إضاءات
مالية مصرفية

نشرة توعوية يصدرها معهد الدراسات المصرفية بدولة الكويت - أكتوبر/نوفمبر ٢٠٠٨ - العدد الأول

الاحتيال الإلكتروني

أصبح الانترنت وسيلة سريعة لنشر المعلومات وتبادل البيانات بين جهات مختلفة، وتزايدت وسائل استخدام الانترنت فأصبح هناك ما يسمى بالتجارة الالكترونية والتعليم الالكتروني. وأصبحت أغلب المؤسسات والشركات تقدم خدماتها لموظفيها وعملائها عن طريق الانترنت، ومع هذا التطور انتشرت كذلك ظاهرة خطيرة وهي سرقة البيانات الخاصة عن طريق الانترنت، وذلك باستخدام وسائل الاحتيال على الآخرين بالعبث بالبرامج الخدمية التي تقدمها المؤسسات التجارية. والاحتيال هو أخذ واغتصاب لحقوق الآخرين وسلبهم ملكياتهم بدون وجه حق.

محاور العدد:

- مفهوم الاحتيال الالكتروني.
- أهم طرق الاحتيال الالكتروني المنتشرة عالميا.
- كيف يتعرض عملاء المصارف للنصب والاحتيال الالكتروني؟
- مدى خطورة هذه الظاهرة وأثرها على التعاملات التجارية.
- أهم وسائل الحماية الالكترونية.
- دور البنوك وشركات الأمن المعلوماتية في حماية مستخدمي شبكة الانترنت.
- أسباب زيادة عمليات الاحتيال الالكتروني المالي والمصرفي.

مفهوم الاحتيال الالكتروني:

تحول الاحتيال الإلكتروني عبر الإنترنت إلى ظاهرة عالمية جديدة أتاحت لمرتكبيها دخول المنازل والمكاتب واجتياز الحدود والوصول إلى الضحايا بسهولة بالغة، خاصة مع التطور الذي تشهده الخدمات البنكية الإلكترونية، حيث تقدم غالبية البنوك خدمات مالية واسعة عبر الإنترنت بما فيها تسديد الفواتير وتحويل الأموال.

وتتلخص عمليات الاحتيال الإلكترونية بمحاولة عدد من الأشخاص سرقة البيانات الشخصية لحاملي البطاقات ومستخدمي الإنترنت عبر رسائل بريد إلكترونية أو روابط إلكترونية تقود المستخدمين إلى مواقع إلكترونية شبيهة بالمواقع المعروفة، حيث تطلب هذه المواقع من المستخدمين بيانات شخصية هامة، يتم بواسطتها سحب مبالغ من أرصدة بعض العملاء أو تحويلها إلى حسابات أخرى أو الوقوع في مصيدة المشاركة في أنشطة مالية ومصرفية غير مشروعة.

أهم طرق الاحتيال الالكتروني المنتشرة عالمياً:

• القرصنة وذلك بعمل برامج ورموز خاصة تهاجم المجمع الرئيسي الداخلي للمؤسسة أو اختراق المجمعات الرئيسية المستضيفة للمجمع الداخلي للمؤسسة وإذا كانت المؤسسة تحمي نفسها باتخاذ التدابير الأمنية لمنع اختراق المجمع الداخلي، فإن المخترق يقوم بسرقة المعلومات والبيانات الاقتصادية للمؤسسة أو بيانات العملاء المالية ثم بيعها للمؤسسات المنافسة بأسعار عالية أو استغلالها لحسابه.

• تعطيل شبكة المجمع للمؤسسة المقصودة، حيث يقوم المحتال بإحداث أعطال بسيطة فيها تتسبب في إبطاء المجمع فتصبح الخدمات الالكترونية التي يقدمها موقع المؤسسة ضعيفة جدا

مما يؤثر على جودة الخدمات فيها ويهدد عملها، فيتسبب في انسحاب العملاء وبحثهم عن مؤسسات تقدم خدمات أفضل وأسرع. هذه الطريقة يتخذها المنافسون والمؤسسات المنافسة للمؤسسة المستهدفة.

• إرسال رسالة أو فيروسات أو برنامج مفخخ لموقع المؤسسة المقصودة فيقوم الفيروس بتخريب الموقع وتتوقف خدمات المؤسسة الالكترونية مما يؤثر على جودة الخدمات المقدمة لعملائها بشكل سلبي.

