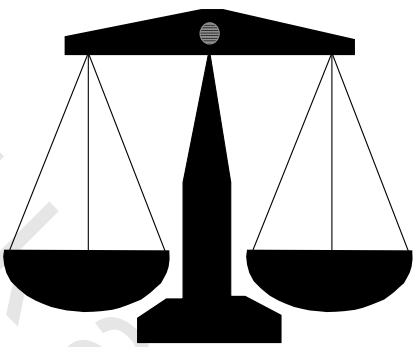

الفصل السابع

الحماية من الجرائم الرقمية وطرق مكافحتها

الحماية من الجرائم الرقمية

وطرق مكافحتها

س١٢١: ما هي وسائل الحماية من جرائم الإنترنت والكمبيوتر؟

ج : تتشعب وسائل الحماية من الجرائم الرقمية من الإنترنت والكمبيوتر فهي قد تتعلق بالأجهزة وقد تتعلق بالأشخاص وقد تتعلق بالدولة .

وتنقسم برامج الحماية إلى:

١ـ برامج حماية من الفيروسات .
٢ـ برامج جدر النار .
٣ـ برامج التشفير للبريد الإلكتروني .
٤ـ برامج تشفير للملفات .

س١٢٢: كيف يمكن حماية الخصوصية على الإنترنت؟

ج : بتجنب الأخطاء الشخصية في التعامل مع الكمبيوتر واتخاذ الوسائل الأمنية .

س١٢٣: كيف نحمي الأجهزة من الفيروسات ومكافحتها؟

ج : يمكن حماية الأجهزة من الفيروسات ومكافحتها عن طريق :

١ـ الالتزام بالنصائح الخاصة بتجنب الأخطاء الشخصية كترك ملفات مفتوحة أو فتح ملفات غير معروفة .
٢ـ الاطلاع على أحدث البرامج واستخدامها .
٣ـ الاطلاع على أنواع الفيروسات وطرق مكافحتها .
٤ـ تنزيل التعديلات الأمنية على الجهاز .
٥ـ عمل تحديث Update لمعالجة أوجه القصور .

٦ـ تنزيل البرامج التي تكافح الفيروسات على الجهاز .

س١٢٤: ما هي برامج مكافحة الفيروسات؟

ج : من برامج مكافحة الفيروسات ما يلي :

١ـ مواقع الإنترنت التي توفر خدمات فحص الكمبيوتر من الفيروسات أثناء الاتصال بالشبكة **Virus Scan Online** وهى مجانية على الشبكة .

٢ـ موقع شركة **Trend Micro** وموقع شركة **Symantec** والتي تقوم بفحص الكمبيوتر بالمجان عند الاتصال بالشبكة للبحث عن الفيروسات .

٣ـ من خلال موقع **www.symantec.com/securityche ck** يمكنه إجراء فحص أمنى أثناء الاتصال بالإنترنت لاكتشاف المخاطر الأمنية كما يمكنه البحث من عنوان الإنترنت **IP** لمعرفة مصدر الرسالة الرقمية وتتبع الهجوم .

٤ـ تقوم خدمة **Virus Check** من برنامج **Virus Scan** وباستخدام الأداة **Active x** بفحص الملفات وذاكرة الجهاز للتأكد من خلوه من الفيروسات .

س١٢٥: لمكافحة الاختراق كيف يمكن التعرف على وجود برنامج تشغيلي مساعد للاختراق بالجهاز؟

ج : يمكن الكشف على ذلك عن طريق اتباع الآتي :

١ـ عن طريق زر **Start** يتم اختيار أمر التشغيل **Run**

٢ـ كتابة **Masconfig** والنقر على **O.k.** . ٣ـ اختيار **startup** من التبويب .

٤ـ اختر **Check** من ملف التعقيب **Patch exe** وإزالة العلامة لتعطيل تشغيله إن كان موجوداً .

٥ـ إزالة العلامات أمام الملفات التي تعمل من خلال مجلد الملفات المستقبلة

Received Files نتيجة عمل برامج الدردشة أو في مناطق ملفات الإنترنت المؤقتة Internet Temperary Files .

س١٢٦: كيف يمكن التعرف على اختراق حماية الجهاز؟

ج : يمكن التعرف على أن الجهاز مخترق من قبل آخرين من الدلائل الآتية :

١ـ ظهور صور مفاجئة على الشاشة أو حدوث تغير إعداد الشاشة .

٢ـ فتح وغلق باب مشغل القرص المضغوط CD Rom دون تدخل المستخدم .

٣ـ توقف حركة أو تغير شكل مؤشر الفأرة أو الحركة العشوائية له .

٤ـ عرض رسائل أو نوافذ على الشاشة تختفي فجأة أو إغلاق نوافذ مفتوحة .

