المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثاني والستين شهر (8) 2023

الاحتيال الإلكتروني وأنواع الغش والتلاعب في النظم الإلكترونية وتحليل أبعادها وحالات عليها(دراسة حالة البنوك السعودية)

د.عبد الناصر طلب حسن أحمد

جامعة الامام مُحَّد بن سعود الاسلامية

ملخص الدراسة:

هدفت هذه الدراسة إلى التعرف علي جرائم الاحتيال الالكتروني وأنواع الغش والتلاعب في النظم الالكترونية وبيان كيفية محاربتها والتصدي لها ، فمع التطورات في استخدام الحواسيب وبرامجها وتطبيقاتها خصوصا فيما يتعلق بتناقل البيانات والمعلومات والمعارف المختلفة قد يرافقه حدوث الجرائم الحاسوبية، وهذه الجرائم قد تكون في البيئة الداخلية للشركات والبنوك وغيرها ، وقد تكون من البيئة الخارجية وتحديدا عن طريق الاحتيال المعلوماتي الالكتروني، لذا فقد هدفت هذه الدراسة إلى التعرف على مفهوم هذه الجرائم الحاسوبية والاحتيال الالكتروني وأشكاله والأسباب التي تدفع لارتكاب مثل هذا النوع من الجرائم والتعرف على طرق الحماية من هذه الجرائم .

وقد خلصت الدراسة إلا أن مشكلة الغش والتلاعب باستخدام الحاسب الإلكتروني مشكلة عالمية لا تقتصر على قاره أو بلد دون آخر وتواجه البنوك والشركات والقطاعات الحكومية ، كما أن الخسائر الماليّة فيها في تزايد مستمر. كما أن أكثر الإفراد ارتكابا للغش والتّلاعب في ظل النظم الإلكترونيّة هم أفراد يعملون أساساً في مراكز مرتبطة بالحاسب الآلي بصفة عامة ، ومصممو البرامج على وجه الخصوص، وأكثر المنافذ التي يتم عن طريقها ارتكاب الغش والتلاعب هي المدخلات والبرامج. كما اتضح أن المصارف السعودية تلتزم بتطبيق معايير أمنية صارمة في مجال أمن المعلومات واستخدامها لأنظمة "دفاعية" متكاملة، تحصنها من عملية اختراق أو سطو إلكتروني محتملة.

وقد توصلت الدراسة إلى عدد من التوصيات من أهمها أن تقوم البنوك بتنفيذ حملات توعية مصرفية على مستوى المملكة، تستهدف من خلالها إحاطة موظفيها وعملائها كافة وبقية أفراد المجتمع بالأنماط الجديدة لعمليات الاحتيال المالي والمصرفي وسبل الوقاية منها.

المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثاني والستين شهر (8) 2023

Mail fraud and the types of fraud and manipulation in the electronic systems and the analysis of the dimensions and the cases (a case study of Saudi banks)

D. Abdel Nasser Hassan Ahmad
Professor of Business Administration at thehuraimla community college

Abstract

This study has aimed at exploring electronic crimes along with types of cyber fraud and manipulation of electronic systems. It has underlined the know-how of confronting these misdoings and fighting them. The development of computers and their programs as well as their applications most especially in so far data is concerned. The heaps of information and knowledge has enticed these crimes that might appear domestically in companies and banks and so on or attacking from the external environment. Thus this study seeks an investigation of electronic crimes concept and forms of electronic fraud along with handling the reasons behind committing such crimes, not to mention the methods of protections against cyber crimes.

The study concluded that fraud and manipulation through computers is an international problem not limited to a specific country. It menaces banks, business sector and governmental institutions on equal footing.. the Financial loss of such entities is increasing. It has been revealed that the persons who commit these crimes most are –broadly speaking- those working in computer centers, in addition to programmers in particular. It has been disclosed also that the methods used most in hacking are input units and programs. It has been unveiled that the Saudi banks abide to the application of strict safety criteria in the field of informatics security, let aside employing intact and integrate shields against any potential hacking.

The study has put forward a number of recommendations most important of which is the launching of bank awareness campaigns during which employees, clients and other people are cautioned against fraud and how to prevent them.

المقـدمة:

شهد العالم في العقود الأخيرة ثوره غي مجال الحاسب والمعلومات والاتصالات والتي انعكست بموجبها علي جميع القطاعات سوى أفراد أو شركات أو بنوك والتي انعكست بدورها على تقديمهم لأعمالهم وخدماتهم ، وأصبحت الدول والشركات الكبري تمتلك القدرة على التعامل إلكترونيا، وتقديم العديد من الخدمات من خلال الاتصال المباشر .on-line بل إن الاعتماد المكثف على النظام الرقمي Digitizationمكن الأفراد من الاتصال بشكل أكثر فعالية وأقل تكلفة مقارنة بالماضي .

ومع ذلك الكم الهائل من البيانات والمعلومات الهائلة المتدفقة بشتى أنواعـها كانت لابد من حمايتها من التداخلات التي تحدث إما عن طريق الأخطاء غير المقصودة أو العمدية سواء كان ذلك أثناء إدخال البيانات أو أثناء معالجتها وقد يدخل في ذلك وجود خلل في بعض التقنيات والتطبيقات وبرامج الحماية .