• عبر مواقع الشراء الإلكتروني غير الموثوقة، حيث تطلب من العميل إدخال رقم بطاقته الائتمانية، إضافة إلى تاريخ انتهاء صلاحية البطاقة وأرقام التحقيق الأمنية المدرجة خلف البطاقة، وبمجرد الكشف عنها يكون مصير هذه البطاقة في حينه في يد المحتال، كما تقوم بعض المواقع المشبوهة بطلب رقم حساب العميل الجاري ورقم بطاقة الصراف الآلي الخاصة به وطلب إدخال رقم بطاقته السري بحجة الخصم المباشر من حسابه، في حين يتمكن المحتال من طبع بطاقة مزورة برقم البطاقة الأصلية نفسه واستخدامها عبر أجهزة الصراف الآلي بالرقم السري نفسه.

• عملية الاصطياد الالكتروني وذلك بأن يرسل المحتال رسالة للضحية باسم مؤسسة معينة يخبره فيها أنه إذا أراد الحصول على خدمة ما من موقع المؤسسة وهي خدمات مجانية فكل ما عليه فعله هو أن يكتب بياناته الخاصة، أو قد تصل الضحية رسالة الكترونية كتب فيها انك ربحت مليون دولار وللحصول عليها اكتب اسمك وبياناتك الخاصة ورقم حسابك بالبنك فيقوم بعض الناس بكتابة تلك البيانات أملا في الفوز ولكنه في الحقيقة يرسل بياناته للمحتال فيستغلها.

• طرق احتيال أخرى من نقاط البيع، إذ ينسخ البائعون في هذه المحلات بيانات العميل ويقومون بعمليات شرائية كبيرة عبر الإنترنت أو تحويل مبالغ مالية.

طرق الاحتيال الالكتروني التي يتعرض لها عملاء البنوك:

يتعرض عملاء البنوك للعديد من طرق الاحتيال الالكتروني والتي تعتمد على ثقة العملاء في البنك، ولكنها في الوقت نفسه لا تمر بسهولة على الأنظمة الأمنية للبنوك التي تملك حماية كافية ومتطورة لأجهزتها، ونورد أهمها كالتالي:

• سرقة البيانات الإلكترونية باستخدام موقع مزور، وهذه العملية من أخطر العمليات التي تواجهها البنوك، حيث يقوم المحتال بإنشاء صفحة الكترونية لموقع شبيه تماما بالموقع الحقيقي للبنك يقوم خلاله العميل بإدخال رقم المستخدم والرقم السري الخاصين

بالعمليات المصرفية له عبر الانترنت، فتظهر هذه المعلومات عند المحتال الذي يقوم باستخدامها فورا دون أن يشعر العميل بذلك.

ورغم أن هذه الحيلة سريعة الكشف من قبل البنوك في الوقت الحاضر إلا أن التأخر في اتخاذ الإجراء المناسب والسريع يؤدي إلى نجاح عملية الاحتيال.

• ورود رسائل الكترونية إلى بريد العميل يذكر فيها أن البنك بصدد العمل على تحديث بياناته وتطوير إجراءاته الأمنية وأن عليه إرسال جميع تفاصيل حساباته وأرقامه السرية بالسرعة الممكنة ويتم توجيهه للدخول إلى موقع البنك المزيف عبر رابط الكتروني لا يمت لموقع البنك الأصلي بصلة، فيثق العميل لكون الموقع شبيها بالموقع الأصلي فيكتب بياناته المطلوبة ويرسلها. أو عبر رسائل الكترونية مزيفة من جهات تدعي أنها شركات خاصة بالبطاقات الائتمانية، تطلب فيها بعض البيانات من العملاء، وهناك رسائل صوتية تدعي أنها من هذه الجهات أيضا.

يوجد عصابات اجرامية متخصصة في عمليات الاحتيال الالكتروني في بنوك دول الخليج

• ومن الأساليب الأخرى محاولات اختراق أو سرقة البريد الالكتروني والمعلومات الشخصية لعملاء المصارف، حيث يقوم المحتال بهذا العمل لبيع البريد الالكتروني والبيانات الشخصية للضحية أو الاستفادة الشخصية من تلك المعلومات بسحب وتحويل مبالغ من حساب الضحية إلى حساباته المصرفية.

• ومن أخطر عمليات الاحتيال التي واجهتها بعض البنوك الخليجية في أجهزة الصراف الآلي مؤخرا هي وضع عصابات متخصصة أجهزة مزيفة لقراءة البطاقات عند مكان إدخال البطاقة في أجهزة الصراف الآلي تمكنهم من اصطياد أية بطاقة ائتمانية بنكية أو بطاقة صراف آلي، فيقوم بنسخ بيانات البطاقة وأرقام التعريف الشخصي الموجودة عليها، بالإضافة إلى تركيب آلة تصوير دقيقة في مكان محدد لقراءة رقم التعريف الشخصي عند إدخاله من قبل العميل.