٥ـ حركة القرص الصلب لتحميل ملفات أو حذف ملفات .

س١٢٧: كيف يتم حماية النظام من الاختراق؟

ج : يتم حماية النظام من الاختراق عن طريق :

١ـ تحديث البرامج المضادة لفيروسات .

٢ـ منع استقبال الملفات أو البرامج أو الصور من أشخاص غير موثوق بهم .

٣ـ عدم فتح ملفات منقولة إلا بعد الاتصال وبعد فتحها يتم البحث عن الفيروسات .

٤ـ الحرص في نقل ملفات مرفقات البريد .

٥ـ استخدام كلمات سر قوية طويلة متغيرة .

٦ـ عدم تحميل برامج من موقع غير معروف أو موثوق به .

٧ـ عدم جعل الجهاز المتصل بالشبكة على وضع مشاركة .

س١٢٨: كيف يمكن الوقاية من تزوير المستندات؟

ج : الحماية من الاختراق بعمل تحديث، واتخاذ الاحتياطات السالف ذكرها، واستخدام برامج جدر النار، وعدم استقبال أو فتح ملفات غير موثوق فيها .

س١٢٩: كيف يمكن حماية الجهاز من أحصنة طروادة؟

ج : يمكن الحماية من أحصنة طروادة باتباع ما يلي .

١ـ استخدام مضادات حديثة للفيروسات .

٢ـ استخدام برامج جُدر النار .

٣ـ عدم تحميل البرامج المجانية مجهولة المصدر .

٤ـ عدم فتح الرسائل المجانية الغير معروفة المصدر خاصة الملفات المرفقة **Attached Files**

٥ـ تعديل مستوى أمن المتصفح بحيث لا يتم تنزيل أو قبول برامج .

٦ـ قبول البرامج التي تحمل توثيقاً إلكترونيًا .

س١٣٠: كيف يمكن حماية الرسائل الإلكترونية؟

ج : بإرسال رسائل مشفرة وموقعة إلكترونيا ويتم تبعاً للخطوات التالية :

١ـ يتم إعداد رسالة بريد إلكتروني جديد واختيار الأمر **Digitally Signature** من قائمة الـ **Tools** ليتم توقيع الرسالة رقمياً وإضافة المُعرِّف الرقمي الخاص إليها ويظهر رمز التوقيع الرقمي مقابل عنوان الرسالة .

٢ـ يتم تشفير الرسالة باختيار الأمر **Encrypt** من قائمة الـ **Tools** ويتطلب هذا أن يكون لدينا المعرف الرقمي للشخص الذي ترسل إليه الرسالة فيظهر رمز التشفير مقابل عنوان المرسل إليه .

٣ـ نقر **Send** يظهر صندوق حوار وعاء المفتاح المحدد والمستوى أمام الرسالة .

٤ـ نقر زر **O.K.** يظهر صندوق حوار تحديد مستوى الأمان .

٥ـ يتم تحديد مستوى الأمان المطلوب ثم النقر على **Next** .

٦ـ النقر على **Finish** لإرسال الرسالة .

هذا ويلاحظ أنه يجب استخدام نفس عنوان البريد الإلكتروني للرسائل الموقعة رقمياً لتلقى الردود عليه .

س١٣١: ما هي طرق الوقاية من الهجمات الخداعية؟

ج : للوقاية من الهجمات الخداعية كخداع ويب **Web Spoofing** والذي يسمح للمخترق بإنشاء نسخة مزيفة من شبكة ويب يتصل بها المستخدم عبر كمبيوتر المهاجم فيجب عمل الآتي :

١ـ العمل على تعطيل عناصر **Java Script** وتحكمات **Active x** في المتصفح أو عمل اختيار لإمكان قبولها من عدمه .

٢ـ التأكد من بيانات ومحتويات سطر عنوان المتصفح ومراقبة تغيير العنوان .

٣ـ مراجعة سطر الحالة أثناء التجوال ومراقبة محتوياته عند وضع مؤشر الفأرة فوق وصلته .

٤ـ ملاحظة المؤشرات المتطورة في صفحات الوصلات الآمنة لإدراك وقوع الهجمات .

س١٣٢: كيف يتم حماية المواقع التي تم زيارتها؟

ج : يتم حماية المواقع التي تم زيارتها عن طريق المتصفحات التي تقوم بحفظ صفحاتها ومحتوياتها على القرص الصلب **Hard Disk** وتقوم برامج التصفح بتخزين عناوين المواقع التي سبق زيارتها في شريط يعرف بشريط العناوين **Address Bar** أو تاريخ الزيارة .

