ثمان نصائح لحماية الجهاز الشخصي من مخاطر الإنترنت

CERT.sa

المركز الوطني الإرشادي لأمن المعلومات

COMPUTER EMERGENCY RESPONSE TEAM

هيئة الاتصالات وتقنية المعلومات

Communications and Information Technology Commission

CERT.sa

المركز الوطني الإرشادي لأمن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

المركز الوطني الإرشادي لأمن المعلومات CERT-SA

لمحـــة:

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

أولاً: حصن جهازك ضد الفيروسات والبرامج التخريبية

تعتبر الفيروسات والبرامج التخريبية مثل حصان طروادة أو التروجان (Trojan Horse) والدودة (Worm) من البرامج التي صممت لإحداث أضرار في جهاز الكمبيوتر، مثل العبث بالملفات أو استهلاك موارد النظام والشبكة، وغالباً ما تختبئ الفيروسات والبرامج التخريبية في ملفات أخرى حتى يصعب إيجادها والتخلص منها.

وتتلخص خطوات الحماية من الفيروسات والبرامج التخريبية فيما يلي:

- تركيب برامج مكافحة الفيروسات مثل البرنامج المجاني (Calmwin) أو البرامج التجارية مثل (McAfee) أو (Norton) وغيرها.
- تحديث برامج مكافحة الفيروسات بشكل دوري (أسبوعي).
- عدم فتح مرفقات البريد الإلكتروني قبل التأكد من هوية المرسل؛ تحسباً من أن تكون مصابة بإحدى الفيروسات، كما ينبغي تفحص الملحقات ببرنامج الحماية قبل فتحها.
- تحديث نظام التشغيل ومتصفح الإنترنت (راجع الخطوة الخامسة).
- عدم تركيب برامج من مصادر ومواقع إنترنت غير معروفة، مثل مواقع النسخ غير القانونية على الإنترنت، فغالباً ما تكون هذه المواقع تابعة لمخترقين يسعون من خلالها إلى اختراق أجهزة الزوار. وعوضاً عن ذلك يمكن استخدام الطريقة الآمنة للحصول على البرنامج سليماً وخالياً من الفيروسات، وهي تحميل البرنامج من موقع الشركة المنتجة أو أقراصها المتوفرة في الأسواق.

ثانياً: احذر من برامج التجسس والدعاية

أ. برامج التجسس

برامج تستخدم لجمع معلومات عن مستخدم الجهاز دون علمه، وتقوم بإرسال المعلومات لنقطة تجميع معلومات على الإنترنت. بعض هذه البرامج تتنصت على ما يكتبه المستخدم على لوحة التحكم.

ب. برامج الدعاية

برامج أو مواقع تعرض على شاشة المستخدم دعايات ونوافذ عرض دعائية أو قد تقوم بعرض مواقع معينة على جهاز المستخدم مما يسبب الإزعاج للمستخدم واستهلاك خط الاتصال بالإنترنت، وتستخدم برامج الدعاية نفس أسلوب برامج التجسس لجمع المعلومات عن المستخدم.

طرق مكافحة برامج التجسس والدعاية

- استخدام برامج مكافحة التجسس والدعاية لاكتشافها وحذفها، وأيضاً تساعد هذه البرامج على منع برامج التجسس من إصابة الجهاز، ومن هذه البرامج (Windows Defender, Lavasoft, Spybot).
- عدم النقر بالفأرة على النوافذ الدعائية أو أي من الروابط داخلها، وإغلاقها يكون عن طريق الضغط على علامة (X) في الشريط العلوي للنافذة.
- تجنب استخدام البرامج المجانية قدر الإمكان، فقد تكون برامج الدعاية والتجسس جزءاً من اتفاقية استخدام البرنامج المجاني، حيث تعمد بعض الشركات لذلك لتغطية كلفة إنتاجها لهذه البرامج.
- تجنب زيارة المواقع المشبوهة مثل المواقع الإباحية لأنها كثيراً ما تحتوي على نوافذ دعائية أو برامج تجسس.
- اضبط إعدادات المتصفح لمنع النوافذ الدعائية من الظهور باستخدام خاصية (Pop-up blocker).

ثالثاً: حافظ على كلمات السر

تكمن أهمية كلمات السر بأنها الطريقة التقليدية لحماية حساب المستخدم في الجهاز الشخصي أو على الإنترنت، مما يجعل كلمات السر من أهم ما يجب الحرص عليه، ويجب تجنب كلمات السر سهلة الكسر لتجنب سرقة الملفات الشخصية أو البريد الإلكتروني أو غيره من الحسابات على الإنترنت، وفيما يلي عدد من خصائص كلمات السر الجيدة:

- ألا تقل عن سبعة خانات.
- أن تكون خليطاً من الأرقام والحروف والرموز مثل (# أو @).
- ألا تكون مبنية على معلومات شخصية مثل رقم الهاتف أو أسماء الأقارب.
- ألا تكون كلمة من القاموس العربي أو الإنجليزي.
- يجب استخدام كلمة سر مستقلة لكل حساب هام، مثل حسابات البنوك.
- أن تكون سهلة التذكر بحيث لا يضطر المستخدم لكتابتها على ورقة.
- تغيير كلمة السر بصفة دورية.

رابعاً: حصن جهازك بجدار ناري (Firewall)

الجدار الناري برنامج ينظم آلية الاتصال بالإنترنت عن طريق تأدية وظيفتين:

الوظيفة الأولى

أن يمنع المخترقين من الاتصال بالجهاز الشخصي عبر الإنترنت؛ حيث يراقب الاتصالات الواردة للجهاز ويمنع المشبوه منها.

