جرائم الحاسوب والانترنت

الاستخدام المتزايد للحاسبات والانترنت حقق أهدافا كثيرة لجميع المستخدمين وزاد من كفاءة الأعمال، إلا أن هناك مخاوف مستمرة من مخاطر الجرائم المختلفة المتعلقة بسرقة المعلومات والاحتيال وتدمير البيانات والإطلاع على خصوصيات الأفراد والمؤسسات والحكومات.

في هذا الفصل سنتعرف على مفاهيم متعلقة بجرائم الحاسوب المختلفة ثم سنتطرق إلى المفاهيم المتعلقة بأمن وحماية وخصوصية البيانات، وفيروسات الحاسوب المختلفة، وسنذكر الطرق المختلفة اللازمة للحذر والوقاية من هذه الأخطار التي لها آثار سلبية كبيرة ليست على الأفراد والمؤسسات فقط بل على المجتمع بشكل عام وسنلقي الضوء في هذا الفصل أيضا على القواعد الأخلاقية العامة للتعامل مع الحاسبات.

إن الاستخدام المتزايد مؤخرا للحاسبات والانترنت ساهم في ظهور الجرائم الناشئة في بيئة الحاسبات وبيئة الشبكات.

١. الاحتيال بالوصول إلى البيانات.
٢. الاحتيال باستخدام بطاقات الائتمان.
٣. نسخ البرامج.

الدوافع لارتكاب مختلف جرائم المعلوماتية فهي عديدة منها:

١. الرغبة في التفوق وتحدي التقنية المتطورة.
٢. السعي إلى تحقيق مكاسب مالية والابتزاز.
٣. دوافع سياسية وفكرية.
٤. القيام بأعمال غير مشروعة
٥. الأحقاد والدوافع الثأرية والانتقام من أرباب العمل.

الهاكر Hacker

عرفت كلمة هاكر (بارع) في البداية إلى مستخدم الحاسوب المتحمس للمعرفة، إلا إن هذا المصطلح عادة ما يصف في وقتنا الحالي شخصا يتصل بنظام الحاسوب بطريقة غير قانونية بهدف إحداث خلل في هذا النظام.

فيروس الحاسوب Computer Virus

تعريف فيروس الحاسوب: الفيروس هو برنامج مكتوب بإحدى لغات البرمجة بواسطة أحد المخربين بهدف إحداث الضرر بنظام الحاسوب. ويمثل فيروس الحاسوب نوعاً من أنواع جرائم التعدي على نظم الحاسبات.

ومن خصائص الفيروس القدرة الكبيرة على اختراق الملفات والانتشار والاختفاء بينها ثم التدمير هذه الملفات وتعطيل عملها.

تصنيف الفيروسات

يمكن تصنيف فيروسات الحاسوب إلى:

١. الديدان Worm

ينتقل برنامج فيروس الديدان من حاسوب إلى آخر عبر الشبكة، ويكون في صورة ملف مستقل على القرص يقوم بإعطاء أوامر خاطئة أو مضللة للحاسوب، ويحتل حيزاً كبيراً من الذاكرة.

٢. أحصنة طروادة Trojan Horses

ينتقل عبر البريد الإلكتروني e-mail عادة، وهو برنامج يجذب المستخدم باسمه أو بشكله وعند تشغيله يخترق جهاز الحاسوب وينطلق في تدمير البيانات والتحكم في الجهاز.

٣. القنابل الموقوتة Time Bombs

يستخدم هذا الفيروس من قبل شركات البرمجيات التي توزع نسخاً مجانية من برامجها على أمل شراء النسخة الأصلية لاحقاً، فيتم إلحاق برنامج الفيروس إلى نسخة البرنامج وينشط الفيروس في وقت محدد أو بعد تنفيذ البرنامج عدة مرات.

أسباب انتشار الفيروس:

١. تبادل أقراص التخزين دون معرفة مصدرها والتأكد من خلوها من الفيروسات.

٢. التوسع في استخدام الانترنت والبريد الالكتروني. دون التحصن الكافي ببرامج الحماية من الفيروسات.

٣. انتشار ظاهرة النسخ غير المشروع والقرصنة للبرمجيات.

٤. زيادة انتشار أشكال جديدة وذكية من الفيروسات يصعب اكتشافها بسرعة.

طرق انتشار الفيروس:

أ – انتشار الفيروس من خلال الانترنت:

١. تحميل ملف مصاب بالفيروس من حاسوب مصاب بالفيروس إلى الحاسوب الرئيسي للإنترنت – الخادم Server أو توزيع ملف بريد إلكتروني e-Mail مصاب بالفيروس.

٢. إصابة القرص الصلب للحاسوب الخادم بالفيروس.

٣. إصابة مستخدمي الإنترنت لهذا الحاسوب بالفيروس

ب – انتشار الفيروس من خلال تبادل الاقراص:

١. استخدام قرص مصاب بالفيروس في حاسوب سليم.

٢. إصابة القرص الصلب للحاسوب بالفيروس.

٣. اصابة أي قرص سليم عند استخدامه في الحاسوب المصاب.

ج – انتشار الفيروس من خلال الشبكة:

١. تحميل ملف مصاب بالفيروس إلى الحاسوب الرئيسي للشبكة – الخادم Server.

٢. ينتقل الفيروس إلى كل نقطة Node في الشبكة.

