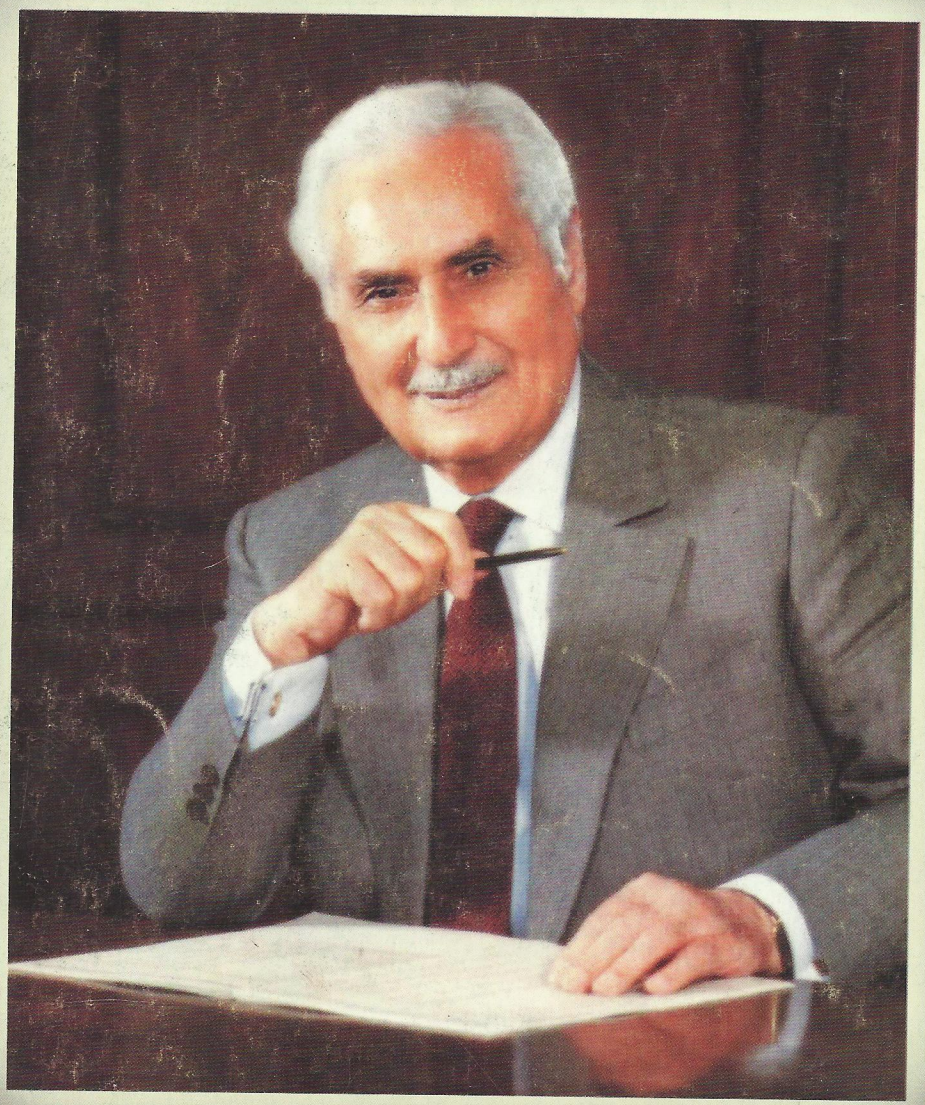
البنوك في الأردن
المواقع والانجازات

البنوك

في الأردن العدد الرابع / المجلد الرابع والعشرون / أيار - حزيران 2005



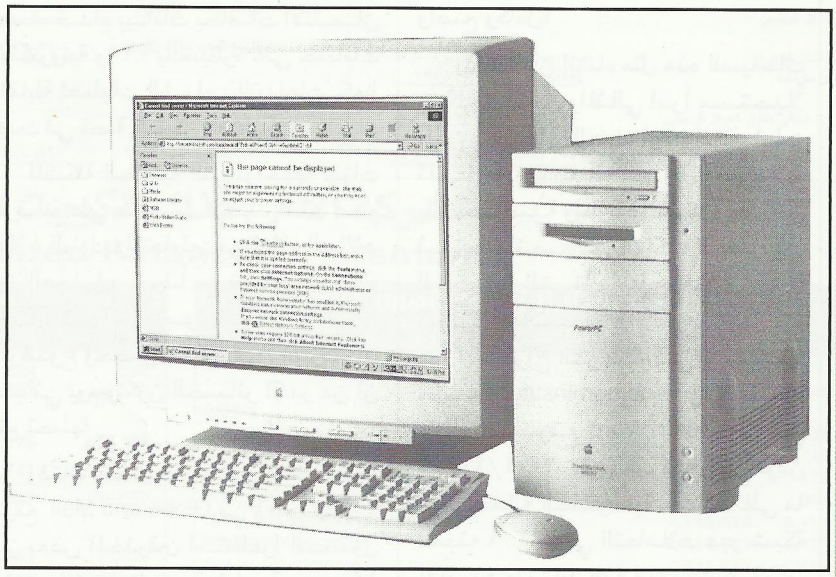
شومان
فقيد المجتمع المصرفي والمالي

رحلة عطاء استمرت ٧٠ عاماً مع البنك العربي

هل أصبح استخدام الانترنت لعنة تلاحق البنوك ؟

د. ظاهر القشي
رئيس قسم المحاسبة
جامعة الاسراء الخاصة

أ. د. نعيم دهمش
رئيس قسم المحاسبة والتمويل
جامعة عمان العربية للدراسات العليا



مع ظهور شبكة الإنترنت وبروز آلية التعاملات بواسطة التجارة الإلكترونية أخذت البنوك تطور أنظمتها بشكل ملحوظ ومتسارع لاستغلال هذه الفرصة الاستثمارية غير مسبوقة النظير مما لها من مردودات كبيرة لم يكن بالإمكان تحقيقها في السابق في ظل التجارة التقليدية ولكن وللأسف ورغم الإيجابيات الكثيرة التي رافقت هذا النوع من التعامل الجديد إلا أن سلبيات خطيرة رافقته كذلك والتي أصبحت لعنة تلاحق كل من البنك وعميله، فكما واكبت البنوك هذه التقنية العصرية بشكل متسارع واكبها كذلك المتحايلين عبر شبكة الإنترنت في ابتداع وسائل خداع كثيرة من أهمها وسيلتين رئيسيتين :

