الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

دليل الاستخدام الآمن لشبكة الإنترنت

أولاً: التوصيات العامة:

- استخدام كلمات سر قوية سهلة التذكّر وصعبة التخمين.
- إلغاء تفعيل خاصية تذكّر اسم المستخدم وكلمة السر، والحذر بشكل كبير عند استخدام حواسيب الغير.
- إلغاء تفعيل خاصية الإكمال التلقائي للاسم وفراغات النماذج في متصفح الانترنت.
- إلغاء تفعيل خاصية تذكّر الصفحات التي تمت زيارتها لفترات طويلة وتقليل هذه المدة ما أمكن.
- التأكد من ضبط الإعدادات الآمنة لمتصفح الإنترنت إلى الوضع المتوسط أو الأعلى للحد من النوافذ الإعلانية المنبثقة وتأثير الكعك Cookies.
- إغلاق المتصفح عند الابتعاد عن الحاسوب لتعطيل خاصية الرجوع للخلف في المتصفح.
- إلغاء تفعيل التشغيل المباشر لكلٍ من Active X و JavaScript و Java Applets في متصفح الانترنت.
- تحديث نسخة متصفح الانترنت وبرنامج تصفح البريد الإلكتروني بشكل دوري من موقع الشركة الأم حصراً.
- الحذر من انتحال شخصية المواقع من خلال التأكد الحرفي من اسم الموقع المطلوب.
- الحذر من استخدام الحواسب في الأماكن العامة وخاصة عند إجراء التعاملات المالية أو إرسال المعلومات الشخصية.
- تجنب إرسال أية معلومات تتعلق بالبيانات المالية بواسطة البريد الالكتروني.

ثانياً: الاختيار الأمثل لكلمات المرور:

- تجنب تضمين اسم المستخدم داخل كلمة المرور.
- تجنب استخدام كلمات المرور التي يصعب تذكرها أو كلمات المرور التي من السهل تخمينها (مثل الاسم، الكنية، تاريخ الميلاد،..)، وتجنب استخدام كلمات المعجم.

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

- ينبغي أن تكون كلمة المرور طويلة (أكثر من 10 محارف).
- ينبغي أن لا تكون كلمة المرور من كلمة واحدة مثل: .. ,Syria, Ali.
- استخدام مزيج عشوائي من الحروف والأرقام والرموز وأن تتضمن رموزاً خاصة كـ $ # @ كي يصعب تخمينها. حيث يمكن أن يعتمد كل شخص مصطلحات خاصة به لكلمة المرور؛ مثلاً يمكن اعتماد المحرف @ بدلاً من الحرف a ، والحرف o بدلاً من الرقم 0، والمحرف ! بدلاً من الرقم 1. فعلى سبيل المثال بدلاً من أن نكتب كلمة المرور على الشكل (samer1990) والتي تُعتبر كلمة مرور ضعيفة، يمكن كتابتها بالصيغة ($@m3r!99o) والتي هي عبارة عن كلمة مرور قوية ويسهل تذكرها.
- تجنب استخدام نفس كلمة المرور في جميع الحسابات الخاصة بالمستخدم.
- تجنب كتابة كلمة مرور لاتينية باستخدام المفاتيح العربية أو العكس.
- تجنب إفشاء كلمة المرور، وعدم كتابتها على أوراق خارجية.
- تجنب إرسال كلمات المرور عبر البريد الإلكتروني أو برامج المحادثة الفورية.
- تجنب تخزين كلمة المرور على الحاسوب بشكل ملف نصي، واستخدام برمجيات موثوقة وآمنة لتخزين كلمة المرور بشكل مشفر.

