CERT.sa
المركز الوطني الارشادي 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

الرسائل المزعجة
(SPAM)

CERT.sa
المركز الوطني الارشادي 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

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

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

Z CO. 477 00 33

الرسائل المزعجة (SPAM)

تُعرف أيضاً بالرسائل الاقتحامية، وهي الرسائل المرسلة بشكل عشوائي إلى الكثير من الناس دون أخذ موافقتهم على استقبالها، وتهدف بالعادة إلى الترويج لسلع أو خدمات أو مواقع إنترنت.

وتتمثل أضرار الرسائل المزعجة (SPAM) بالدرجة الأولى في إساءة استخدام نظم تبادل الرسائل، لأنه يتم عن طريقها إرسال رسائل إعلانية وتجارية لجدواها الاقتصادية، إذ يستطيع المرسل إرسال إعلانه بقيمة لا تتجاوز تكلفة البحث عن عناوين الاتصال أو القوائم البريدية، ويعتمد أصحاب الرسائل المزعجة على إرسال الملايين منها على أمل استجابة شخص واحد من ألف شخص مما يحقق لهم الثراء بسرعة.

ومع تزايد عدد هذه الرسائل في الوقت الحاضر يظهر مصدر خطورتها، وبالإضافة إلى الإزعاج الذي تتسبب فيه لمتلقيها، وفي بعض الأحيان قد تحمل عبارات نابية وإباحية تخدش الحياء، وتحطم القيم والأخلاق.

وفي إحصائية من شركة رائدة في مجال حماية البريد الإلكتروني (Postini.com) نشرت عام ٢٠٠٥م، تبين أن ٨٨٪ من نسبة الرسائل الإلكترونية تمثل رسائل مزعجة، بينما تمثل الرسائل الصالحة منها ما نسبته ١٢٪.

أشهر أنواع الرسائل المزعجة

١. رسائل البريد الاقتحامية

وهي رسائل تكون ذات مضمون تجاري ودعائي في الغالب، وترسل بكميات كبيرة وبشكل عشوائي إلى العناوين البريدية لمجموعة من مستخدمي الإنترنت عن طريق استخدام برامج تستطيع التعرف على شكل العناوين البريدية المدرجة في مختلف مواقع الإنترنت، ومن ثم إرسال الرسائل المزعجة إلى هذه القوائم.

وفي هذه الأيام أصبحت نسبة الرسائل الاقتحامية عبر البريد مرتفعة جداً، مما أجبر المستخدمين ومقدمي خدمات الإنترنت على تحمل تكاليف إضافية لمواجهة هذه المشكلة.

٢. الرسائل الاقتحامية عبر برنامج المراسلة الفورية

تتيح الكثير من برامج المحادثة الفورية الاطلاع على معلومات المستخدمين، مما سهل جمع عناوين الاتصال التي يمكن أن تستخدم في الرسائل الاقتحامية الفورية، وعن طريقها يتم إرسال الرسائل ذات المضامين المختلفة لهم.

٣. الرسائل الاقتحامية عبر غرف المحادثة

تظهر هذه الرسائل في أي من غرف المحادثة بشكل يسهل رؤيته من قبل المستخدم، وتتألف الرسائل الاقتحامية المرسلة المستخدمة في هذه الغرف من نص يتم تكراره عدة مرات للفت نظر المستخدم واهتمامه.

٤. الرسائل الاقتحامية عبر الهواتف المتنقلة

يتم إرسال هذه الرسائل إلى أرقام الهواتف المتنقلة، وهناك العديد من الطرق للحصول على هذه الهواتف واستغلالها لمثل هذا الغرض، ومنها جمع أرقام الهواتف المتنقلة المدرجة في قوائم بيانات مختلف المواقع، إذ يتم إرسال الإعلانات التجارية إلى هذه الإرقام عبر نظام الرسائل النصية القصيرة (SMS).

طرق الحماية من الرسائل المزعجة

- استخدام برامج ترشيح الرسائل الاقتحامية في الجهاز مثل برنامج (Mailwasher Pro) أو برنامج (Norton Antispam).
- استخدام خاصية التبليغ عن الرسائل الاقتحامية التي يوفرها بعض مزودي خدمة البريد الإلكتروني، ليتم حذف الرسالة ووضع المرسل في قائمة المنع، مما يعني عدم قدرته على مراسلتك مرة أخرى، وفي حال عدم توفر هذه الخاصية من قبل مزود البريد فعليك حذف الرسائل الاقتحامية مباشرة.
- استخدام برنامج حماية من الفيروسات، وجداراً نارياً والحفاظ على تحديثهما، فأجهزة الكمبيوتر غير المحمية قد تستغل من مرسلي الرسائل الاقتحامية، وذلك باختراقها ثم إرسال البريد المزعج عن طريقها فيظهر جهازك بأنه هو المصدر.
- استخدم طرقاً مختلفة لكتابة معلوماتك في صفحات الإنترنت، فإن مرسلي البريد المزعج يستخدمون عدة برامج تستطيع جمع معلومات الاتصال آلياً، فإذا كنت مضطراً مثلاً لكتابة بريدك الإلكتروني فيمكنك وضعه ضمن صورة وهذا هو أفضل أسلوب، أو كتابته بطريقة مختلفة كأن تستبدل علامة (@) بكلمة (AT) والنقطة (.) بكلمة (dot) على أن تكون بين قوسين مثال:

  (username@server.com) (username(at)server(dot)com).
- عدم إعطاء الآخرين معلومات خاصة بك مثل بريدك الإلكتروني أو رقم هاتفك، وإذا لزم تداول هذه المعلومات فأعطها للمواقع أو الأشخاص الموثوقين فحسب، ولا تنشر هذه المعلومات في أي من مواقع الإنترنت.
- احذر استخدام بريدك الرسمي للتسجيل في المواقع غير الموثوقة، كمواقع المحادثة أو المنتديات أو غيرها من المواقع، واستخدم بريداً إلكترونياً بديلاً لهذه الأغراض، لذلك ينصح باستخدام أكثر من بريد إلكتروني يكون أحدهما للمراسلات المهمة والحساسة، والآخر للاستخدامات غير المهمة.
- احذر فتح الرسائل الاقتحامية أو الملفات المرفقة بها، لأنها قد تتسبب في أضرار لجهازك مثل إصابته بالفيروسات، وعلى العموم يجب عدم الرد أو الاستجابة لهذه الرسائل بأي طريقة لكي لا يتأكد مرسلوها بأن بريدك صحيح وقيد الاستخدام ومن ثم يتم إغراقه بإرسال المزيد.
- احذر من رسائل الاحتيال الاقتحامية، فقد تستقبل رسالة تظهر بأنها من بنك أو مؤسسة مالية تطلب إرسال معلومات مهمة، مثل رقم الحساب أو البطاقة الائتمانية، وعند ورود مثل ذلك يجب عدم الرد عليها، وتبليغ البنك مباشرة للتعامل مع هذه الرسالة، وننصح بالرجوع للنشرة الإرشادية الخاصة بالتصيد الإلكتروني الصادرة من المركز الوطني الإرشادي لأمن المعلومات.