حماية البريد الإلكتروني

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

CERT.sa
المركز الوطني الإرشادي لأمن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

CERT.sa
المركز الوطني الإرشادي لأمن 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

Z.CO.477.00.33

CERT.sa
المركز الوطني الإرشادي لأمن 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

حماية البريد الإلكتروني

يمثل البريد الإلكتروني أداة من أبرز أدوات التواصل العصرية. ومن النادر وجود شخص لم يسمع عن البريد الإلكتروني أو لم يستخدمه، كما أنه أصبح من أول الأهداف التي يسعى وراءها المخترقون (Hackers)، لذلك يجب الحرص على حمايته، والخطوات التالية توضح بعض الأساليب والطرق التي تساعد على حماية بريدك الإلكتروني:

١. المرفقات Attachments

وهي الملفات التي ترفق مع الرسالة، فقد يستغلها المرسل بإرفاق بعض البرمجيات الضارة، وإليك بعض النصائح لتجنب ذلك:

- لا تقم بفتح أو حفظ أي مرفق إلا إذا كنت تتوقع استقبال ذلك الملف.
- قبل فتح أي ملف مرفق قم بفحصه بأحد برامج مكافحة الفيروسات.

وإليك أمثلة لبعض امتدادات الملفات المرفقة التي غالباً ما تحتوي على البرمجيات الضارة (pif, scr, exe, dll, vbs, bat).

٢. الرسائل الاحتيالية Phishing

هي إحدى الطرق المفضلة لدى المخترق (Hacker) أو المحتال، حتى يتمكن من سرقة بريدك الإلكتروني أو معلوماتك الحساسة، والأمثلة على ذلك كثيرة ومتجددة، منها أن تصلك رسالة بنفس شكل وصياغة مزود خدمة بريدك الإلكتروني أو البنك الذي تتعامل معه، ويطلب منك تعديل بياناتك الخاصة لوجود مشكلة فنية ويضع رابط موقع إلكتروني مزيف شبيه بموقع مزود الخدمة الأصلي أو البنك، وهنا قد لا يستطيع المستخدم تمييز الموقع المزيف ويضع جميع معلوماته المهمة ومنها كلمة السر. ولتفادي الوقوع في مثل هذه الحيل يجب التأكد من وجود قفل الأمان في زاوية المتصفح والتي تدل على وجود الشهادة الرقمية (digital certificate) لاعتماد الموقع عند صفحة تسجيل الدخول، كما ينصح بالحذر والتحقق قبل إدخال أي معلومة خاصة على أي موقع إلكتروني.

٣. استخدام أكثر من بريد

الطريقة المثلى في التعامل مع البريد الإلكتروني هي الاشتراك في أكثر من بريد واحد، بحيث يكون أحدهما مخصص للمراسلات المهمة والحساسة، وفي هذه الحالة ينصح بالتالي:

- حاول قدر المستطاع ألا ينشر بريدك للعامة.
- اختيار كلمة سر لا تقل عن ٨ خانات مكونة من حروف وأرقام ورموز.
- احرص على تغيير كلمة السر من فترة لأخرى.
- لا تتصفح البريد الإلكتروني إلا على جهازك الخاص.
- يفضل أن يكون حساب البريد الإلكتروني من شركة موثوقة.

أما البريد الآخر فيكون بعكس الأول بحيث يكون للاستخدامات غير المهمة، فعلى سبيل المثال بعض المواقع تلزمك بوضع بريدك الإلكتروني حتى تقرأ المحتوى وعند القيام بذلك تقوم بإرسال رسائل دعاية وتنشر بريدك لمواقع أخرى، لذلك سيكون أكثر عرضة للخطر والرسائل الاقتحامية (SPAM) – الاحتيالية (Phishing).

٤. استخدام النص الخالي من رموز لغة الترميز (HTML)

عند استقبال رسالة إلكترونية ويكون الخط فيها بألوان عديدة وأحجام مختلفة، فهي دلالة على أنها مكتوبة برموز (html)، لذلك ينصح خبراء أمن المعلومات على أن تستقبل الرسالة (plain text) أي تكون خالية من رموز (html)؛ وذلك لتفادي خطرين أولهما احتمال معرفة معلومات خاصة بجهازك، والثاني احتمال زرع برمجيات ضارة في جهازك، وفيما يلي تفصيل لهذين الخطرين.

أولاً: خطر انتهاك الخصوصية

عندما يرسل لك شخص رسالة تحتوي على رموز (html) فقد يكون باستطاعته معرفة التالي عنك:

- عنوان آي بي (IP) لجهازك.
- وقت قراءة الرسالة وتاريخها.
- نوع نظام التشغيل ومتصفح الإنترنت.

ومعرفة هذه المعلومات من قبل المخترق تجعل جهازك أكثر عرضة لمخاطر أمن المعلومات.

ثانياً: احتواؤها على برمجيات تنفيذية

أيضاً باستطاعة المرسل أن يضيف من خلال رموز (html) بعض البرمجيات الضارة وتكون مخفية داخل الترميز ولا يستطيع المستخدم تمييزها.

٥. الاتصال الآمن

تستطيع تصفح بريدك الإلكتروني بأحد الأساليب التالية:

أولاً: عن طريق متصفح الإنترنت مثل هوتميل (hotmail) وياهو (yahoo)، ففي هذه الحالة تأكد أن الموقع يدعم بروتوكول التشفير (https)، وتستطيع معرفة ذلك عن طريق ظهور أيقونة قفل صغير في شريط الحالة للمتصفح.

ثانياً: عن طريق برامج إدارة البريد مثل مايكروسوفت أوتلوك (microsoft outlook)، ففي هذه الحالة تأكد من وضع الإعدادات الصحيحة عند استخدام بروتوكول جلب البريد (pop3) وذلك عن طريق خاصية التشفير (ssl) ويكون البريد محمياً باسم مستخدم وكلمة سر.

٦. استخدام التوقيع الإلكتروني

يستخدم التوقيع الإلكتروني في حال الحاجة للمراسلات الموثوقة والرسمية والتجارية، التي تتطلب قدراً أعلى من الحفاظ على السرية وأمن المعلومات. والتوقيع الإلكتروني لا يقصد به الاسم أو الصورة التي تظهر أسفل الرسالة، بل يقصد به توثيق مصدر الرسالة باستخدام شهادة رقمية تستطيع الحصول عليها من جهة موثوقة مخولة بإصدار هذا النوع من الشهادات، وتحتوي الشهادة الرقمية على مفتاح عام وحيد ومعلومات عن صاحب المفتاح العام، وأيضاً مفتاح خاص لا يعرفه إلا مالك الشهادة، والتوقيع الإلكتروني يولّد عن طريق برنامج البريد والمفتاح الخاص، والغرض من استخدامه تأكيد الرسالة وضمان عدم تحريف محتوى الرسالة.