CERT.sa
المركز الوطني الارشادي لامن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

المركز الوطني الإرشادي لأمن المعلومات CERT-SA

لمحة:

المركز الوطني الإرشادي لأمن المعلومات بهيئة الاتصالات وتقنية المعلومات، هو مركز غير ربحي يهدف إلى رفع مستوى الوعي والمعرفة بأخطار أمن المعلومات، ويعمل بالتعاون مع أعضائه وشركائه على تنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة العربية السعودية.

رؤيتنا:

أن نكون المرجعية الموثوق بها لأمن المعلومات في المملكة العربية السعودية.

مهمتنا:

- رفع مستوى الوعي بأمن المعلومات في المملكة العربية السعودية.
- تنسيق الجهود على المستوى الوطني لتفادي الاختراقات الأمنية، والعمل على احتواء أضرارها حال وقوعها.
- رفع مستوى الثقة في التعاملات الإلكترونية.
- التعاون والتنسيق مع المؤسسات والأطراف المؤثرة في تقديم خدمات الاتصالات وتقنية المعلومات في المملكة العربية السعودية في سبيل وقاية البنى التحتية والخدمات الإلكترونية من أخطار وتهديدات أمن المعلومات.
- تقديم المشورة والنصح للأفراد والمؤسسات فيما يتعلق بأمن المعلومات.

لمزيد من المعلومات الرجاء زيارة موقع المركز
www.cert.gov.sa

سبل حماية الخصوصية في العالم الرقمي

CERT.sa
المركز الوطني الارشادي لامن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

مجمع الملك عبدالعزيز للاتصالات
هاتف ٢٦٣٩٢٣١ ١ ٩٦٦+
فاكس ٤٥٤٦٩٨٤ ١ ٩٦٦+
ص.ب ٧٥٦٠٦ الرياض ١١٥٨٨
المملكة العربية السعودية
www.cert.gov.sa
info@cert.gov.sa

CERT.sa
المركز الوطني الارشادي لامن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

Z CO. 477 00 33

سبل حماية الخصوصية في العالم الرقمي

تعد الشبكة العنكبوتية (الإنترنت) وسيلة الاتصال الأولى بالعالم في هذا العصر. وبسبب انتشارها وتنوع خدماتها وانخفاض تكلفة الوصول إليها نسبياً، أصبح العالم مجتمعاً افتراضياً، ويمكن أفراده من التفاعل مع بعضهم ومشاركة معارفهم (Knowledge Sharing).

ومع تزايد إقبال الناس للاستفادة من إيجابيات استخدام الإنترنت، ظهر الشعور بمخاطره وتهديداته أيضاً، وتنامى هذا الشعور مع زيادة حالات الاعتداء على البيانات الشخصية للمستخدمين واستخدامها بشكل غير قانوني.

إن مفهوم خصوصية المعلومات يعني حق الإنسان في التحكم بوصول الآخرين واطلاعهم على معلوماته الشخصية حتى وإن كانت هذه المعلومات لدى جهات أخرى مخولة بحفظها أو حفظ بعضها (مثل السجل الطبي للمريض لدى المستشفى)، وتشمل البيانات الشخصية للمستخدم كل المعلومات المتعلقة بجوانب حياته الخاصة كإسمه وعمره ومكانه وسجلاته الطبية والمالية وغيرها مما يتعلق بشخصه.

ومما يدخل في نطاق الخصوصية للإنسان مراعاة الشركات والمؤسسات لخصوصية معلومات موظفيها وعملائها، فهذه المؤسسات مسؤولة قانونياً عن حماية المعلومات الشخصية التي تحفظها من المتطفلين أو غير المخولين، ويجب اقتصار استخدامها على الخدمات التي تم الاتفاق مع العميل على تقديمها له.

إن معرفة سبل حماية خصوصية معلوماتك أثناء استخدامك للإنترنت يقلل من احتمال تعرضها لمخاطر الاستخدام غير المشروع والذي يلحق الضرر بك معنوياً أو مادياً.

خطوات حماية المعلومات الشخصية

١. يجب عدم إعطاء المعلومات الشخصية لمواقع الإنترنت إلا عند الضرورة، ويجب التأكد من هوية الموقع وأنه يمثل منشأة معروفة، وعلى المستخدم الاطلاع الدقيق على سياسة حماية الخصوصية التي يتبعها الموقع للتأكد من عدم احتوائها على شروط قد تخل بالخصوصية وتسمح للموقع بالتصرف بالمعلومات، فالكثير من المستخدمين يوافقون على الشروط دون الاطلاع عليها، وعلى الجانب الآخر تجنب المغامرة بإعطاء معلوماتك للمواقع غير الموثوقة مثل المنتديات وغيرها.

