصية، مثل الأسماء والعناوين وأرقام الضمان الاجتماعي والائتمان، إضافة إلى حماية البيانات الحساسة مثل المعلومات الصحية والمالية.

مراحل كل نوع من أنواع الخصوصية

1. **جمع البيانات**: يجب جمع البيانات بطرق قانونية وأخلاقية، مع إعلام الأفراد بنوع البيانات التي يتم جمعها والغرض منها.
2. **استخدام البيانات**: يجب استخدام البيانات فقط للأغراض التي جُمعت من أجلها، مع الحق في معرفة كيفية استخدام البيانات.
3. **تخزين البيانات**: يجب تخزين البيانات بشكل آمن لحمايتها من الوصول غير المصرح به.
4. **مشاركة البيانات**: يجب أن تكون هناك قيود على كيفية مشاركة البيانات مع الأطراف الثالثة، ويجب الحصول على موافقة الأفراد قبل المشاركة.

5. **الوصول إلى البيانات**: يشمل ذلك حق الأفراد في الوصول إلى بياناتهم، تصحيحها، وحذفها إذا لزم الأمر.

اختراق البيانات

يشير اختراق البيانات إلى حدوث كشف غير مصرح به للبيانات، حيث يتم الوصول إلى معلومات سرية أو حساسة بواسطة أشخاص ليس لديهم الحق في الاطلاع عليها. يمكن أن يشمل ذلك تسريب البيانات أو سرقتها، ويؤثر على الأفراد، الشركات، وحتى الحكومات .

القوانين المتعلقة بالأطفال

تنص العديد من القوانين على حماية خصوصية الأطفال عبر الإنترنت، وتوجيه الآباء إلى أهمية الاطلاع على شروط الخدمة في منصات التواصل الاجتماعي للتأكد من الامتثال للقوانين المحلية التي تتعلق بإنشاء الحسابات للأطفال .

الإجراءات القانونية المتعلقة بحماية البيانات

تهدف الإجراءات القانونية المتعلقة بحماية البيانات إلى وضع قوانين وأنظمة لمنع الوصول غير المشروع إلى البيانات أو التلاعب بها. تشمل هذه القوانين عادة فرض غرامات مالية على الأفراد أو المؤسسات التي تنتهك قوانين حماية البيانات، مع إمكانية اتخاذ إجراءات قانونية ضد المخالفين

الهدف من حماية البيانات

الهدف من حماية البيانات هو حماية البيانات الشخصية من الوصول غير المصرح به أو استخدامها بشكل غير قانوني. يتضمن ذلك حماية البيانات الحساسة مثل الأسماء، العناوين، أرقام الهواتف، وأرقام بطاقات الائتمان، كما يمتد إلى البيانات المالية والصحية.

1. القوانين والتشريعات

1. **قانون الجرائم الإلكترونية**: يهدف هذا القانون إلى مكافحة الجرائم التي تتم عبر الإنترنت والتكنولوجيا الحديثة، ويشمل حماية البيانات الشخصية للمستخدمين ومنع استخدامها أو نشرها دون إذن.

2. **قانون حماية البيانات الشخصية** :ينظم هذا القانون كيفية التعامل مع بيانات الأفراد، بما في ذلك الحصول على موافقتهم الصريحة قبل جمع البيانات. كما يحدد كيفية استخدام هذه البيانات ومنع استخدامها لأغراض غير قانونية.

القانون العام لحماية البيانات

القانون العام لحماية البيانات، مثل قانون GDPR (اللائحة العامة لحماية البيانات)، يهدف إلى توحيد قوانين الخصوصية في الاتحاد الأوروبي ويشمل مبادئ أساسية مثل إعلام الأفراد بنوع البيانات التي يتم جمعها والغرض منها، الحفاظ على دقة البيانات، وعدم الاحتفاظ بالبيانات لفترة أطول من اللازم.

2. مبادئ جمع البيانات وأخلاقياتها

1. **الشفافية** :يجب أن يتم جمع البيانات بطريقة شفافة، مع إبلاغ الأفراد بوضوح حول كيفية استخدام بياناتهم.
2. **الحد الأدنى** :يجب جمع الحد الأدنى من البيانات الشخصية الضرورية لتحقيق الغرض المحدد.
3. **الموافقة** :يتطلب جمع البيانات موافقة صريحة من الأفراد، ويجب أن تكون هذه الموافقة قابلة للسحب في أي وقت.
4. **السرية** :يجب الحفاظ على سرية البيانات وعدم الكشف عنها لأطراف غير مصرح لها، والاحتفاظ بالبيانات فقط للفترة اللازمة.