وهنا نسلط الضوء الاحتيال الالكتروني وأنواع الغش والتلاعب في النظم الإلكترونية باعتبارها أخطر جرائم العصر الحديث ولصعوبة اكتشافها .

مشكلة الدراسة:

مع التطورات المتلاحقة في عالم الاتصالات والإنترنت ومع زيادة أعداد المتعاملين بها ومع زيادة الحاجة لاستخدام البرامج الحاسوبية والانترنت. زادت الجريمة الإلكترونية وذلك للاتي:

1/ نقص التوعية الكافية لدى المستخدمين.

2/قله برامج الحماية وعدم متابعه تطور التقنيات الحديثة المستخدمة في عمليات الحماية من مشاكل الاحتيال ألمعلوماتي الالكتروني.

3/ صعوبة اكتشافها في المدى القصير.

أهـداف الدراسـة:

هدفت هذه الدراسة إلى:

1/ التعرف جرائم الاحتيال الالكتروني وأنواع الغش والتلاعب فيها.

2/ بيان كيفية محاربتها والتصدي لها من جميع الجهات المعنية.

فروض الدراسة :

1/ نقص التوعية الكافية لدى المستخدمين أدى إلى زيادة أعداد ضحايا جرائم الاحتيال الإلكتروني.

2/ قله برامج الحماية وعدم متابعه تطور التقنيات الحديثة المستخدمة في عمليات الحماية من مشاكل الاحتيال ألمعلوماتي الالكتروني ذاد من تفشي المشكلة.

6/ منهجية الدراسة :

سيتم الحصول على المعلومات والبيانات من المصادر المتمثلة في الكتب والمقالات والبحوث المنشورة والمقالات والمحاضرات والقوانين والمكاتبات الرسمية .

أولاً: الغش والتلاعب في النظم الإلكترونية وأنواعه :

يعتبر الغش بصفة عامّة نوعاً من الأخطاء المقصودة التي ترتكب عمداً وذلك أما :

1/ للتضليل

2/ الإخفاء ((لأي بيانات أو معلومات))

3/ الاختلاس

4/ التأثير علي أعمال أي مشروع

ويمكن تقسيم حالات الغش والتلاعب التي تحدث في ظل النّظم اليدويّة التقليديّة إلى مجموعتين رئيسيّتين:

1] تلاعب في الدفاتر والسّجلات بقصد إخفاء عجز أو اختلاس أو سوء استعمال أصل من أصول المنشأة مثل:

1. إثبات مدفوعات وهمية بالدفاتر لتغطية اختلاس.
2. عدم إثبات نقدية واردة من عميل واختلاسها أو استخدامها لتغطية عجز بالخزينة.
3. عدم إثبات بضائع واردة بسجلات المخازن.

2] تلاعب في الدفاتر والسّجلات بقصد التأثير على مدى دلالة القوائم الماليّة عن نتيجة أعمال المنشأة من ربح أو خسارة خلال فترة معيّنة وعن مركزها المالي في نهاية هذا الفترة . ويحدث هذا النّوع من التلاعب بتوجيه من إدارة المنشأة . وتكون نتائجه خطيرة وعادة يكون الغرض من ارتكابه تحقيق أحد الأهداف التالية:

أ/ إظهار أرباح أكثر من الأرباح الحقيقية.

ب/ إظهار أرباح أقل من الأرباح الحقيقيّة لتكوين احتياطيات سريّة.

ت/ إظهار المركز المالي على غير حقيقته عن طريق التلاعب في قيم بعض عناصر الأصول والخصوم

مفهوم الغش وأنواعه في ظل النظم الإلكترونية:

في الواقع فإن الغش في ظل النظم الإلكترونيّة لن يختلف من حيث المفهوم والأهداف عن الغش في النظم اليدوية التقليدية ، وإن كان يختلف في طبيعته وطرق ارتكابه والقائمين به ، وذلك نتيجة لاختلاف طبيعة التشغيل الإلكتروني للبيانات أساساً عن التشغيل اليدوي التقليدي ولقد عرّف البعض الغش في النّظم الإلكترونيّة بأنّه الاستخدام غير المشروع لأجهزة الكمبيوتر ، الأنظمة الإلكترونيّة ، أو شبكة الأنظمة الإلكترونية ، وذلك بهدف الحصول على أموال أو أصول أو خدمات بطريقة التّلاعب.

ويمكن تقسيم الغش في ظل النّظم الإلكترونية حسب أنواعه إلى المجموعات الأربعة التالية:

1. غش يترتّب عليه اختلاس أصول.
2. غش يترتب عليه سرقة معلومات.
3. غش يترتب عليه استخدام الحاسب في غير أعمال المنشأة.
4. غش يترتب عليه سرقة برنامج.

ولقد ارتفعت قيمة الخسائر النّاجمة عن الغش والتّلاعب من خلال الحاسب الإلكتروني بشكل ملحوظ خلال السّنوات القليلة الماضية .

تحليل أبعاد مشكلة الغش والتّلاعب في ظل النّظم الإلكترونية:

تعتبر الدّراسات التي تناولت أبعاد مشكلة الغش والتّلاعب في ظل النّظم الإلكترونية قليلة نسبيّاً نظراً لعدم توفّر النّشر الكافي عن حالات الغش والتلاعب لتأثيراتها البالغة على المنشآت التي تعرّضت لهذه الجريمة من ناحية ، ولعدم إتاحة الفرصة لتكرار هذه الحالات من ناحية أخرى . ونعرض في هذا الجزء ما توصّلنا إليه لنتائج دراستين في هذا المجال لتحديد أبعاد مشكلة الغش والتّلاعب في ظل النّظم الإلكترونيّة.

