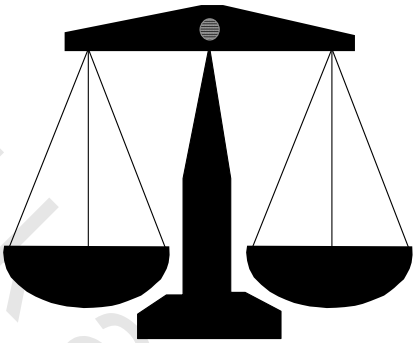

الفصل الخامس

الخصوصية (التشفير والأمن الرقمي)

الخصوصية

(التشفير والأمن الرقمي)

س٨١: ماذا يقصد بالخصوصية على شبكة الإنترنت؟

ج : الخصوصية خلال شبكة الإنترنت تعنى الأمن والأمان وعدم تركيب الصور والاحتفاظ بالأسرار وعدم كشفها أو إباحتها لأن كشف الأسرار يعنى ضياعًا للأخلاق وضياعًا للأموال وتعريض الأبرياء ـ دونما ذنب اقترفوه ـ للتكدير والتشويه .

س٨٢: هل هناك خصوصية مطلقة على الإنترنت؟

ج : لا توجد خصوصية مطلقة على شبكة الإنترنت، ويرجع هذا إلى الطبيعة المفتوحة للإنترنت إذ إن كل موقع Site هو شباك مفتوح أو شبه مغلق، أما أن يكون مغلقاً تماماً فلا .

س٨٣: ما هي حدود الخصوصية على الإنترنت؟

ج : الخصوصية هي كل ما يحتفظ به الأشخاص أو الدولة أو الشركات أو غيرها من الأسرار وليس هناك رغبة أن يطلع عليها أحد .

والقوانين لا تحدد ماهية المعلومات الشخصية .

س٨٤: كيف يمكن تقليل الأخطار الناشئة من التدخل في الخصوصية على الشبكة؟

ج : يمكن تقليل الأخطار الناجمة عن التدخل في الخصوصية على الشبكة إذا تم عمل الآتي :

١ـ استخدام التشفير .

٢ـ انتقاء المواقع التي يتم زيارتها .

٣ـ إغلاق البريد الإلكتروني عقب الانتهاء من استخدامه .

٤ـ انتقاء المعلومات التي يتم الإدلاء بها .

٥ـ استخدام أساليب حماية .

٦ـ استخدام مضادات الفيروسات .

٧ـ استخدام جُدر النار **Firewalls** .

٨ـ استخدام كلمات سر طويلة وغير معتادة ويفضل أن تكون من حروف وأرقام .

٩ـ تغيير كلمة السر من حين لآخر .

١٠ـ اللجوء إلى استخدام أسماء مستعارة .

س٨٥: هل من السهل اعتراض البريد الإلكتروني؟

ج : من السهل اعتراض البريد الإلكتروني وقراءة ما به من رسائل لأنه عند نقل البريد عبر الشبكة وبعد مغادرة الرسالة كمبيوتر المرسل تنتقل الرسالة من كمبيوتر خادم إلى كمبيوتر خادم آخر حتى تصل إلى المرسل إليه .

بهذه الطريقة فإنه ليس بالإمكان معرفة ما إذا كان شخص ما قد قرأ الرسالة المفترض أن تكون ذات خصوصية وتكون سرية قبل وصولها إلى المرسل إليه .

س٨٦: هل يمكن استيضاح بعض الحيل لاختطاف الرسالة المرسلة بالبريد الإلكتروني؟

ج : توجد الكثير من الحيل لاختطاف الرسالة الرقمية أثناء انتقالها بين الأجهزة الخادمة حتى لو كان الكمبيوتر الخادم محمياً بحائط صد وجدار النار (هو برنامج يمنع وصول غير المسموح لهم الدخول إلى النظام)، حيث يمكن للمخترقين تشغيل برامج تجرب كل احتمالات كلمات السر أو كلمات المرور البسيطة حتى تجد الكلمة التي تفتح بها شبكة الشركة، أو يمكنهم إلحاق أنفسهم بخادم الويب الخاص بالشركة والذي يوضع خارج جدار النار وبذلك يمكنهم التسلل إلى الشبكة الداخلية **Intranet** .