ثالثاً: الاستخدام الآمن للبريد الإلكتروني:

- تجنب استخدام كلمة المرور الخاصة بالبريد الإلكتروني عند التسجيل بالمواقع والمنتديات على شبكة الإنترنت.
- تفعيل خاصية مسح الرسائل الواردة والصادرة الحاوية على فيروس تلقائياً في البرنامج المضاد للفيروسات.
- عند تسجيل بريد إلكتروني جديد لدى إحدى الشركات العالمية التي تقدم خدمة البريد الإلكتروني كالـ Yahooو Hotmail و Google وغيرها، يفضل إدخال معلومات وهمية بحيث لا يتوقعها المخترق، وخاصةً جواب السؤال السري.
- عند الانتهاء من قراءة الرسائل يجب الخروج Sign Out من موقع أو برنامج تصفح البريد الإلكتروني، لأن معظم برامج البريد أو المواقع تتذكر الزائر لمدة تصل إلى 8 ساعات.
- تجنب فتح أي ملف مرفق مع رسالة إلكترونية مُرسلة من مرسل مجهول، حتى وإن كان المرفق موقعاً رقمياً أو ظهر على شكل ملف نصي أو صورة لا تحمل فيروساً لأنه يمكن التلاعب باسم الملف ليظهر الملف التنفيذي الذي يحمل فيروساً بمظهر سليم يحمل صورة أو نصاً يتضمن بداخله ملفاً تنفيذياً، على سبيل المثال .picture.jpg.exe .
- تجنب فتح أي ملف مرفق مع رسالة إلكترونية مُرسلة من مرسل معروف، إلا إذا كنت تتوقع استقبال

ذلك الملف. وفي حال الشك بسلامة الملف المرسل يمكن التحقق من المرسل بأي طريقة اتصال مُتاحة، لوجود احتمال بأن يكون الإرسال قد تم بواسطة نوع من الفيروسات يقوم بإرسال رسائل عشوائية تحوي ملفات مؤذية إلى القائمة البريدية للمرسل الفعلي.

- التأكد من امتداد الملف المرفق مع الرسالة قبل تشغيله على الحاسوب. مع التنويه إلى أن امتدادات البرمجيات المؤذية غالباً ما تكون على شكل ملف تنفيذي واضح مثل (.dll , .exe)
- إلغاء تفعيل خاصية تحميل الملفات المرفقة مع الرسالة في برنامج تصفح البريد الالكتروني.
- فحص الملف المرفق المراد تحميله على الحاسوب باستخدام برنامج مضاد للفيروسات للتأكد من خلوه من برمجيات مؤذية.
- تجنب التحديثات الوهمية المرسلة عبر البريد الإلكتروني والتي يزعم مرسلوها أنها مرسلة من الشركة الأم.
- تفعيل خاصية فلترة الرسائل غير المرغوب بها في برنامج تصفح البريد الالكتروني.
- تفعيل خاصية استقبال الرسائل الإلكترونية من أشخاص غير موثوقين ضمن مجلد البريد غير المرغوب به في برنامج تصفح البريد الإلكتروني.
- تجنب الرد على الرسائل الإلكترونية التي تطلب معلومات شخصية لأغراض مختلفة.
- تجنب كتابة العنوان البريدي الشخصي في مواقع الانترنت غير الموثوقة.
- حذف أية رسائل غير مرغوب بها فور وصولها أو عند اكتشافها.

رابعاً: الاستخدام الآمن لتطبيقات شبكة الانترنت:

- مراجعة سياسات الخصوصية في مواقع الشبكات الاجتماعية المراد استخدامها، ويُفضل الاشتراك بالمواقع التي تراعي حجب ومنع بيانات المشترك الشخصية من الظهور للجميع إلا لأشخاص يقوم المشترك نفسه بالسماح لهم بمشاركته هذه البيانات.
- تجنب إرسال أو ذكر أيّة معلومات شخصية أو مالية عبر مواقع الإنترنت (مثل أرقام البطاقات المصرفية أو رقم الهاتف الشخصي، ..) أو أية معلومات تدل على تفاصيل بيئة العمل كالعنوان ونوع العمل أو اسم الشركة وما إلى ذلك.
- تجنب وضع أية صور شخصية أو عائلية كي لا يتم استغلالها لأغراض سيئة من قبل الآخرين.
- تجنب كتابة أية بيانات قد تساعد المتلصصين على اكتشاف كلمة المرور المستخدمة في هذه المواقع.
- الحذر عند قبول طلبات الإضافة من قبل أشخاص غير معروفين ومحاولة الاتصال بهم للتأكد من هوياتهم (عن طريق البريد الالكتروني مثلاً) قبل قبول طلباتهم.
- التأكد من اعتمادية الموقع الذي يتعامل بالدفع الالكتروني ومن الوجود الفعلي للمتجر أو الشركة عن

طريق التقصي والبحث أو عن طريق الاتصال الهاتفي المباشر بالمعلن.