ولقد شملت دّراسة عن حالات الغش لحوالي 238 حالة غش حدثت في كل من الولايات المتّحدة الأمريكية ، كندا والمملكة المتّحدة ، وبعض الدّول الأوربيّة الأخرى ، وتتضمن الجداول من الجدول رقم (1) إلى الجدول رقم (5) التالية ملخصاً لأهم نتائج هذه الدراسة طبقاً للأبعاد المختلفة لهذه المشكلة والتي من أهمّها:

1. الخسائر المالية النّاجمة عن ارتكاب الغش والتّلاعب.
2. الوظائف والمستويات الإداريّة لمرتكبي حالات الغش والتّلاعب.
3. مجالات الأنشطة التي تم ارتكاب الغش والتّلاعب فيها.
4. المنافذ التي تم استغلالها لارتكاب الغش والتّلاعب.
5. نظم التشغيل الإلكتروني المطبّقة التي تم من خلالها ارتكاب الغش والتلاعب.

جدول رقم (1)

يوضح الخسائر المالية الناجمة

عن ارتكاب الغش والتلاعب

الحالات التي أمكن تحديد الخسائر الناجمة عنها	عدد الحالات	إجمالي الخسائر (بالمليون)	متوسط الخسارة للحالة الواحدة
الولايات المتحدة الأمريكية	124	125.951دولار	مليون دولار
المملكة المتحدة	21	3.278 دولار	156 ألف إسترليني

المصدر : د: سمير احمد أبو غابه ، المبادئ والاتجاهات الحديثة للمراجعة ص رقم422

جدول رقم (2)

يوضح الوظائف والمستويات الإدارية

لمرتكبي حالات الغش والتلاعب

وظائف و مستويات مرتكبي الغش والتلاعب	عدد الحالات	النسبه %
مصممي البرامج	59	%25
مشغلي الحاسب	40	%17
المسئولين عن إعداد البيانات	29	%12
مديري مركز الحاسب الآلي	23	%10
مشغلي أجهزة تغذية الأنظمة الإلكترونية بالبيانات	12	%5
محللي النظم	3	%1
الإجمـــــــــــــــــالى	**166**	**%70**

المصدر : د: سمير احمد أبو غابه ، المبادئ والاتجاهات الحديثة للمراجعة ص رقم423

جدول رقم (3)

يوضح الأنشطة التي تم فيها

ارتكاب حالات الغش والتلاعب

المجـــــــــــــــــــالات	عدد الحالات	النسبة %
المشتريات وحسابات الدائنين	65	%27
المخزون	40	%17
الاستغلال غير المشروع للأنظمة الإلكترونية	38	%16
الإيداعات والقروض	32	%13
الأجور	22	%9
المبيعات والمتحصلات	15	%6
أخرى متنوعة	26	%11
الإجمـــــــــــــــــــالى	**238**	**%100**

المصدر : د: سمير احمد أبو غابه ، المبادئ والاتجاهات الحديثة للمراجعة ص رقم424

جدول رقم (4)

يوضح المنافذ التي تم استغلالها

لارتكاب حالات الغش والتلاعب

منافذ ارتكاب حالات الغش والتلاعب	عدد الحالات	النسبه %
المدخـــــــــــلات	114	%48
البرامـــــــــــج	47	%20
قاعـــــــــده البيانات	43	%18
الحاسب الإلكتروني ذاته	22	%9
المخـــــــــــرجات	12	%5
الإجمـــــــــــــــــــالى	**238**	**%100**

المصدر : د: سمير احمد أبو غابه ، ا المبادئ والاتجاهات الحديثة للمراجعة ص رقم425

جدول رقم (5)

يوضح نظم التشغيل الإلكتروني التي تم من خلالها

ارتكاب حالات الغش والتلاعب

نظام التشغيل الإلكتروني	عدد الحالات	النسبة %
التشغيل في مجموعات	121	%51
التشغيل المباشر / الفوري	110	%46
المشاركة الزمنية	4	%2
مكاتب خدمات الحاسب المتخصصة	3	%1
الإجمـــــــــــــــــــــالى	**238**	**%100**

المصدر : د: سمير احمد أبو غابه ، المبادئ والاتجاهات الحديثة للمراجعة ص رقم418

ولعل من أهم ما كشفت عنه الدّراسة السّابقة:

[] أن متوسّط الخسارة الماليّة في حالة الغش الواحدة بلغت مليون دولار.

[] أن 70% من عدد حالات الغش والتلاعب تم ارتكابها بواسطة أفراد يعملون داخل مركز الحاسب الإلكتروني.

[] أن مصمّمي البرامج من أكثر الأفراد ارتكابا للغش والتّلاعب حيث أن 25% من الحالات أرتكب في هذه المجالات .

[] ويعتبر منفذ المدخلات من أكثر منافذ ارتكاب الغش حيث أن ما يقرب من نصف عدد حالات ارتكبت من خلال هذا المنفذ.

أمّا الدراسة الثّانية ، فلقد تضمّنت تحليل 150 حالة غش وتلاعب ، وتشمل الجداول من رقم (6) إلى الجدول رقم (9) ، ملخّصاً لأهم نتائج هذه الدّراسة والتي غطّت عدّة أبعاد لهذه المشكلة أهمّها ما يلي.

1. الخسائر الماليّة النّاجمة عن ارتكاب الغش والتّلاعب.
2. الوظائف والمراكز الإداريّة لمرتكبي حالات الغش والتّلاعب.
3. المجالات والأنشطة التي تم ارتكاب الغش والتلاعب فيها.
4. طرق ارتكاب الغش والتلاعب.

جدول رقم (6)
يوضح الخسائر الناجمة
عن ارتكاب حالات الغش والتلاعب

الجهات التي تعرضت لحالات الغش والتلاعب	مقدار الخسائر بالألف
الشركـــــــــــــــــات	621 دولار
البنوك والشركات المالية	193دولار
الوحدات الحكومية	374 دولار
الإجمـــــــــــــــــالى	**1.88 مليون دولار**

المصدر : BRANDT AALLEN OP CIT . P.60

جدول رقم (7)
يوضح الوظائف والمستويات الإدارية
لمرتكبي حالات الغش والتلاعب

وظيفة مرتكب الغش	بنوك	شركات	و/ حكومية	الجملة
مسئولين عن تغذية الحسابات	**2**	6	7	**15**
كاتب / صراف	**4**	6	6	**16**
مصممي برامج	**7**	7	1	**15**
مديرين	**12**	7	2	**21**
مشغلي الحاسب	**5**	3	1	**9**
وظائف أخرى	**-**	4	1	**5**
من خارج المنشأة	**3**	2	-	**5**
غير معروف	**1**	2	-	**2**

المصدر : BRANDT AALLEN OP CIT . P.61

جدول رقم (8)

يوضح المجالات والأنشطة التي تم فيها ارتكاب حالات

الغش والتلاعب

المجالات	عدد الحالات
المحاسبة / الرقابة على المخزون/ المدفوعات	69
سداد مبالغ للعاملين وافراد اخرين	56
فواتير / تحصيلات / ايداعات	27
متنوعة	4
الإجمالى	**156**

المصدر : BRANDT AALLEN OP CIT . P.50

جدول رقم (9)
يوضح طرق ارتكاب حالات
الغش والتلاعب

المجالات	عدد الحالات
إضافة عمليات أو تعديلها	101
إجراء تغيرات غير مشروعه في البرامج	14
تغيير غير مشروع في الملفات	12
حذف عمليات	7
عمليات تشغيل غير صحيحه	5
متنوعه أو غير معروفه	17
الإجمالى	**156**

المصدر : BRANDT AALLEN OP CIT . P.56

ولقد كشفت هذا الدراسة أن الغش والتّلاعب في ظل النّظم الإلكترونيّة لا يقتصر على قطاع الأعمال والبنوك فقط وإنّما يمتد أيضاً إلى الوحدات الحكوميّة .

كما أظهرت هذه الدّراسة أيضاً أن المديرين ومصمّمي البرامج كان لهم دور كبير في ارتكاب حالات الغش والتّلاعب .

وإن مجال المحاسبة والرّقابة على المخزون والمدفوعات من أكثر المجالات تعرضاً للغش والتّلاعب .

وأن أكثر الطّرق شيوعاً في ارتكاب الغش والتلاعب هي طريقة إضافة عمليات أو تعديلها ، حيث بلغ عدد الحالات التي ارتكاب الغش فيها بهذه الطريقة 101 حالة من 150 حالة.

النتائج:

نخلص من واقع نتائج كل من الدّراستين السّابقتين بمجموعة من الملاحظات العامّة نوجزها فيما يلي:

1. إن مشكلة الغش والتلاعب باستخدام الحاسب الإلكتروني مشكلة دوليّة لا تقتصر على بلد دون آخر وتواجه البنوك ووحدات قطاع الأعمال والوحدات الحكومية ، كما أن الخسائر الماليّة عنها في تزايد مستمر.
2. إن أكثر الإفراد ارتكابا للغش والتّلاعب في ظل النظم الإلكترونيّة هم أفراد مراكز الحاسبات الإلكترونية بصفة عامة ، ومصممو البرامج على وجه الخصوص.
3. إن أكثر المنافذ التي يتم عن طريقها ارتكاب الغش والتلاعب هي المدخلات والبرامج.
4. إن إضافة عمليات أو تعديلها هي من أكثر الطرق شيوعاً لارتكاب الغش والتلاعب

ثانياً: الاحتيال الإلكتروني؟

يعتبر الاحتيال الإلكتروني من الطرف الحديثة في السرقة والتي تعتمد على الشبكة العنكبوتية ((الإنترنت)) في معرفة وسرقة البيانات وأرقام الحسابات والبطاقات الائتمانية واسم المستخدم وكلمات السر وغيرها من المعلومات الخاصة والشخصية ((بغرض التجسس أو انتحال الشخصية))

فى الغالب يستخدم المحتالون مواقع أنترنت مزيفة ويرسلون رسائل خادعه ألي ضحاياهم وهو جريمة ذات طابع مادي، تتمثل في كل فعل غير مشروع أو سلوك غير مشروع, من خلال استعمال :

1- الحاسب الآلي.
2- أجهزة النقال
3- الهواتف الأرضية
4- شبكات الإنترنت .