اكتشاف إصابة الأقراص بالفيروس:

يمكن اكتشاف إصابة الملفات بالفيروس عن طريق الخبرة والملاحظة الشخصية كامتلاء الذاكرة أو البطيء أو زيادة حجم الملفات أو فقدانها وعدم رؤيتها على القرص أو توقف الحاسوب عن العمل، كذلك يمكن اكتشاف الإصابة بصورة أدق باستخدام البرمجيات المتخصصة في البحث واكتشاف الفيروس.

١. نورتن Norton من موقع الانترنت http://www.norton.com

٢. كافي MacAffee من موقع الانترنت http://www.macaffee.com

التخلص والحماية من الفيروس:

استخدم البرامج المضادة للفيروسات وقم بتحديثها بشكل دائم من خلال مواقعها على الانترنت، فعادة ما تظهر الفيروسات في صور جديدة وللشركات المتخصصة في اكتشاف الفيروسات مثل McAfee مواقع على الانترنت يمكنك تحميل برامجها على جهازك.

أمن وحماية البيانات Data Security:

المخاطر التي تتعرض لها البيانات:

يعتبر أمن وحماية البيانات من المجالات الهامة في نظم الحاسبات. ويعرف أمن البيانات Data Security بأنه الإجراءات التي تتبناها المؤسسة للعمل على تأمين ملفات البيانات وحمايتها من:

أ – مخاطر الوصول غير المشروع Unauthorized Access

وتتضمن وصول أشخاص من خارج المؤسسة أو موظفين بها إلى ملفات البيانات والإطلاع عليها أو تعديلها بشكل غير قانوني.

ب – مخاطر الفقد أو التلف Lost/Corrupt Data

وهي المخاطر المتمثلة في تغيير محتويات الملفات أو حذفها أو إحداث خلل بها بحيث يمنع من الاطلاع عليها. وترجع هذه المخاطر إلى عدة أسباب منها الإهمال وسوء الاستخدام أو الأعطال المفاجئة في النظام أو إصابة الملفات بفيروس الحاسبات.

أنظمة أمن وحماية البيانات Data Security Systems :

تضع المؤسسات نظم أمن متعددة لحماية البيانات من الضرر المتعمد وغير المتعمد أو من دخول أي شخص غير مسموح له إلى نظام الحاسوب. وتتلخص طرق وضع أنظمة أمن وحماية للبيانات في الآتي:

١. إعطاء اسم تعريفي للمستخدم User ID.

٢. تحديد كلمة مرور (كلمة سر User Password).

٣. وضع أدلة تأكيدية User Authentications: يمكن أن تكون هذه الأدلة صوت أو بصمه أو رقم سري أو توقيع المستخدم أو بطاقة ذكية.

٤. تحديد صلاحيات المستخدمين.User Authorization

٥. استخدام برامج الكشف عن فيروس الحاسوب Computer Virus والعمل على تحديث هذه البرامج.

٦ – الاحتفاظ بوسائط تخزين البيانات من الأقراص والشرائط والميكروفيلم وغيرها في خزائن أمنية مخصصة لهذا الغرض وعمل نسخ احتياطية دورية للبيانات.

٧. عدم إهمال مخرجات الحاسوب الورقية وتعريضها للاطلاع من قبل غير المسموح لهم خاصة إذا كانت تحتوي معلومات مهمة.

٨. توظيف العاملين المشهود لهم بالأمانة والاستمرارية حيث إن التلاعب بالبيانات قد يكون من صائغي البرامج أو مشغلي الحاسبات.

٩. استخدام نظماً مختلفة للدخول إلى المواقع الخاصة بأنظمة المعلومات وذلك لضمان سرية العمل ومن هذه الأنظمة:

١. بصمات الأصابع أو كف اليد بالكامل Finger Print & Hand Geometry Reader.

٢. الصوت Voice Recognition.

٣. قرنية العين Iris Scanner.

٤. الوجه بالكامل Face Reader.

٥. وضع كاميرات مراقبة Camera.

استخدام كاميرات مراقبة لتحديد هوية الأشخاص

جهاز استخدام العين للكشف عن هوية الأشخاص

جهاز استخدام بصمة الأصابع للكشف عن هوية الأشخاص

حقوق الملكية الفكرية

حقوق الملكية الفكرية تعني حق المؤلف، المنتج أو المبدع وحده في الترخيص أو المنع لأي استغلال لمنتجه (الكتب، برامج الحاسوب، العلامات التجارية، المقاطع الموسيقية، الصور، الأفلام وغيرها) بأي شكل من الأشكال سواء بالنسخ أو الاستخدام أو البيع أو التأجير أو الإعارة بما في ذلك إتاحته عبر الحاسبات أو من خلال شبكات المعلومات وغيرها من الوسائل. وقد عقدت منظمة التجارة العالمية WTO العديد من المؤتمرات والاتفاقيات لتنظيم عملية التجارة الدولية ومنها حقوق الملكية الفكرية، وتتلخص حقوق الملكية الفكرية في مجال الحاسوب بتحديد وتعريف من يحق له استخدام البرامج المنتجة وشروط سحب حقوق الملكية الفكرية.

قوانين حقوق الملكية الفكرية عادة ما تمنع:

١. نسخ المواد أو البرامج أو الاقتباس منها إلا بعد الحصول على ترخيص كتابي مسبق من المؤلف أو ممثله القانوني.

٢. الإزالة أو التعطيل لأية حماية تقنية يستخدمها المؤلف (ككسر التشفير أو إزالة كلمة السر وغيره).

٣. النشـــر عبـــر أجهـــزة الحاســـبات أو شـــبكات المعلومـــات دون اخـــذ إذن كتـــابي مسبق من المؤلف.

٤. الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف.