

## تكنولوجيا العصر والجرائم المرافقة لها د ظاهر شاهر القشي

إن للتكنولوجيا المعاصرة إيجابيات عديدة قد بدا العالم فعلا بجني ثمارها بشكل منقطع النظير، ومن أهم تلك التكنولوجيات الحديثة شبكة الانترنت التي استطاعت ربط العالم بعضه البعض وجعلته أشبه بالقرية الواحدة، وألغت جميع الحدود الاقتصادية بين الدول من خلال ظهور تقنية التجارة الإلكترونية التي مكنت كل من التاجر والمستهلك بالتعامل دون قيود أو حدود تذكر، وجعلت الشركات تحقق إيرادات كانت في حكم الخيال قبل ظهور هذه التقنية.

رغم الفوائد والإيجابيات الكثيرة التي رافقت هذه التقنيات التكنولوجية الحديثة، إلا أنه رافقها سلبيات كثيرة بدأت تهدد وجودها إن لم يتم السيطرة عليها، وعلى رأس هذه السلبيات الجرائم التي ترتكب من خلالها، كجرائم الحاسوب بشكل عام وجرائم شبكة الانترنت بشكل خاص، فلقد أصبح العالم يفيق كل يوم على واقع جريمة جديدة ترتكب من خلال هذه التقنيات الحديثة، وباتت هذه الجرائم تهدد اقتصاد الدول بشكل خطير جدا، ومن الملاحظ بأن تلك الجرائم تتزايد بشكل متسارع يجاري ويوازي التسارع التكنولوجي، وللأسف أصبحت فن من الفنون له قواعده وقوانينه الخاصة.

ويمكن تصنيف هذه الجرائم ضمن فئتين رئيسيتين: ١- الهجوم على مواقع الشبكة بفيروسات معروفة وغير معروفة وإيقاع أضرار متعددة الأشكال والنتائج بأنظمة أصحاب تلك المواقع و٢- اختراق أنظمة الشركات عن طريق مواقعها الإلكترونية عبر شبكة الانترنت والحصول منها على معلومات سرية خاصة بعملائها لاستغلالها بالجرائم المالية.

فقد ذكرت صحيفة ناشيونال بوست National Post في ٢٠٠٣/٢/١٩ وضمن مقاله معنونة (قد استطاع قرصنة الانترنت إلى الوصول إلى الملايين من بطاقات الاعتماد) بأن أحد القرصنة استطاع اختراق قاعدة بيانات إحدى الشركات التي تعمل على إتمام تبادل العمليات بين التجار (كوسيط) واستطاع أن يصل إلى معلومات بطاقات الاعتماد وأرقام حسابات عملاء الشركة الإلكترونية. ووفقا لتصريحات هيئة بطاقات الاعتماد الدولية MasterCard International بأنه

وبسبب ذلك الاختراق تأثر أكثر ثمانية مليون حساب، منها ٣,٤ مليون حساب تخص حسابات بطاقات الفيزا، و ٢,٢ مليون حساب تخص بطاقات الاعتماد.

وحسب تصريحات ريك بروهيد Rick Broahead (كاتب ومحلل تكنولوجي) بأن ذلك الاختراق يعد من اكبر الاختراقات التي اطلع عليها. وقد رفض المتحدث باسم هيئة بطاقات الاعتماد الدولية إعطاء أية تفاصيل عن الآلية التي تم الاختراق بواسطتها والكيفية التي تأثرت بها الحسابات نتيجة ذلك الاختراق.

وقد قال السيد كيفين واسلين Kevin Wasslen (مدير إدارة المخاطر في هيئة بطاقات الاعتماد الدولية) بأننا لا نستطيع الجزم فيما إذا كانت المعلومات التي وصل إليها المخترق ستستخدم بأسلوب تلاعب أو غش أو خداع، من منطلق بأن بعض قرصنة الانترنت يخترقوا أنظمة الشركات لغايات التحدي لا اكثر ودون تبييت النية لاستخدام المعلومات التي يحصلون عليها لتحقيق غايات غير شرعية.

من الملاحظ بأن الشركات التي تصدر مثل هذا النوع من بطاقات الاعتماد التي تستخدم عبر شبكة الانترنت تحمي زبائنها وتمنحهم ضمانات أكيدة لتعويضهم عن أي خسائر تنتج من الاستخدام غير المصرح له لبطاقاتهم من قبل الغير. ومن الملاحظ كذلك بأن اغلب الشركات التي يتم اختراقها لا تعترف بحصول عملية الاختراق، وفي الحالة التي نتداولها لم تستطع الشركة التغاضي عن عملية الاختراق حيث أن عملائها هم الذين فضحوا الأمر للعموم، وقد اكتفت هيئة بطاقات الاعتماد الدولية بالقول بأنها كانت على علم بعملية الاختراق بمدة شهر واحدة من خروجها للعلن وبأنها لم تستطع أن تحدد إن كان الاختراق تما داخليا من الولايات المتحدة أم خارجيا.

مثل هذه القضية تطرح تساؤل مهم جدا، هل بالإمكان حماية الأنظمة المرتبطة بشبكة الانترنت بشكل كامل؟ الإجابة بالطبع ستكون لا، فأي شخص يود اختراق أي نظام سيتمكن من ذلك عاجلا أم آجلا وخصوصا إن كان مؤهلا تكنولوجيا، فكل نظام ولا بد من وجود نقاط ضعف فيه يستطيع الغير استغلالها إن وجدها، ولاكن ما تستطيع الشركات عمله والتركيز عليه بالوقت الحاضر الاستمرار في البحث عن وسائل وتطوير أنظمة حماية ومواكبة كل جديد لتقليل الفرص أمام المخترق بالوصول إلى نظامها والحد من الخسائر التي قد يسببها.

وأستطیع أن أشبه الحل، كالقضية الأزلية بین القط والفأر أو بین الشرطي والمجرم، فما دام الشرطي یطارء المجرم تبقى السرقات متدنية ولكن لم ولن تنتهي.