س١٣٣: كيف يتم الكشف عن المواقع التي تم زيارتها والتي حُفظت؟

ج : عن طريق تنشيط الخاصية **Auto Complete** في برنامج التصفح فيتم استكمال كتابة عناوين المواقع التي تم زيارتها من قبل بمجرد كتابة حرف منها .

س١٣٤: بصفة عامة كيف يمكن حماية مواقع ويب؟

ج : يتم حماية مواقع ويب إما عن طريق الحماية الداخلية أو الحماية الخارجية كالآتي :

أـ الحماية الداخلية : وتتمثل في حماية الخدمة والأنظمة من إفشاء الأسرار بواسطة الأشخاص المؤتمنين عليها وذلك عن طريق مراقبتهم بعناية وعدم إعلام الواحد منهم بما يفعله الآخر .

ومن ضمن هذه الحماية فحص ملفات العاملين لمعرفة الشركات التي سبق أن عملوا بها كما يجب تدريبهم وتعريفهم بأهمية المعلومة .

هذا وتتضمن الحماية الداخلية تغيير نظام الحماية من وقت لآخر .

ب ـ أما الحماية الخارجية : فتكون لمنع تخريب الجهاز واختراق النظام والديدان التي يمكن أن تحدث بدون حماية .

هذا ورغم أن المواقع يقال إنها محمية إلا أن كل موقع هو شباك مفتوح أو شبه مغلق ، ويتم اختراقها لتنامي الفكر وتنامي الثقافة مع وجود العبقرية والرغبات الداخلية لدى المهاجمين في التحدي .

س١٣٥: لماذا يتم حماية المعلومات؟

ج : للوقاية من التشويه الناتج عن مشاكل الأجهزة وللحماية من السرقة .

س١٣٦: كيف يتم الوقاية بصفة عامة من الجريمة الرقمية؟

ج : عن طريق التشفير **Encryption** بتحويل المعلومات إلى رموز بحيث تصبح محمية من عمليات الوصول إليها من غير المرخص لهم وتمكن من الاتصال بأمان .

وعن طريق جدر النار المعروفة باسم Fire Walls للتحكم في منع الوصول إلى الأنظمة الحساسة ولحماية خدمات مواقع ويب وتعمل كإدارة مركزية للأمن وتتحكم في النقاط التي تتصل بها الشبكة .

س١٣٧: كيف يمكن مكافحة الجرائم الرقمية شعبياً؟

ج : الجريمة الرقمية عبارة عن سباق بين الفكر اليقظ والتسلح بالمعلومة وبين قلة الحيلة وقلة المعلومة ، فهي تنشأ بين شخص أو أشخاص لديهم معلومات وآخرين غير متوفر لديهم المعلومات ، أشخاص أصحاب حيل وابتكارات وأشخاص ليسوا فطنين لما يحدث ، لذا فإن الاعتماد على تنمية الوعي الشعبي وتثقيف الجمهور له دور للوقاية من هذه الجرائم .

وتوعية الجمهور تكون من خلال البرامج الإعلامية التي توضح الطرق الصحيحة للتعامل مع الشبكات ووسائل الاتصالات ، والتحذير من مواقع معينة وخاصة مواقع الدردشة للشباب والتي هي عبارة عن مصائد للسرقة ، والحث على البعد عن كل ما ينافي الخلق الكريم .

كما يمكن توعية الطلاب بالمواقع الآمنة والتعريف بها .

وتشمل التوعية الشعبية توعية الأسر بتتبع أولادهم والمواقع التي يقومون بزيارتها ، وحثهم على الفضيلة ، والاستفادة من شبكة الإنترنت بما يعود بالفائدة لهم ولوطنهم ، كما يجب على الآباء معرفة أصدقاء أولادهم (البنات والبنين) .

هذا وقد أنشئت جمعيات لمكافحة قرصنة الإنترنت وهى جمعيات أهلية تعمل على حماية سرقة أرقام بطاقات الائتمان Credit Cards .

س١٣٨: كيف يتم مكافحة الجرائم الرقمية فنياً؟

ج : عن طريق تشفير مواقع بعينها وعن طريق المراقبة الدائمة واستخدام أحدث الوسائل في الكشف عنها وزيادة درجات التخصص ومستواه .

س١٣٩: كيف يمكن مكافحة الجرائم الرقمية قانونياً؟

ج: عن طريق دراسة واسعة للجرائم وخطورتها ومدى تأثيرها في المجتمع وعلى الأفراد وعلى الدولة، ووضع التشريع الرادع لمن تثبت عليه التهمة وأن تصل العقوبة إلى المؤبد.

س١٤٠: ما هي طرق الوقاية الآمنة للشبكات؟

ج: تطوير الشركات لبرامجها لمنع الاختراق بوسائل أمنية تصاحب البرامج وسد الفجوات في المواقع التي تحدثها برامج الشركات المصنعة للبرامج نفسها.