وتهدف هذه الجرائم إلى الوصول غير مصرح به إلي المعلومات ولبيانات الخاصة والسرية غير مسموح بمعرفتها إلي للشخص نفسه وذلك بهدف نقل تلك البيانات والمعلومات أو نسخها أو حذفها.

كما قد يلجأ السارقون إلى عمليات التهديد أو الابتزاز أو حتى التدمير لتلك البيانات والمعلومات وتدمير الحواسيب بواسطة الفيروسات ..

و تعدد أشكال وأنواع هذه الجرائم حسب الهدف من الجريمة :

بعضها يهدف الي جمع المعلومات والبيانات فقط .

البعض الآخر يهدف إلي الاستغلال المادي.

ومنها ما يهدف إلي الابتزاز الأخلاقي.

كذلك منها ما يهدف إلى التشهير وتشويه السمعة

وأخيراً منها ما يكون فقط بغرض التحدي وروح المغامرة

وقد صنفها المختصون في مجال أمن المعلومات إلى عدة أنواع حسب نوع الجريمة وهدفها، فمنها:

1/ جرائم التخريب المعلوماتي .

2/ جرائم التجسس الإلكتروني .

3/ جرائم التلاعب والاحتيال الإلكتروني.

وما يهمنا هنا هو جرائم التلاعب والاحتيال الإلكتروني والتي انتشرت بصوره كبيره وذادت ونمت خلال العقد الأخير بسبب الانتشار الهائل للشبكات الاجتماعية ومواقع التواصل الالكتروني .

وقد وصف تقرير دولي الهجمات الإلكترونية التي تتعرض لها الشركات والمؤسسات والهيئات السعودية بأنها من «أشرس أنواع الهجمات الإلكترونية». وأفاد بأن غالبية خسائر القطاع البنكي في المملكة ناتجة عن اختراق البيانات وسرقة البيانات المصرفية من عملاء وبنوك ومصارف.

وقد خسرت البنوك السعودية وحدها منذ 2008 وحتى الآن أكثر من مليار دولار من جراء الجريمة الإلكترونية. كما أفاد تقرير آخر صدر في عام 2010 بأن الجرائم الإلكترونية تكبد دول مجلس التعاون الخليجي خسائر تقدر بـ 735 مليون دولار سنويا. كما أكد اقتصادي متخصص أن معدل نسبة الجرائم الالكترونية في العالم يصل إلى 57.6% حيث يكلف الاقتصاد العالمي ما يقارب (12.950) مليار دولار سنوياً. وقال إن نسبة معدل الهجمات الالكترونية في السعودية يقارب 45.8% لعام 2009, كما كانت نسبة الهجمات للحسابات البنكية للأفراد عام 2009بلغت40%, واختراق المواقع الالكترونية لعام 2009 بلغ 63%,و رسائل الاحتيال في المملكة لعام 2009م بلغت 43.7%

كما كشفت السلطات الأمريكية أن عمليات قرصنة وسرقة طالت أكثر من 130 مليون بطاقة ائتمان وبطاقة سحب مصرفية.

و أظهر تقرير نشرته "سيمانتك كوربوريشن" تزايداً مطرداً في هجمات الجريمة الإلكترونية حيث تم رصد أكثر من 99 تهديد إلكتروني في الثانية خلال العام 2009.

وفي دراسة أجرتها شركة نورتن الرائدة في تطوير الحلول البرمجية الأمنية أن ثلثي مستخدمي الانترنت حول العالم تعرضوا لجريمة إلكترونية على الأقل مرة واحدة وقد تمثلت في هجمات فيروسية و تجسسية واحتيالية لسرقة بطاقات الائتمان وسرقة الهوية أو البيانات المصرفية والشخصية الحساسة. كما أشارت الدراسة إلى أن عملية إزالة الآثار المترتبة من الجريمة الإلكترونية تستغرق في المتوسط 28 يوم كما تكلف في المتوسط 334 دولار.

وفي دراسة أجرتها شركة تريند مايكرو المشهورة بمحاربة الفيروسات أشارت إلى أن السعودية والإمارات تتصدر المركز الأول والثاني على مستوى الدول المجلس التعاوني الخليجي , وفي السعودية فقط حصل 700 ألف انهيار نظام خلال تسعة شهور.

وقد قسمت شركة كاسبر سباي –المتخصصة في منتجات الحماية الإلكترونية– دول العالم إلى ثلاث مجموعات وذلك حسب نسبة تعرضها لمخاطر الجرائم الإلكترونية:

مجموعة عالية المخاطر:

وهي التي يتعرض فيها 40ـ 61% من مستخدمي الإنترنت للهجمات الإلكترونية.

مجموعة متوسطة المخاطر:

وهي التي يتعرض فيها 20ـ 41% من مستخدمي الإنترنت للهجمات الإلكترونية.

مجموعة منخفضة المخاطر:

وهي التي يتعرض فيها اقل من 19% من مستخدمي الإنترنت للهجمات الإلكترونية.

