

## البرامج الخبيثة وأخطارها

استكمالاً للنشرة رقم (4) عن البرمجيات الخبيثة وأساليب انتشارها، نضع بين أيديكم هذه النشرة التي تبين المظاهر العامة لوجود هذه البرمجيات على أجهزة الحاسوب والآليات التي يمكن اتباعها للتخلص من هذه البرامج.

### أعراض البرمجيات الخبيثة

- الأداء السيء للحاسوب (أكثر من المعدل الطبيعي المتوقع) خاصة عند الاتصال بالانترنت.
- توقف الحاسوب عن الاستجابة بشكل متكرر بعد فترة كافية من العمل بدون مشاكل.
- يستغرق الحاسوب فترة أطول أثناء بدء التشغيل.
- الإغلاق الفجائي للمتصفح أو توقفه عن الاستجابة.
- نتائج البحث من موقع معين تقود إلى صفحات على مواقع غير الظاهرة في نتائج البحث
- تحويل نتائج البحث في الانترنت إلى مواقع أخرى.
- الضغط على روابط معينة قد لا يستجيب أو قد يتم التحويل إلى مواقع ليست ذات علاقة.
- تغيير الصفحة الرئيسية للمتصفح، وقد لا يكون من الممكن إعادة ضبطها.
- إعلانات منبثقة متكررة أثناء تصفح مواقع لا تحتويها عادةً أو عند عدم تشغيل المتصفح أصلاً.
- وجود أشرطة أدوات إضافية في متصفح الانترنت.
- إضافة بعض المواقع إلى المفضلة بدون تدخل المستخدم.

- إضافة بعض الأيقونات الدعائية لسطح المكتب بدون تدخل المستخدم.
- تشغيل المتصفح بشكل آلي وعرض إعلانات لبعض المواقع.
- عند فتح المتصفح لعرض بعض المواقع، يتم تشغيل صفحات أخرى إعلانية.
- لا يمكن تشغيل بعض البرامج، خاصةً برامج الحماية.
- بعض مكونات نظام التشغيل أو برامجه تتوقف عن العمل.

### منع البرامج الخبيثة والحد منها

- استخدام نظام حماية من الفيروسات و البرامج الخبيثة الأخرى مع ضرورة التحديث المستمر.
- تغيير إعدادات الأمان في المتصفح إلى مستوى مرتفع من الحماية.
- حظر أو تقليل الإعلانات المنبثقة (Pop-up Ads) أثناء التصفح.
- تحديث نظام التشغيل و المتصفح و تطبيق التحديثات الأمنية بانتظام.
- استخدام برامج فحص الأمان للمواقع مثل McAfee Site Advisor
- الحذر أثناء تصفح الانترنت و معرفة البرامج التي يتم تثبيتها.

في الخلاصة فإن أفضل حماية ممكنة هي عبارة عن الدمج بين استخدام برنامج قوي للحماية من الفيروسات لا باضافة إلى تغيير إعدادات الأمان في المتصفح و أيضاً الحرص و الحذر أثناء الاستخدام. حيث لا يوجد حتى اللحظة برنامج حماية يستطيع كشف كل البرامج الخبيثة و ذلك بسبب أعدادها الكبيرة و التي تزيد بشكل مهول كل يوم، و لكن عند استخدام الانترنت بطريقة حذرة و حريصة فإن امكانية التثبيت الغير متعمد للبرامج الخبيثة تقل كثيراً.

## إزالة البرامج الخبيثة:

عند ملاحظة وجود أي مظاهر على الحاسوب و أداءه من تلك المذكورة أعلاه، يمكن اتباع

التعليمات التالية:

- لا تحاول إزالة هذه البرامج بشكل شخصي، بل يمكن الاتصال أولاً على مكتب الدعم الفني و الذين يمكنهم تأكيد أو نفي وجود برامج خبيثة و عند وجودها يمكنهم طلب احضار جهاز الحاسوب لتتم صيانتة، هذه العملية ضرورية حتى يتم الحفاظ على الملفات و البيانات الموجودة على الحاسوب. و في أسوأ الظروف عندما يكون الخلل الناتج عن البرامج الخبيثة كبيراً و لا يمكن ازالته بالطرق التقليدية، فعندها يجب إعادة تهيئة الحاسوب و تركيب نظام التشغيل من جديد عليه و إذا لم يتم الحفاظ على البيانات في أقراص منفصلة أو في نسخ احتياطية على أقراص تخزين خارجية، فعندها قد يتم فقدان كافة البيانات الموجودة على الحاسوب.
- قد تكون إزالة البرامج الخبيثة مهمة صعبة جداً، و حتى عند إزالة البرامج الخبيثة عن طريق إضافة و إزالة البرامج، فإن أجزاء من هذه البرمجيات غالباً ما تظل كامنة في النظام و تسبب تدهوراً في أداء النظام.
- لا يتم حالياً تقديم الدعم لبرامج إزالة البرمجيات الخبيثة بشكل آلي، و أي استعمال لهذه البرامج يتم ضمن مسؤولية المستخدم نفسه، و لهذا فيجب الحرص على انشاء نسخة احتياطية من الملفات و البيانات الهامة على أقراص CD أو DVD أو Flash قبل تشغيل أي من هذه البرامج.
- يوجد بعض البرمجيات التي تم تصميمها لفحص أجزاء معينة في النظام مثل سجل النظام وملفات البرامج:

- Windows Defender
- IOBit Security 360
- Webroot Spysweeper
- ESET Smart Security
- Norton Internet Security 2010
- Kaspersky Internet Security

عند العزم على استخدام أي من هذه البرامج، يجب التأكد أولاً من الحصول على أحدث نسخة من البرنامج، كما يجب تحديثها إن كانت قابلة للتحديث ومن ثم تجريب استخدام مجموعة من هذه البرامج وعدم الاقتصار على واحد فقط، كما يستحسن تكرار الفحص أكثر من مرة.

#### دائرة أمن المعلومات