٢. إن التعامل مع أشخاص مجهولي الهوية من خلال شبكة الإنترنت يحتم توخي الحذر وعدم المجازفة بإعطاء معلومات تخص المستخدم، وكذلك عدم إبداء الثقة مباشرة مع أي شخص أو موقع على الشبكة، لأن شبكة الإنترنت قد أصبحت مصدر قلق وأخذت الجريمة المنظمة تتنامى فيها، فبرامج المحادثة والمنتديات ومشاركة الملفات كلها أدوات يجب استخدامها بحذر، كما ينبغي تنبيه الأطفال وتعليمهم أهمية حماية خصوصياتهم وخصوصيات أسرهم، وعدم تسريب المعلومات الشخصية للغرباء على شبكة الإنترنت، واستشارة الوالدين عند مواجهتهم لمثل هذه المواقف.

٣. يفضل عدم إرسال معلومات شخصية إلا من خلال قناة مشفرة باستخدام بروتوكول (https)، لأن بروتوكول التشفير يعتمد على شهادة إلكترونية تصدر من جهة مستقلة تتحقق من هوية الموقع قبل إصدارها، وتنتقل البيانات داخل قناة مشفرة بحيث لا يستطيع أحد الاطلاع عليها أثناء انتقالها، وللتعرف على نوع البروتوكول يمكن للمستخدم قراءة حقل العنوان في المتصفح والتأكد من أنه يبدأ بحروف (https)، أو التأكد من وجود علامة القفل في إحدى زوايا المتصفح.

٤. ضرورة تصميم سياسات الخصوصية في المنشآت لحماية المعلومات الشخصية للموظفين والعملاء، وهذا أمر أساسي في سبيل حماية المعلومات الشخصية من الاستخدام غير المشروع، فالسياسات والإجراءات يجب أن تحدد كيفية تخزين المعلومات والدخول إليها وتنظيمها وحمايتها وذلك باستخدام تقنية التشفير، وتنظيم الدخول والتدقيق في سجلات الدخول للمعلومات لاكتشاف أي عمليات غير مشروعة وإيقافها ومحاسبة المتسببين في ذلك، كما يجب عدم إفشاء المعلومات لطرف ثالث دون الرجوع لصاحب هذه المعلومات وأخذ الإذن منه لتجنب أي ملاحقة قانونية.

٥. تقوم بعض المواقع على شبكة الإنترنت بجمع معلومات شخصية عن المستخدم قد تساعد في تحديد هويته واهتماماته، فعلى سبيل المثال تقوم مواقع البحث الشهيرة باستخدام البريد الإلكتروني الذي تقدمه هذه المواقع لتحديد هوية المستخدم والكلمات والمواضيع التي يبحث عنها، بل إن بعض المواقع مثل ياهو (yahoo) صرّح بأنه يقوم بجمع معلومات شخصية لأصحاب البريد.

٦. اتبع الخطوات التالية للمحافظة على أمن جهازك وملفاتك الشخصية:

- لا تعتمد رقماً سرياً موحداً لجميع حساباتك على الإنترنت، ولكن استخدم كلمات سر مختلفة بحسب أهمية الحساب، مع ضرورة تجنب استخدام كلمات سر سهلة التخمين.
- لا تستخدم أجهزة الحاسبات العامة مثل مقاهي الإنترنت أو معامل الجامعة للوصول إلى معلوماتك الشخصية الهامة، فقد تكون عرضة للمراقبة من خلال برامج التجسس أو المخترقين.
- افحص جهازك دورياً للتأكد من خلوه من الفيروسات وبرامج التجسس المعروفة بـ (Spyware) وبرامج الدعاية المعروفة بـ (ad-ware) فهذه البرامج تتبع نشاطاتك واهتماماتك (من خلال المواقع التي تقوم بزيارتها)، ثم ترسل معلوماتك التي تجمعها إلى المنظمات والشركات التي أنتجتها.
- كذلك قم بتحديث نظام التشغيل والمتصفح بشكل منتظم (من خلال مواقع الشركات المنتجة لها) لسد الثغرات التي قد يتسلل منها المخترقون لسرقة الملفات والمعلومات الشخصية.
- استخدم التشفير لحماية ملفاتك الإلكترونية التي تحتوي على معلومات شخصية هامة.
- قد تكون ملفات كوكيز (وهي ملفات نصية تحفظ في جهاز المستخدم أثناء زيارة بعض المواقع) تهديداً لخصوصيتك، لذا عليك التخلص من ملفات الكوكيز غير الضرورية من فترة لأخرى وذلك عن طريق الخيارات التي توجد في متصفح الإنترنت.
- لمزيد من النصائح بخصوص حماية الأجهزة الشخصية يرجى الاطلاع على النشرة التوعوية (ثمان نصائح لحماية الجهاز الشخصي من مخاطر الإنترنت) الصادرة عن المركز الوطني الإرشادي لأمن المعلومات.