والمملكة العربية السعودية من الدول تقع ضمن المجموعة عالية المخاطر وذلك مع عدة دول أخرى وهي روسيا والعراق وأرمينيا وعمان والسودان وأذربيجان والهند.

وطبقا لتقارير نفس الشركة، فإن أعلى نسبة لمرتكبي جرائم اختراق مواقع الإنترنت تقع في الهند، وتبلغ 14.8% من إجمالي مرتكبي هذه الجرائم في العالم، بينما تبلغ هذه النسبة 1.33% لكل دول مجلس التعاون الخليجي، وتحوز السعودية أعلى نصيب من هذه النسبة، وهي نسبة عالية لو أخذنا في الحسبان العلاقة بين هذه النسب وبين عدد مستخدمي الإنترنت الذين يبلغ عددهم في الهند 141 مليون مستخدم، وفي دول مجلس التعاون مجتمعة نحو 17 مليونا

كما أشارت دراسة أجراها أحد باحثي جرائم الإنترنت في المملكة أن نسبة 14.2% من المجموع الكلي لمستخدمي الإنترنت من السعوديين يخترقون المواقع السعودية مقارنة بنسبة 8.9% من المجموع الكلي للمستخدمين غير السعوديين.

كما تبين من خلال فحص بيانات مستخدمي الإنترنت أن 15.1% من مستخدمي شبكة الإنترنت في المجتمع السعودي قاموا باختراق البريد الإلكتروني للآخرين، منهم 11.8% سعوديين، مقابل 3.3% من الأجانب. ولو علمنا أن عدد مستخدمي الإنترنت في السعودية يبلغ حوالي 14 مليون مستخدم، فإننا نصل إلى حقيقة مخيفة، وهي أن مرتكبي جرائم اختراق مواقع الإنترنت في المملكة يزيدون على مليون شخص.

ويصعب تحديد تلك الخسائر بدقة، حيث إن حصرها يستلزم أن تقوم الجهات التي تتعرض لهجوم إلكتروني بالإبلاغ عن ذلك، وهو ما لا يحدث في كثير من الأحيان لأسباب مثل الخوف من المساءلة أو الخوف من اهتزاز سمعة المؤسسة أو موثوقيتها أمام عملائها أو غير ذلك.

أما عن خطورة تلك الجرائم، فإنها إذا كانت تستهدف المؤسسات فإنها تنطوي على أضرار وأخطار جسيمة تلحق بالمؤسسات المستهدفة، حيث إن هدفها في أغلب الأمر هو تعطيل العمليات وتدمير البنية المعلوماتية للمؤسسة.

ومن أمثلة الاحتيال الالكتروني:

1/الرسائل التي تصل عبر البريد الإلكتروني والتي تتطلب رقم حسابك المصرفي أو تحديث بيانتك الشخصية أو معرفة رمز الدخول والرمز السري وغيرها .

2/الاتصالات الهاتفية من أفراد ينتحلون صفة ممثلي لمعرفة بياناتك وأرقام حساباتك الشخصية.

3/ قد يتظاهر لك شخص ما بأنه يمثل منظمة حقيقية بهدف الحصول على بعض المعلومات الشخصية لك.

4/ تركيب برامجك فى أجهزتك الشخصية أو أجهزة الشركات بغرض التجسس وسرقة المعلومات.

5/ كذلك بعض الرسائل التي ترد أليك بطلب الاتصال بأحد الأرقام للتحقق من بياناتك الشخصية.

6/ وأخيراً الاحتيال والتلاعب الإلكتروني الصوتي وهو الأخطر من الرسائل وفيه يقوم المحتال بتزييف رقم هاتف أو رقم جهة معينة معروفه لديك أو موقع معروف..

الاحتيال عن طريق أجهزة الصراف الآلي:

يعتبر جهاز الصراف الآلي من الأجهزة الحديثة التي تسمح للشخص بسحب وايداع النقود وإجراء التحويلات في أوقات خارج الدوام الرسمي بهدف التسهيل علي العميل في عملية السحب والإيداع ، وقد زادت في الفترة الأخيرة وسائل الاحتيال فيها

ومن أنواع الاحتيال فيها ما يلي:

1/ مسح البطاقات: يقوم المجرمون بتركيب أجهزة على جهاز الصراف الآلي للحصول على تفاصيل حساب البطاقة وتسجيل الرقم السري الذي قام العميل بإدخاله. ثم يتم استخدام هذه المعلومات لإجراء عمليات سحب نقدي غير مشروعة باستخدام بطاقات مزورة.

2/ النظر من أعلى الكتف: يتظاهر المجرمون بمساعدة العملاء في استخدام أجهزة الصراف الآلي، ولكنهم في الواقع يحفظون الرقم السري.

3/ إدارات النقد التشغيلي: في الوجهات السياحية التي يوجد فيها عدد قليل من البنوك وأجهزة الصراف الآلي يعرض المجرمون تقديم خدماتهم إلى السياح حيث يقومون بتوجيههم إلى تجار محليين الذين يستخدمون أجهزة نقاط البيع لإصدار النقد. يقوم التاجر بمسح تفاصيل حساب البطاقة ويستخدم جهاز مزيف للحصول على الرقم السري لحاملي البطاقات. ثم يتم استخدام هذه المعلومات لإجراء عمليات سحب نقدي غير مشروعة باستخدام بطاقات مزورة.