- التأكد من استخدام البروتوكول الآمن (Https) لموقع الدفع الإلكتروني.
- استخدام البطاقات ذات الرصيد المنخفض نسبياً في التعاملات الالكترونية.
- تجنب التعاملات المالية عبر الشبكات أو الحواسيب الموجودة في الأماكن العامة.

خامساً: الحفاظ على البيانات الشخصية:

- إجراء نسخ احتياطي للملفات المهمة بشكل دوري.
- التأكد من قفل Lock الحاسوب أثناء مغادرة المستخدم ولو لفترة وجيزة.
- التأكد من خلو الحاسوب من أيّة ملفات هامة أو سرية أثناء العمل على شبكة الانترنت.
- التأكد من إزالة جميع الملفات الشخصية والهامة قبل تسليم الحاسوب إلى جهة ما (مستودع التجهيزات، ورشة الصيانة،..) باستخدام برامج إزالة الملفات بشكل آمن، لمنع إمكانية استرجاع أي ملف باستخدام برامج الاسترجاع المنتشرة بكثرة.
- مسح الملفات المحفوظة ضمن مجلد التآريخ History للمتصفح.
- تنظيف الذاكرة الخبيئة Cash بشكل دوري.
- التخلص من ملفات الكعكة Cookies فور الانتهاء من تصفح الانترنت.
- استخدام برامج التشفير المحمية بكلمات مرور لحماية الملفات الشخصية على الحاسوب، ولحماية البيانات المتداولة عبر البريد الإلكتروني. ومن برامج التشفير المجانية مفتوحة المصدر (PGP – Pretty Good Privacy).
- تجنب تسجيل الدخول (Log in) إلى محرك البحث الذي تريد استخدامه؛ حيث أن الدخول بهذه الطريقة يسهّل على محركات البحث تتبع المعلومات الجاري تصفحها على الشبكة، والمواقع التي تتم زيارتها من خلال قيام هذه المحركات بإنشاء ملف خاص بالمستخدم.

سادساً: الوقاية من الملفات المؤذية وملفات التجسس:

- استخدام برامج مضادة للفيروسات مرخصة، وتجنب استخدام البرامج المزيفة غير النظامية.
- تشغيل البرنامج المضاد للفيروسات بشكل صحيح على الحاسوب دون أي رسائل تحذيرية.
- تحديث البرنامج المضاد للفيروسات وقاعدة المعطيات الخاصة به دورياً.
- تفعيل خاصية المراقبة الآنية للفيروسات حال اكتشافها في الحاسوب.
- تفعيل خاصية مراقبة الرسائل البريدية فور تحميلها من المخدّم .
- تفعيل وظيفة الفحص الدوري لملفات بدء التشغيل، وملفات الذاكرة الخبيئة للنظام.
- تفعيل وظيفة الفحص الفوري لأي واسطة تخزين خارجية يتم توصيلها إلى الحاسوب.

- استخدام برامج خاصة مضادة للملفات المؤذية (ديدان، تروجان،..) لكون بعض البرامج المضادة للفيروسات لا تتعرف على مثل هذا النوع من الملفات المؤذية، والتأكد من عدم وجود تعارض بين البرنامج المضاد الفيروسات وبرنامج إزالة الملفات المؤذية.
- تنصيب البرامج الخدمية من أقراص ليزرية آمنة، وإن كان ولا بد من تنصيبها من شبكة الانترنت، ينبغي تنصيبها موقع موثوق.
- تغيير كلمات المرور المستخدمة والمخزنة في الحاسوب فور اكتشاف أي ملف مؤذي فيه.
- تجنب الضغط على أية روابط داخل النوافذ المنبثقة، أو المواقع التي يتم التوجيه الآلي إليها.
- تجنب الدخول إلى المواقع الإلكترونية الدعائية التي تدّعي تقديم خدمة الفحص المجاني للحاسوب من الملفات المؤذية.
- استخدام برامج تعمل كجدار ناري Firewall.
- إغلاق المنافذ التي تستخدمها البرامج المؤذية المشهورة، باستخدام برامج مسح للمنافذ المفتوحة في الحاسوب.

دمشق في ٢٠١٢/٤/١٢