الوظيفة الثانية

أن يمنع البرامج غير المصرح لها بالاتصال الخارجي بالشبكة، وتكمن أهمية هذه الوظيفة بمنع تسريب معلومات المستخدم من قبل برامج التجسس.

ويمكن لمستخدمي (ويندوز إكس بي) نسخة الترقية الثانية (sp2) استخدام الجدار الناري المدمج مع نظام التشغيل لحماية أجهزتهم الشخصية.

خامساً: المداومة على تحديث نظام التشغيل والمتصفح

تنشر الشركات المنتجة لنظم التشغيل ومتصفحات الإنترنت والبرامج الأخرى تحديثات أمنية لسد ثغرات برامجها بصورة دورية، وتحمي التحديثات المستخدم من التهديدات الجديدة على الإنترنت؛ حيث غالباً ما يستغل المخترقون هذه الثغرات للهجوم على الأجهزة الشخصية أو إنتاج فيروسات تستغل هذه الثغرات.

يمكن تحديث نظام ويندوز بزيارة هذا الموقع (www.windowsupdate.com) شهرياً، وتنشر شركة مايكروسوفت التحديثات بصفة شهرية لكل من نظام ويندوز ومتصفح إنترنت إكسبلورر وبرامج مايكروسوفت الأخرى. أما أنظمة التشغيل الأخرى مثل لينكس فيمكن استخدام برنامج التحديث التابع للشركة الموزعة للنسخة مثل ردهات أو سوزي. وفيما يخص البرامج الأخرى فغالباً ما يتم تخصيص خيار في قوائم البرنامج لتحميل التحديثات.

سادساً: تصفح الإنترنت بوعي ومسؤولية

إن سلوك ونوعية المواقع التي يتم تصفحها لها تأثير مباشر على أمن الجهاز الشخصي، لذا يجب على المستخدم اتباع التالي:

- عدم إعطاء معلومات المستخدم الهامة أو رقم حسابه البنكي أو بطاقته الائتمانية إلا لمواقع موثوقة من خلال قناة مشفرة باستخدام بروتوكول (https)، لأن بروتوكول التشفير يعتمد على شهادة إلكترونية تصدر من جهة مستقلة تتحقق من هوية المصدر قبل إصدارها، وتتنقل البيانات داخل قناة مشفرة بحيث لا يستطيع أحد سرقتها أو الاطلاع عليها أثناء انتقالها، وللتعرف على نوعية البروتوكول يمكن للمستخدم الاطلاع على حقل العنوان في المتصفح للتأكد من أنه يبدأ بالحروف (https) أو النظر في إحدى الزوايا السفلية والتأكد من وجود علامة قفل ظاهرة في إكسبلورر النسخة السادسة (في النسخة السابعة وما بعدها تكون علامة القفل بجانب حقل العنوان).
- عدم زيارة المواقع المشبوهة أو المواقع التابعة للمخترقين أو المواقع الإباحية، وغالباً ما تحاول هذه المواقع استغلال وجود ثغرات في متصفح الإنترنت أو جهاز المستخدم لتقوم بتركيب برامج تخريبية في جهاز المستخدم.

- عدم تحميل وتركيب برامج مجانية من مواقع غير موثوقة أو مواقع النسخ غير المرخصة لأن الكثير من هذه المواقع تدار من قبل مخترقين وتحتوي على برامج تخريبية.
- ضبط إعدادات الأمن في متصفح الإنترنت على مستوى متوسط على الأقل.

سابعاً: احتفظ بنسخة احتياطية

إن المعلومات عرضة للفقدان والضياع لأسباب عديدة مثل حدوث الحرائق أو الأعطال الفنية التي قد تصيب القرص الصلب للجهاز الشخصي، لذا يوصي خبراء أمن المعلومات بالاحتفاظ بنسخة محدثة من المعلومات الهامة على قرص ليزر أو دي في دي أو أي وسائط حفظ معلومات لتجنب خسارتها للأبد.

ومما ينبغى ملاحظته عدم حفظ النسخة الاحتياطية في نفس مكان جهاز الكمبيوتر تجنباً لحدوث خسارة مزدوجة، أيضاً يجب الحفاظ على النسخة الاحتياطية في مكان آمن بعيداً عن أعين الآخرين، ووضع معلومات توضح تاريخ النسخة الاحتياطية ونوع المعلومات المخزنة فيها، ويجب على المستخدم التأكد من مناسبة الحرارة والرطوبة لمواصفات الأقراص المستخدمة.

ثامناً: لا تقع ضحية للمواقع والرسائل الاحتيالية (Phishing)

تعتبر هذه الرسائل والمواقع الاحتيالية من أكثر الأساليب التي يتبعها المخترقون في هذه الأيام، وتعتمد على إرسال بريد إلكتروني أو تصميم موقع إنترنت لخداع المستخدمين وإيهامهم للدخول إلى موقع مشابه للموقع الأصلي الذي يتعاملون معه من أجل سرقة معلومات هامة مثل كلمات السر أو بطاقات الائتمان.

ومما ينبغى التنبه له أن عنوان الموقع المزيف مخالف لعنوان الموقع الأصلي بالإضافة إلى أنه في الغالب لا يستخدم بروتوكول التشفير (https)؛ لأن بروتوكول التشفير يعتمد على شهادة إلكترونية تصدر من جهة مستقلة تتحقق من هوية الموقع قبل إصدارها.

إن أفضل طريقة للتعامل مع أساليب الخداع هو تجاهل الروابط المرفقة مع الرسالة، والقيام بزيارة الموقع الأصلي الذي سبق التعامل معه أو الاتصال بالموقع للتأكد من صحة الرسالة، وحالياً تحتوي بعض متصفحات الإنترنت على خاصية مضادة لهذه الأساليب (Phishing Filters) ينبغي للمستخدم تفعيلها.

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