النتائج:

مع التزايد المستمر في العمليات المصرفية في اجهزة الصرافات الإلكترونية وتزايد عدد البنوك و العمليات المصرفية فيها وتزايد عدد تلك الصرفات كما في الجدول التالي:

عدد المصارف في المملكة	30مصرف
عدد فروع المصارف في المملكة	1941 مصرفا
عدد اجهزة الصرافات الالية	حوالي 4884ا صراف آلي
إجمالي قيمة السحوبات من تلك الصرفات	141 مليار ريال

بيانات الجدول أعلاه في 2022م .

إلا أن عدد الشكاوى المتعلقة بتلك التعاملات رغم كبر حجمها وضخامتها لا تزال في حدوده معقولة مقارنة مع ضخامة عدد الصرافات وعدد البطاقات نسبة إلى ضخامة عدد وحجم العمليات.

وعلى الرغم من أن المملكة العربية السعودية هي حالياً في المرتبة الأولى بين جميع الدول العربية في التعامل بالشبكة العنكبوتية إذ تجاوز عدد الذين يستخدمونها أكثر من 18 مليون مستخدم ، الأمر الذى أدي إلى ازدياد عمليات الاحتيال الإلكتروني مع تلك المعاملات المالية الضخمة المتبادلة عبر الشبكات العنكبوتية محلياً وخارجياً .

ومع ذلك فأن البنوك السعودية تتبع العديد من الوسائل وطرق الحماية مثل المعيار الثنائي للتحقق من هوية الشخص ،حيث يقوم البنك يقوم بإرسال رقم سري آخر (إضافي) إما من خلال جهاز تشفير يوفره البنك للعميل أو من خلال إرسال رسالة نصية إلى رقم تلفون العميل المعتمد لدى البنك المعني.

كم تلتزم البنوك السعودية بتطبيق المعايير الأمنية الصارمة في جميع مجالات أمن المعلومات المصرفية وتستخدم البنوك السعودية الأنظمة الدفاعية القوية والمتكاملة لتحصينها من أي سرقة أو اختراق .

كم تقوم المملكة العربية السعودية بتنويع وسائل الحماية مما يصعب عمليات اختراقها مستخدمة أفضل وأحدث الوسائل والبرامج العالمية ((للحماية من الفيروسات والاختراقات)) في ذلك ، كما أنها تستخدم ما يعرف بالجدران النارية Fire Walls بمستويات وقدرات متعددة.

كذلك من بين الاحتياطات الأمنية المعلوماتية التي توفرها المصارف السعودية لعملائها لدى إنجازهم تعاملاتهم المصرفية سواء عبر الهاتف المصرفي أم من خلال أون لاين، ما يعرف بـ "المعيار الثنائي للتحقق من الهويةTwo Factor Authentication "، الذي هو نظام إلكتروني يسمح للعميل بالدخول إلى خدمة الهاتف المصرفي والـ "أون لاين" بشكل أكثر أماناً، وذلك بإرسال رقم سري آخر أو إضافي للعميل إلى جانب رقمه السري للسماح بتمرير العملية المصرفية وتنفيذها عبر أنظمة المصرف.

ومن بين الاحتياطات الأمنية كذلك التي تتمتع بها المصارف السعودية بهدف توفير مستوى عال من الحماية والسرية للبيانات الخاصة بعمليات بطاقات الدفع (بطاقة الصراف الآلي والبطاقات الائتمانية) والتقليل من مخاطر الاحتيال، اعتمدت المصارف جميعها استخدام المعيار الأمني لصناعة بطاقات الدفع (PCI DSS-Payment Card Industry Data Security Standard)الذي أقره "مجلس المعايير الأمنية لصناعة بطاقات الدفع" المعني بوضع المعايير الأمنية لبطاقات المدفوعات عالمياً. وهذا المعيار الأمني يضفي المزيد من الأمن والأمان المعلوماتي للمعلومات المزود بها ذلك النوع من البطاقات.

كذلك إصدار بطاقات دفع مزودة بشرائح ذكيةSmart Chip ، التي توفر المزيد من الحماية المعلوماتية لذلك النوع من البطاقات مقارنة بالتقنية القديمة والتقليدية التي كانت تعرف بتقنية الشريط الممغنط.Magnetic Tape

كما أن مؤسسة النقد العربي السعودي (ساما) تبذل جهودا كبيرة في مجال أمن المعلومات للرفع من مستوى حماية المعلومات والتعاملات المصرفية الإلكترونية، حيث على سبيل المثال لا الحصر، تتمتع الشبكة السعودية للمدفوعات (SPAN) بمستوى مرتفع للغاية من الحماية المعلوماتية، وذلك على مستوى المصارف وجميع الأطراف ذات الصلة بالعمليات المالية، مثل مزودي خدمات الربط وشركات

توريد أجهزة نقاط البيع وشركات طباعة البطاقات المصرفية، ومقدمي خدمة الدفع بواسطة نقاط البيع. كما حصلت مؤسسة النقد على شهادة التوافق مع المعيار الدولي الخاص بصناعة بطاقات الدفع، إضافة إلى حصول جميع المصارف التي تقدم خدمات بطاقات الدفع في المملكة على ذلك المعيار، الأمر الذي يؤكد اتباع مؤسسة النقد خطوات كبيرة ومهمة للغاية في سبيل الرفع من مستوى أمن بيانات وعمليات بطاقات الدفع الخاصة بالعملاء والتعزيز من أمن المعلومات بشكل عام في القطاع المصرفي السعودي.