س٨٧: هل هناك طريقة لحماية البريد الإلكتروني من المتلصصين؟

ج : الطريقة الوحيدة لحماية البريد الإلكتروني من المتلصصين هي التشفير وهو الذي يؤدى إلى جعل الرسالة غير مقروءة إلا بواسطة المرسل إليه، والبرنامج الرسمي للتشفير هو Pretty Good Privacy (PGP) والخصوصية هي الـ Privacy .

س٨٨: ما دور الشبكات والخصوصية؟

ج : كل من شبكة سكيب نافيجيتور ومايكروسوفت إنترنت إكسبلورر ـ تحتوى على أدوات تسمح لمواقع الويب بالبحث في القرص الصلب وتشغيل البرامج، وهذه الشبكات تقدم حلولاً لمنع الاختراق .

س٨٩: ما هي خطورة اختراق الخصوصية؟

ج : تعد عملية تجميع المعلومات وعرضها للبيع إحدى مخاطر اختراق الخصوصية .

س٩٠: ماذا تعنى السرية والتأمين للبيانات؟

ج : هناك فروق بين السرية والتأمين والخصوصية نوضحها فيما يلي :

* السرية تعنى إخفاء البيانات بطريقة تمنع التعرف عليها في كل مراحلها ابتداء من التحرير والتعديل والحفظ والتداول .

* أما التأمين فيعنى حماية البيانات من محاولات التغيير أو التعديل أو الحذف أو الإضافة أو الإتلاف أثناء مرحلة التداول، كما يعنى ضمان وصولها إلى المستفيد والتحقق من شخصية كل من المرسل والمرسل إليه (المستقبل) .

* أما الخصوصية فهي عدم استخدام البيانات أو جزء منها في غير الغرض المرخص به من صاحبها ولا يصرح بإتاحتها أو إتاحة جزء منها دون موافقته .

س٩١: ماذا يقصد بالتشفير؟

ج : التشفير **Encryption** يقصد بـه تحقيـق التـأمين والـسرية حيـث يعتمـد علـى تحويـل المعلومات إلى رموز تصبح محمية مـن عمليـات الوصـول غـير المـرخص أو الاخـتراق وذلك باستخدام مفتاح يعرف بمفتاح التـشفير قبـل إرسـال الرسـالة الأصـلية بعمليـة عكسية لفك التشفير **Decryption** .

س٩٢: ما الذي يحكم تشفير البيانات؟

ج : يمكن تشفير البيانات الرقمية من خلال ثلاثة مصطلحات :

١ـ المفتاح العام .

٢ـ المفتاح الخاص .

٣ـ رقم الأساس .

ويمكن الاطلاع على أي معلومة مشفرة عن طريق هذه المفاتيح الثلاثة مجتمعة .

ويمكن توضيح هذه العملية من خلال الآتي:

* رقم الأساس يتم إصداره عن طريق جهة متخصصة في الإصدار ومرخص لها بذلك ويعرف برقم التوثيـق **Certificate Authority (CA)** ويكـون لكـل مـستخدم رقم أساس .

ويقسم رقم الأساس إلى قسمين هما :

١ـ رقم عام . ٢ـ رقم خاص .

بحيث يتحقق الآتي :

حاصل ضرب الرقم العام × الرقم الخاص = رقم الأساس

* الرقم العام هو رقم يتم تداوله ونشره بين كل المستخدمين وهو رقم أساس التشفير للشخص والذي بدونه لا تفك الشفرة، أما الرقم الخاص فهو الذي يكمل الرقم العام لإمكان فك الشفرة.