١ ـ إنشاء مواقع وهمية باسم بنوك كبيرة.

٢ ـ سرقة هوية المتعاملين ببطاقات الائتمان الإلكترونية.

ومن الأمثلة الكثيرة على وسيلتي الخداع السابق ذكرهما ما كشفته شبكة الأخبار CNN في ٢٠٠١/٤/١٣ عن فضيحة الخداع الكبيرة التي كشفتها غرفة التجارة الدولية International Chamber of Commerce والمتضمنة إصدار كفالات بنكية بقيمة ٢,٧ مليار دولار من قبل ٢٩ موقع إنترنت انتحل شخصية عدة بنوك عالمية، ورغم أنه تم اعتقال شخصين متورطين بالعملية إلا أن السيد Jon Merrett مساعد مدير غرفة التجارة الدولية يعتقد بأن الأشخاص المسؤولين عن عملية التحايل هذه كثر ولا يزال بإمكانهم إدارة عملية الاحتيال هذه بشكل أو بآخر.

وقد كشفت التحقيقات أن ضحايا هذه العملية قد دفعوا عدة ألوف من الدولارات للحصول على كفالات بنكية حيث صرح أحد التجار الأمريكيين أنه خسر مبلغ ٧٠ ألف دولار.

لقد كانت تظهر تلك المواقع على شبكة الإنترنت أنها تدار من قبل أسواق مالية مرموقة أو وكلاء ماليين مما كان يولد الثقة من قبل مستخدميها للحصول على كفالات بنكية مقابل رسوم اعتيادية.