• ممارسات جديدة يقودها المحتالون استهدفت التغرير بعملاء البنوك من خلال الاتصال على العميل والادعاء بأنه أحد موظفي البنك الذي يتعامل معه الشخص ويطلب جميع المعلومات المتعلقة بأرقام الحساب وأرقام الهوية الشخصية ضمن طلب تحديث البيانات الذي اعتادت عليه البنوك بشكل روتيني.

مدى خطورة هذه الظاهرة وأثرها على التعاملات التجارية:

تكمن خطورة الاحتيال الالكتروني بالنسبة للمؤسسات التجارية في إمكانية أن تخسر السمعة والمال والعملاء، كما تتزعزع ثقة المتعاملين حول العالم بشبكة الانترنت سواء من خلال التجارة الالكترونية أو العمليات المصرفية الالكترونية.

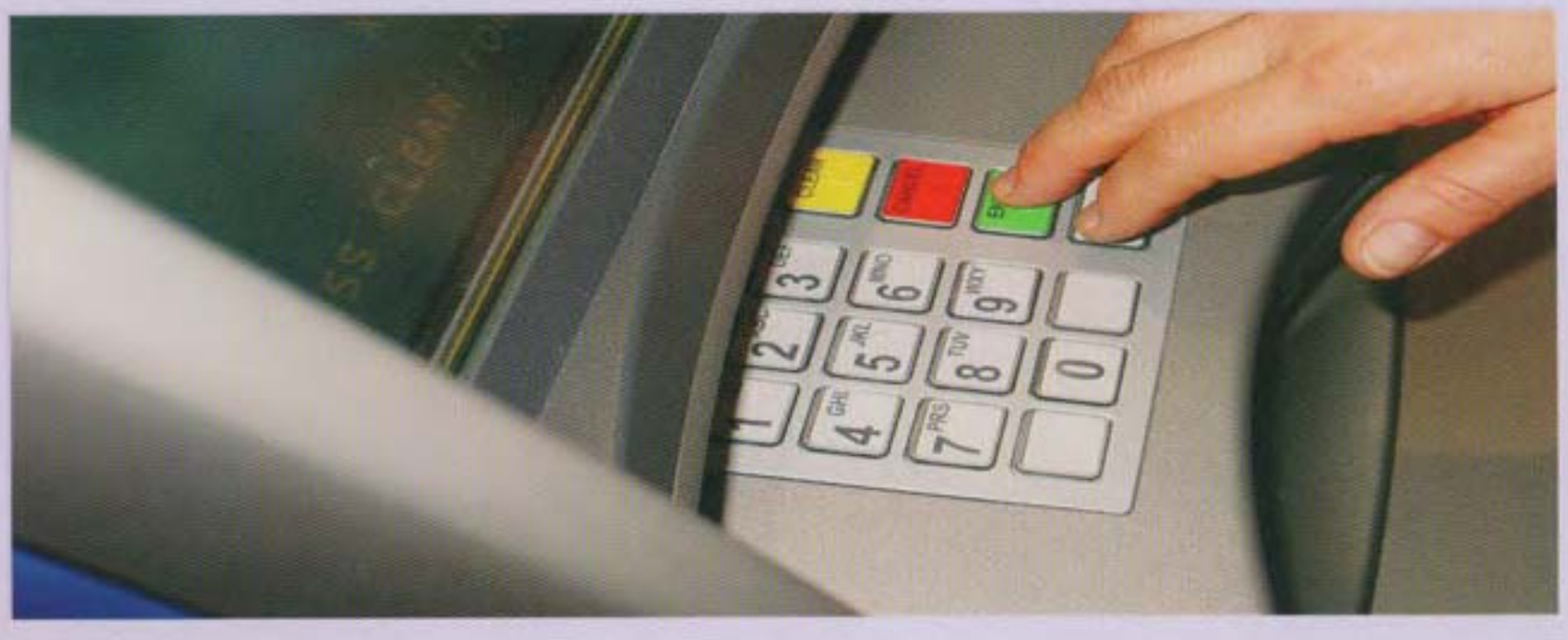
إن الحماية من عمليات الاحتيال الإلكتروني أصبحت ضرورية جدا لكل من يستخدم المنافذ الإلكترونية سواء من قبل المؤسسات أو الأفراد وخاصة عملاء البنوك عبر الإنترنت والهاتف المصرفي.