3. حقوق الأفراد

1. **الحق في الوصول** :للأفراد الحق في معرفة البيانات التي تم جمعها عنهم وكيفية استخدامها.
2. **الحق في التصحيح** :يحق للأفراد تصحيح أي بيانات غير دقيقة أو غير مكتملة.
3. **الحق في المحو** :يحق للأفراد طلب حذف بياناتهم الشخصية في ظروف معينة.

4. **الحق في الاعتراض** :يمكن للأفراد الاعتراض على معالجة بياناتهم الشخصية لأغراض معينة، مثل التسويق المباشر.

4. اجراءات الأمان

1. **التشفير** :يجب استخدام تقنيات التشفير لحماية البيانات الشخصية أثناء النقل والتخزين.
2. **التحقق بخطوتين** :تعزيز أمان الوصول إلى البيانات باستخدام تقنيات التحقق المزدوج.
3. **التدريب والتوعية** :يتطلب من الشركات تدريب موظفيها على أفضل ممارسات حماية البيانات.

كيفية المحافظة على البيانات الشخصية

1. حماية كلمات المرور

- **استخدام كلمات مرور معقدة وفريدة** :من الضروري أن تكون كلمات المرور المستخدمة على الإنترنت طويلة ومعقدة، حيث يجب أن تتضمن مزيجاً من الأحرف الكبيرة والصغيرة والأرقام والرموز الخاصة. هذا يساعد على جعل كلمة المرور أقل عرضة للتخمين أو الهجوم بواسطة تقنيات الاختراق مثل "هجوم القوة العمياء."

2. استخدام المصادقة الثنائية

- **المصادقة الثنائية كوسيلة لحماية الحسابات** :المصادقة الثنائية هي خطوة إضافية من الأمان تتطلب من المستخدم تقديم نوعين من المعلومات للتحقق من هويته. في العادة، تتضمن هذه الخطوة إدخال كلمة المرور ثم رمز يتم إرساله إلى الهاتف المحمول أو عبر البريد الإلكتروني.

3.تأمين البريد الإلكتروني

- **تجنب إرسال معلومات شخصية حساسة عبر البريد الإلكتروني** :يجب على المستخدمين الحذر عند إرسال معلومات شخصية حساسة مثل أرقام البطاقات الائتمانية أو المعلومات المالية عبر البريد الإلكتروني، حيث أن البريد الإلكتروني قد يكون عرضة للاختراق. إذا كان لا بد من إرسال هذه المعلومات، يجب تشفير البريد الإلكتروني أو استخدام خدمات رسائل مشفرة.
- **مراقبة الأجهزة** :يجب الحفاظ على تحديث الأجهزة بشكل دوري وتثبيت برامج مضادة للفيروسات لحمايتها من التهديدات.
- **الحذر من النقر** :يجب تجنب النقر على الروابط المشبوهة أو المرفقات التي تأتي من مصادر غير معروفة أو مشبوهة لأنها قد تحتوي على برمجيات خبيثة.
- **تأكد من تحديث أنظمة التشغيل** :يجب التأكد من تحديث أنظمة التشغيل بانتظام لتأمين الأجهزة ضد الثغرات الأمنية.

اجراءات وقائية مقترحة

حالة 1 :استخدمت نور كلمة المرور نفسها لجميع حساباتها الإلكترونية، مما أدى إلى سرقة بياناتها الشخصية واستخدامها لاختراق حساباتها الأخرى.

- **إجراء وقائي مقترح** :يجب على نور استخدام كلمات مرور معقدة وفريدة لكل حساب وتفعيل المصادقة الثنائية لتقوية الأمان.

الحالة 2 :تلقت ليلى بريدًا إلكترونيًا يحتوي على رابط من مصدر غير معروف. عند النقر على الرابط، تم تنزيل برمجيات خبيثة على جهازها مما أدى إلى فقدان بعض ملفاتها المهمة.

- **إجراء وقائي مقترح** :يجب على ليلى عدم النقر على الروابط أو فتح المرفقات من مصادر غير معروفة. عليها التحقق من المرسل قبل فتح الرسائل أو الروابط

الحالة 3 :شارك أحمد تفاصيل كثيرة عن حياته اليومية على وسائل التواصل الاجتماعي. استغل أحد المتابعين هذه المعلومات لمعرفة أوقات غيابه عن المنزل وسرقته.

- **إجراء وقائي مقترح** :يجب على أحمد تجنب نشر التفاصيل الشخصية بشكل مفرط على وسائل التواصل الاجتماعي، خاصة تلك التي تتعلق بمواعيد تواجده أو غيابه عن المنزل.

الحالة 4 :تعرض حساب بريد راشد الإلكتروني للاختراق، مما أدى إلى فقدان بعض المراسلات المهمة.

- **إجراء وقائي مقترح** :يجب على راشد استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية على حسابات البريد الإلكتروني لحمايتها من الاختراق.