مثل هذه الخدعة تجعلنا نطرح تساؤل مهم : من الذي يتحمل المسؤولية؟ طبعاً لا يمكن تحميل المسؤولية للبنوك ولا حتى العملاء حيث أن نقطة الضعف هنا تكمن بمزودي خدمة الإنترنت وإنشاء المواقع الإلكترونية حيث أن المتلاعبين استخدموا خدمات إنشاء المواقع المجانية المزودة من قبل بعض الشركات التي لا تتأكد من هوية مستخدم تلك المواقع نظراً لكونها مجانية ودعائية وهذا يظهر نقطة ضعف

قوية بآلية الأمان على شبكة الإنترنت ويجب على الحكومات إلزام تلك الشركات مزودة المواقع المجانية بالتأكد من هوية منشأ الموقع وإلزامهم كذلك بتزويد موقعهم الرئيسي بمحرك بحث يستطيع المتعامل استخدامه للتأكد من هوية الموقع المنشأ قبل الخوض بالتعاملات معه.

ومن الأمثلة الأخرى على الوسيلة الثانية "سرقة هوية المتعاملين ببطاقات الائتمان الإلكترونية" ما كشفه موقع Security Wire Digest في ٢٠٠٤/٣/١٦ عن تمكن أحد المتحايلين عبر شبكة الإنترنت اختراق موقع بنك فلوريدا وسرقة بيانات شخصية تعود لـ ٣٦٠٠ عميل، ورغم أن المخترق لم يخترق أي حساب إلا أن حصوله على بيانات العملاء المتضمنة أرقام بطاقات الائتمان الإلكترونية سيمكنه من استخدامها لاتمام عمليات شراء حقيقة وبالتالي فان وقوع أي خسائر على العملاء سيتحملها البنك بالكامل.

ومن الأمثلة الأخرى التي كشفها موقع Halton Crime Stoppers تمكن أحد المتلاعبين عبر شبكة الإنترنت من استخدام بعض بطاقات الائتمان العائدة لشركة Tornoto Man We'll Call Joe لاتمام عمليات شراء بلغت قيمتها ٢٠ ألف دولار، ويضيف الموقع أن الخسائر المعلن عنها من هذا النوع من الاختراقات بلغت هذا العام ١٤ مليون دولار بالمقارنة مع ٨ مليون دولار بالعام الماضي.

رغم أن صاحب متاجر Joe's لا يعلم كيف تم الحصول على بيانات بطاقات الاعتماد الخاصة بمحلاته إلا أنه متأكد بأن من حصل عليها شخص محترف، وقد تم اكتشاف التلاعب عندما قام بنكه بالاتصال به مبلغاً إياه عن تحويلات لحسابات محله من قبل بطاقات ائتمان عائدة لعدة أشخاص آخرين لبطاقة الائتمانية الخاصة قيمتها ١٧٠٠٠ دينار. وقد استطاع البنك فيما بعد اكتشاف آلية التلاعب والتي يمكن تلخيصها بالشكل التالي، فقبل حدوث عملية التلاعب أبلغ السيد Joe's بنكه عن فقدان بطاقة ائتمان عبر شبكة الإنترنت وصادف أحد المخترقين هذه المعلومة عبر الشبكة وأرسل للسيد oe's لطلب مشابه لطلب البنك يطلب منه معلومات البطاقة القديمة لاستبدالها وبعد أن حصل على البيانات قام هو بدوره بانتحال شخصية السيد Joe's وراسل البنك وحصل على معلومات البطاقة الجديدة التي استخدمها لإيداع مبالغ قيمة الشراء المستخدم بها بيانات بطاقات مسروقة من أشخاص آخرين.

رغم أن القصة السابقة لم تسبب خسائر للسيد Joe's أو لبنكه إلا أنها سببت خسائر لأطراف أخرى الذين استخدمت بطاقاتهم في إتمام عملية الشراء والتي تكون بنوكهم تحملتها ولم يعلن عنها خوفاً من خسران العملاء.