فيما يبتكر المحتالون الإلكترونيون وسائل جديدة يوميا للتغرير بضحاياهم والإيقاع بهم، يظهر الدور الهام للتقنيات المتطورة وشركات الأمن المعلوماتي وأنظمة الرقابة الداخلية في المؤسسات المالية في توفير بيئة آمنة لحماية العملاء وتأمين معاملاتهم المالية الالكترونية.

أهم وسائل الحماية الالكترونية:

• المصادقة وهي تعد من أشهر طرق الحماية باستخدام كلمة مرور خاصة واسم مستخدم خاص للتحقق من شخصية المستخدم، باستخدام التوقيع الالكتروني، بصمة اليد، بصمة العين، وترددات موجة الصوت.

• التحكم بخصائص الدخول، بأن يتم تقسيم خصائص الدخول بحسب إسم المستخدم فان كان المستخدم عضوا يتم عرض المعلومات والخصائص الخاصة للأعضاء فقط وان كان من الإدارة يفتح له خصائص الإدارة وهكذا .



• الترميز والتشفير، وتتم هذه الطريقة بتحويل الكلمات إلى رموز خاصة مشفرة متفاهم عليها بين الطرفين المستخدمين ويستخدم المتصفح للانترنت تلقائيا برنامج لتشفير البيانات، ومن طرق التشفير أيضا طريقة التوقيع الرقمي للتحقق من شخصية المستخدم.

• استخدام جدار الحماية الناري، ويشبه هذا الجدار الحاجز بين طرفين أي بين الشبكة الداخلية المحلية لمؤسسة خاصة والشبكة العالمية العامة ليمنع تسريب البيانات الخاصة أو اختراق المجمع للشبكة الداخلية، بالإضافة إلى استخدام رموز خاصة مثل كلمات مرور في التعاملات المالية.

• تركيب البرامج اللازمة للحماية من المتطفلين والفيروسات ومنع الهجمات التخريبية.

• التعرف على أسماء مواقع الاحتيال الالكترونية المتورطة وإدراجها في مختلف البرمجيات وخدمات التصفح والبريد الإلكتروني بحيث يتم التعرف عليها تلقائيا لحماية المستخدمين من أي عملية احتيال عبر الإنترنت، أو إغلاق تلك المواقع التي تقوم بالاحتيال ومنع رسائل الاحتيال الإلكترونية من الوصول إلى المستهلكين وحاملي البطاقات حول العالم.

• التسوق عبر المواقع الإلكترونية الآمنة والموثقة فقط، مع التأكد من أن عنوان الموقع يبدأ بالأحرف <https>. حيث أن حرف "s" يرمز إلى الكلمة "secure" أي أن الموقع المعني آمن تماماً، أو التأكد من وجود صورة قفل عند أسفل يمين متصفح الإنترنت الذي يستخدمه قبل القيام بعملية الشراء مع قراءة البنود الخاصة بها للحصول على معلومات دقيقة حول الإجراءات القانونية التي يمكن اتخاذها ضد التجار المشبوهين. ضرورة حفظ رقم التعريف الشخصي وعدم كتابته في أي مكان أو إرساله عبر الإنترنت، بالإضافة إلى وجوب التعامل بحرص مع البطاقات الإلكترونية كما تتعامل مع المبالغ النقدية.

• وجود فرق متخصصة تعمل على مدار الساعة وتجري البحوث الدورية اللازمة لمعرفة الثغرات والاحتمالات التي يمكن التسلل منها عبر الأنظمة الالكترونية وإغلاقها قبل وصول المحتالين وقراصنة الإنترنت لها.

دور البنوك وشركات الأمن المعلوماتية في حماية مستخدمي شبكة الانترنت:

أما فيما يخص البنوك، فهي تعمل على تعزيز دور الحلول التقنية الحالية في توفير بيئة آمنة لاستخدام وسائل الدفع الإلكترونية ومتابعة آخر المستجدات على الساحة الدولية بهذا المجال، والاستفادة من تجارب البنوك الأخرى في تعاملها مع عمليات الاحتيال الالكتروني، فتقوم بما يلي:

•تثقيف العملاء وتعريفهم بمختلف وسائل الحماية الالكترونية حيث يعتبر من أكثر الوسائل فعالية في إيقاف مثل هذه الجرائم على شبكة الانترنت، من أجل توفير سوق تسوده الشفافية والوعي التام بهذه الوسائل ووجوب الحذر والحيطة في تعاملات العملاء الالكترونية وعدم الانجرار وراء العروض والدعوات التي لا تتم عبر المواقع الرسمية للبنوك، كما أن عليهم التأكد من الروابط الإلكترونية للمواقع التي يدخلونها وعدم الكشف مطلقا عن أرقام بطاقاتهم الائتمانية، وعليهم الاتصال بالبنك وإشعاره عند مشاهدتهم أي ظاهرة غير طبيعية على موقع البنك الإلكتروني الذي يتعاملون معه وعدم الرد على رسائل البريد الإلكتروني التي تطلب بيانات شخصية أو كلمات التعريف السرية بزعم أنها رسائل واردة من البنك، وعدم إعطاء أي معلومات حول رقم الحساب المصرفي ما لم يكن العميل هو من اتصل بالبنك.

تثقيف العملاء هو أكثر الوسائل فعالية في إيقاف جرائم الإحتيال الإلكتروني

• استخدام أحدث أنظمة الحماية والأمان التي توفر درجة تأمين عالية لجميع التعاملات المصرفية عبر الإنترنت، وهي تتنوع بين تشفير جميع بيانات المتعاملين على الشبكة، واستخدام أحدث البرمجيات لضمان عدم الاختراق لأنظمة وقواعد بيانات المتعاملين لدى البنك، إضافة إلى وضع شروط وطريقة استخدام خاصة ومحددة تتفادى كل السيناريوهات المحتملة لإمكانية اختراق الحسابات.

• التعامل مع كبار الشركات المختصة بفحص الأنظمة الإلكترونية بشكل دوري ودائم، وبدورها تقوم الشركات بتقديم تقرير دوري للبنك عن مستوى ودرجة الأمان لأنظمته الإلكترونية، بما يؤدي في النهاية إلى ضمان معاملات مصرفية إلكترونية آمنة.

• وجود تحالف قوي بين التقنيات المتطورة وأنظمة الرقابة الداخلية في البنوك، والتواصل الدائم مع العملاء لاطلاعهم على أحدث المستجدات بهذا الشأن.

وقد قامت شركات عالمية، مثل "مايكروسوفت" بالانضمام إلى "مجموعة عمل مكافحة الاحتيال"، وهي جمعية شاملة لكافة القطاعات تهدف إلى حماية القانون والحد من عمليات الاحتيال عبر الإنترنت ورسائل البريد الإلكتروني.

أسباب زيادة عمليات الاحتيال المالي والمصرفي:

نلاحظ زيادة عمليات الاحتيال الالكتروني المالي والمصرفي في الفترة الأخيرة لعدة أسباب، منها: قلة عدد القنوات المصرفية الاستثمارية الآمنة بالنسبة للعملاء، التطور الكبير في قطاع التقنية المصرفية، التجارة الإلكترونية، وسائل الاتصال، رغبة الأفراد في التنمية السريعة لمدخراتهم وتحقيق أرباح قياسية، وغياب العقوبات الرادعة في حق المحتالين وضعف الأنظمة التشريعية والرقابية، بالإضافة إلى ضعف دور التوعية في وسائل الإعلام بمخاطر هذه الظاهرة، والاعتماد المتزايد على الوسائط الإلكترونية في عمليات البيع والشراء.

وقد أوضح بعض الخبراء في أمن المعلومات أن العديد من أشكال الاحتيال الإلكتروني تنقسم إلى قسمين أولهما اجتماعي نفسي والثاني تقني، وأن ٩٠٪ من عمليات الاحتيال على الإنترنت تنجح لأسباب اجتماعية وليس تقنية، وذكروا أن أكثر عمليات الاحتيال نجاحا في العالم هي تلك التي تعتمد على علم النفس لأن هذا الأسلوب هو الأكثر فعالية وسهولة، والتغرير بالضحية يكون ناتجا عن عدم الحرص وعدم القدرة على التصرف بصورة صحيحة.

المصادر:

• شبكة راصد الإخبارية
• شبكة الأسواق العربية
• دار الحياة – الصفحة الاقتصادية

ص.ب ١٠٨٠ الصفاة - ١٣٠١١ الكويت P.O.Box 1080 Safat 13011 Kuwait
هاتف: ٥/٢٤٥٨٤٦٠ ٩٦٥+ فاكس: ٢٤٦٦٤٣٠ ٩٦٥+
http//www.kibs.edu.kw email: marketing @kibs.edu.kw cs@kibs.edu.kw info@kibs.edu.kw