التوصيات:

اتضح لنا مما سبق أن المشكلة الخطيرة التي تجتاح العالم بأثره مع التطور المستمر في عالم الاتصال والإنترنت مما يستلزم وقفة الجميع للتصدي لها ، فللحد منها يستلزم تطبيق حزمة من الإجراءات والمعالجات نبرزها فيما يلى :

أولاً : دور المصارف :-

1/علي المصارف السعودية أن تقوم باستخدام التطبيقات والأنظمة الحديثة لحماية بياناتها ومعلوماتها وعملائها .

2/ كما علي البنوك التأكد من أن أي استخدام للمعلومات في حواسبها في حدود الصلاحيات المحددة والممنوحة للموظفين فقط.

3/ التأكد من أن جميع البرنامج المستخدمة في التشغيل هي برامج أصلية .

4/التأكد من أن جميع الملفّات أصلية ومناسبة لحفظ بيانات العمليات ،كما يجب عمل نسخ منها لمزيد من الحماية .

5/ كذلك وجود مجموعة للرّقابة تقوم بتحقيق الرّقابة على البيانات التي سوف يتم تشغيلها ، والتأكّد من صحّة نتائج التشغيل ، ومن أن الأشخاص المصرّح لهم باستلام هذه النتائج هم فقط الذين يتسلّمونها دون غيرهم.

6/ التأكد من سرية كلمة المرور للدخول للجهاز ، وتغيرها بشكل دوري وسرى .

ثانياً : دور القانون :

1/ سن قوانين وتشريعات رادعه .

2/ وضع إجراءات تنظيمية لحصر ومتابعة وتنظيم عمل مقاهي الإنترنت داخل المملكة، حيث إن جميع أنواع جرائم المعلومات التي ترتكب داخل المملكة ولا يمكن ضبط مرتكبيها تكون بسبب ارتكابها من أجهزة حاسوبية عامة في مقاهي الإنترنت، .

3/ العمل على وجود تعاون عربي ودولي لمنع الاعتداء الإلكتروني الصادر من خارج المملكة، ولاقتفاء أثر مرتكبي الجرائم الإلكترونية عبر الشبكات الدولية.

ثالثا : دور العميل :

1. معلوماتك وبيانتك الشخصية وكلمات السر خط أحمر لا تصرح بها لأي شخص كان .

2/ حمل برامج أصلية من مواقعها الأصلية

3/ احذر البريد المجهول الهوية

4/ أستخدم برامج مضادة للفيروسات.

5/ استخدم رقم سري بعيد كل البعد عن أي رقم مرتبط بك وغيره بصورة منتظمة.

6/ راقب تعاملاتك المصرفية وكشف حسابك وتابعها دورياً.

7/ لا تقبل أي مساعدة من شخص غريب في جهاز الصراف الآلي عدا موظف البنك.

8/لاحظ لو كان هناك تغيير في جهاز الصراف بخلاف ما كنت معتاد عليه .

9/ حاذر من الأشخاص الذين يقفون علي مقربة منك عند السحب والإيداع وغطي رقمك السري عند ادخاله.

10/لا تحمل رقمك السري مكتوباً أبداً بل أحفظه أحفظ الرقم السري ولا تكشفه لأي شخص مهما كان .

رابعاً : دور الإعلام :

يجب أن يجب الإعلام دوراً هاماً في توعية المواطنين بمخاطر الاحتيال الإلكتروني .

كما يجب أن تلعب البنوك دوراً هاماً في ذلك((بالتنسيق مع الجهات الإعلامية)) بأن تقوم في كل عام بتنفيذ حملات توعية مصرفية على مستوى المملكة، تستهدف من خلالها إحاطة عملائها كافة وبقية أفراد المجتمع بالأنماط الجديدة لعمليات الاحتيال المالي والمصرفي وسبل الوقاية منها.

المراجع:

– احمد ،عبد الناصر طلب حسن : ظاهرة الاختلاسات في الجهاز المصرفي. دار عزة للنشر 2006م ، الخرطوم ،ط اولي.

–أبوغابه ، سمير احمد ، المبادئ والاتجاهات الحديثة في المراجعة.

– منصافي، مُحَّد صالح ، التدقيق والأمان والرقابة، اتحاد المصارف العربية 2010، ط 3 .

المراجع الأجنبية:

TURVEY 1946 2ALL .E.R.60.Cross and jones cases on Criminal law.R.V

BRANDT AALLEN OP CIT

المواقع الإلكترونية:

* مركز التميز لأمن المعلومات: (coeia.edu.sa)
* Trend Micro:

(us.trendmicro.com)

* مدينة الملك عبد العزيز للعلوم والتقنية:

(/http://www.kacst.edu.sa)

* هيئة الاتصالات وتقنية المعلومات:

http://www.alriyadh.com/2012/06/10/article743156.html

صحيفة الرياض

www.samba.com/ar/security-center/phishing-faqs.html

البنك السعودى الامريكي

www.google.com.sa/search?qaqs=chrome.1.69i57j0l5.3928j0j4&sourceid=chrome//:

الإقتصادية