ويكشف الموقع أن ٨٠٪ من حالات الاحتيال عبر شبكة الإنترنت تتم بواسطة استخدام بيانات بطاقات الائتمان الإلكترونية و٢٠٪ بالسيطرة على حسابات المقابلة لعمليات الشراء "الإيداعات" كما حدث في قصة السيد Joe's.

المشكلة الحقيقية التي تواجهها جهات الرقابة على عمليات الاختراقات عدم إبلاغ البنوك والمتعاملين في أغلب الحالات عن العمليات خوفاً من فقدان العملاء ولهذا لا بد من وجود شفافية بهذا الموضوع وخصوصاً من قبل البنوك وإلا سيأتي يوم وتكون الخسائر أكبر من أن يتم تحملها.

وهناك قضية أخرى كشفها موقع Globe and Mail في ٢٠٠٤/٣/١٦ بأن بعض المخترقين استطاعوا الحصول على بيانات شخصية خاصة بـ ١٤٠٠٠ شخص حسب ما صرحت به شركة Equifax Canada Inc. والخاصة بتلقي بلغات قضايا التحايل ببطاقات لائتمان وقد تضمنت تلك البيانات التي تم سرقتها الرقم الوطني وأرقام حسابات البنوك وأرقام بطاقات الائتمان والعناوين الخاصة بأصحابها بشكل يمكن المتلاعب من الاستيلاء على الحسابات الشخصية في البنوك أو فتح حسابات بأسماء أصحاب تلك البيانات واستغلالها للحصول على قروض أو حتى بطاقات ائتمان.

لقد قامت شركة Equifax Canada Inc. بإبلاغ أصحاب تلك البيانات ولكنها لم تتأكد أن تم استخدامها فعلاً في إتمام أي عملية تحايل.

ان جميع الحقائق السابقة تجعل مستخدمي شبكة الإنترنت يتخوفون من استخدام بطاقات الائتمان وهذا ما أثبتته الدراسة التي قام بها معهد Privacy and American Business حسب ما جاء في موقعهم في ٢٠٠٤/١٠/٥ بأن ٩٤ مليون مستخدم لشبكة الإنترنت قرروا عدم التسجيل في المواقع الإلكترونية، والتبضع من خلالها لأيمانهم بأن سياسات حماية الخصوصية غير مكتملة أو غير واضحة. ومن هذه الحقيقة يمكن أن نطرح تساؤل : ماذا يجب على الشركات المتعاملة بشبكات الإنترنت عمله لتزويد المستخدمين بسياسات حماية الخصوصية بشكل واضح وكامل؟

ونعتقد بأن إنشاء مثل هذه السياسات بشكلها الكامل والمثالي أمراً مستحيلاً ولكن يجب على البنوك أولاً والمتعاملين ثانياً تأمين نظم الحماية الخاصة بالخصوصية وتطويرها بشكل يومي من قبل مختصين كي تواكب التغيرات السريعة التي تطرأ على تقنية شبكة الإنترنت العصرية. والدليل على صحة هذا الاقتراح الدراسة التي قامت بها مؤسسة Penemon Institul وفقاً لما جاء في موقع Computer Word في ٢٠٠٤/١٢/٢٩. بأن الشركات التي تؤمن آليات حماية الخصوصية حصلت على ما نسبته ٦٢,٩٪ في التعاملات عبر شبكة الإنترنت وتتزايد الثقة بهم بشكل دوري بنسبة ٩,٠٪ خلال مطلع عام ٢٠٠٤. وهذه الحقيقة تجعلنا ننصح البنوك بشكل عام والبنوك الأردنية بشكل خاص والتي ترغب في خوض التعاملات عبر شبكة الإنترنت بتوفير أقصى درجات الحماية بخصوصية زبائنها حيث أن لهذه الخصوصية ثمن باهض جداً.

بما أن البنوك تعتبر حجر الأساس في البنية الاقتصادية لأي دولة فان استخدام شبكة الإنترنت سيعظم الفوائد على الاقتصاد بشكل عام ولكن لا بد أن يكون للدولة عين رقابة على آليات حماية الخصوصية لدى تلك البنوك لتفادي أي مخاطر مستقبلية قد يكون وقعها فادحاً.