س٩٣: ما هي أنواع التشفير للبيانات؟

ج: يوجد نوعان لتشفير البيانات هما:

١ـ التشفير المتماثل Symmetric Algorithm ويتم تشفير الرسالة أو البيانات عن طريق الرقم العام كما يتم فك الشفرة بواسطته.

٢ـ التشفير غير المتماثل Asymmetric Algorithm ويتم به تشفير المعلومات بالرقم العام لكن لا يتم فك التشفير إلا بالمفتاح الخاص لصاحب المفتاح العام.

س٩٤: اذكر بعض طرق التشفير المتماثل؟

ج: من طرق التشفير المتماثل:

١ـ Digital Encryption Standard (DES).

٢ـ Tiny Encryption Algorithm (TEA).

٣ـ Triple DES.

٤ـ International Data Encryption.

س٩٥: اذكر بعض طرق التشفير غير المتماثل؟

ج: من طرق التشفير غير المتماثل:

١ـ Pretty Good Privacy (PGP).

٢ـ Reviset, Shamir and Aselman (RSA).

س٩٦: كيف يتم تشفير رسالة؟

ج : عن طريق تحويلها إلى رموز سرية بواسطة مفتاح (رقم خاص) يكون طوله عادة ٤٠ أو ٦٤ أو ٨٠ أو ١٢٨ بتاً والمفاتيح الأطول تعطى تشفيراً أكثر أمناً .

كما يتم التشفير عن طريق خدم وآيب بالمفاتيح العمومية للتأكد من أصالة المستخدم **Authentication** والشهادات الرقمية **Digital Certificates** .

س٩٧: ماذا تعرف عن التشفير بتكنولوجيا القياس البيومتري؟

ج : سبق الحديث عن القياس البيومتري وهو استخدام خصائص الإنسان كبصمة العين وبصمة الإصبع وبصمة الصوت وبصمة الدم .

وهناك من يمتدح استخدامه كشفرات، وهناك من يعلق بأنه يمكن الحصول عليها ويكون كشفها بواسطة القراصنة أسهل من شفرات أخرى .

س٩٨: ماذا يعنى التأمين بجدر النار؟

ج : جدر النار **Fire Walls** هي وسائل تأمين تستخدم لحماية الشبكات وخاصة الشبكات الداخلية المعروفة باسم الإنترانيت **Intranet** كالتي تكون بين بنك وبنوك أخرى وذلك لحماية البرامج من الاختراق لغير المصرح لهم .

س٩٩: كيف يتم التأمين ضد القرصنة؟

ج : ١ـ عن طريق الابتعاد عن الدردشة .

٢ـ عن طريق استخدام المضادات وبرامج التأمين .

٣ـ بعدم فتح الملفات الغريبة .

س١٠٠: كيف يتم التأمين ضد الفيروسات، وسرقة أرقام بطاقات الائتمان؟

ج : باستخدام البرامج المضادة للفيروسات مثل برنامج نورتن Norton والذي هو قابع في الجهاز يعطى إشارات لبرج المراقبة، وتشعر بمعاناته عبر رسالة تظهر يقول فيها : إن فيروس (يذكر اسمه) دخل الجهاز الآن . أنا أحاول التخلص منه . إنني غير قادر على السيطرة عليه تماماً . إنني أحاول . لقد تم التخلص من الفيروس . الآن جهازك محمى .

ورسالة أخرى تقول "اخترق جهازك الآن فيروس حصان طروادة . . النوع (يذكر نوعه) أحاول التخلص منه – لقد تم التخلص منه .

إنه برنامج ذكى ونبيه ويقظ ولا ينام ولا يتكاسل عن عمل مادام الجهاز مفتوحًا ويعرف مثل هذا البرنامج بالـ Anti-virus .

أما البطاقات الرقمية فيمكن تأمينها عن طريق المحافظة على الرقم السري وعدم التصريح به لأي شخص مهما تكن صلة قرابته، وتأمين عمليات الشراء، وأن ينتشر في المتاجر القارئات Readers للبطاقات الائتمانية .