تحديات الأمن السيبيراني لأنظمة المعلومات في البنوك والمؤسسات المالية.

Cyber security challenges for information systems in banks and financial institutions.

شايب محمد
Chaib Mohammed
جامعة فرحات عباس سطيف -1-
mchaib@univ-setif.dz

حمادي موراد
Hamadi Mourad
جامعة فرحات عباس سطيف -1-
mourad.hamadi@univ-setif.dz

Received:19/05/2023 Accepted: 23/06/2023 Published:31/07/2023

ملخص:

تسلط هذه الدراسة الضوء على الجرائم الإلكترونية وأمن المعلومات المالية في القطاع المصرفي والمالي، حيث يتناول المحور الأول مقدمة حول الجرائم الإلكترونية في البنوك والمؤسسات المالية وحجمها عالميا وأنواعها المختلفة، أما المحور الثاني فقد تعرض لمصادر وتحديات الخطر في البنوك والمؤسسات المالية.

وتقدم الدراسة معايير أمن وشفافية نظم المعلومات المالية والمصرفية في المحور الثالث، وأخيرا تناولت بعض النصائح والتوجيهات المقدمة للعملاء للتعامل مع النشاط الإلكتروني للمساهمة في ضمان أمن المعاملات المصرفيّة الإلكترونية. وهذه الاجراءات الأمنيّة من شأنها أن تساهم في حماية الأفراد الذين يستخدمون الخدمات المصرفية عبر الإنترنت للحد من سرقة المعلومات الشخصية أو اختراق الحساب المصرفي للعميل.

الكلمات المفتاحية: الأمن السيبيراني، نظم المعلومات، البنوك، المؤسسات المالية.

تصنيف JEL: K24، L86، G21.

Abstract:

This study has spotted the light on the electronic crimes and the safety of the financial data in the banking sector. The first unit tackled an introduction about the electronic crimes in both of the financial institutions and banks, and its different kinds and its global size as well. For the second unit, I have talked about the resources and risks challenges in the financial institutions and banks.

This study also gives the safety standards and the transparency of data and banking systems in the third unit. At last, I have tackled some pieces of advice and instructions given to the customers in how to deal with the recent electronic activity to contribute in the banking transactions safety. And these security measures can protect people whom use e-banking to limit the personal data theft or the piracy of the agent's bank account.

Keywords: Cyber Security, Information Systems, Banking, Financial Institutions.

Jel Classification Codes: K24, L86, G21.

المؤلف المرسل: شايب محمد، **الإيميل:** MohammedChaib19@yahoo.fr

المقدمة:

تمكنت الخدمات الإلكترونية المتوفرة عن طريق الإنترنت أن تقدم فرصا هائلة للبنوك والمؤسسات المالية، حيث أتاحت لها التوسع في خدماتها ومنتجاتها المصرفية والمالية، وفي خلق فرص تنافسية كبيرة في أسواقها من خلال الاستمرار في جذب الودائع ومنح الائتمان بصورة أكبر، وتقديم خدمات ومنتجات مصرفية جديدة، ما أنعكس على تقوية وضعها التنافسي في السوق. وتعد الإنترنت نقطة دخول أساسية للبرمجيات الخبيثة إلى الحواسيب.

وفي ظل تطور التقنية وانتشار المخاطر فالتقنية رغم ما قدمت من خدمة جليلة للإنسان في العصر الحديث إلا أنها وكأي اختراع آخر لها محاسنها الكثر ولها سلبياته الخطيرة، إذا لم يتم التعرف عليها والعمل على تفاديها. فلو أخذنا مثلاً التقنيات البنكية من خلال الخدمات الإلكترونية البنكية، لوجدنا أنه ورغم أن كل هذه الخدمات تعمل على راحة عملاء البنوك وتركز على أن تخدمهم في وقت قصير وفي أماكن متعددة الصراف الآلي ونقاط البيع مثلاً إلا أن هذه الخدمات لها أيضاً مخاطر يمكن أن تؤدي إلى ضياع أموال العملاء.

ولهذا أصبح لأمن أنظمة المعلومات أهمية قصوى استوجبت اهتمام البنوك والمؤسسات المالية والمؤسسات الحكومية والخاصة والأفراد، وتأهيل العنصر البشري في هذا المجال.

_ أهمية وإشكالية الدراسة: كشفت إحصاءات أجريت بواسطة نظام رصد المخاطر عبر شبكة كاسبرسكي للأمان السحابية مثلا أن متصفحي الإنترنت يواجهون نحو هجمة إلكترونية كبيرة في الساعة أو في الدقيقة. وعلي هذا الأساس فإن تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات سوف يعزز إطار الطمأنينة الذي يشمل أمن المعلومات وأمن الشيكات وصون الخصوصية والسرية وحماية المستخدم المالي والمصرفي، مما يعتبر شرطا مسبقا لإنشاء نشاط مالي ومصرفي الكتروني.

وإن إطلاع البنوك والمؤسسات المالية بتبني وسائل الحماية يؤكد على إدراكها التام لأهمية أمن انظمة المعلومات المصرفية والمالية، وضرورة مواجهة التحديات التي أفرزتها العولمة، وما صاحبها من تطور كبير في التقنيات المصرفية. وتدور القضية الرئيسية ونقاط الضعف حول مشاركة واندماج العنصر البشري في البنك والمؤسسة المالية الذي يأتي غالبا عن غير قصد.

ومن هنا جاءت الحاجة للتعريف بأمن المعلومات والحديث عن أهم تحديات مصادر الخطر بالنسبة لعملاء البنوك والمؤسسات المالية وطرق تجنبها. من خلال محاولتنا الإجابة على الأسئلة التالية:

_ ما حجم الجرائم الإلكترونية التي تحدث في البنوك والمؤسسات المالية، وما هي أنواعها؟

_ كيف يمكن تدمير نظام المعلومات الخاص بالبنك والمؤسسة المالية؟

_ ماهي أهم طرق الوقاية من الجرائم الإلكترونية؟

_ ما هي مختلف النصائح والتوجيهات الأمنية المقدمة للعنصر البشري المتمثل في العميل المصرفي المستخدم والموظفين على حد سواء؟

ولمناقشة هذه الدراسة تم تقسيمها إلى المحاور التالية:

المحور الأول: الجرائم الإلكترونية في البنوك والمؤسسات المالية.

المحور الثاني: تحديات ومصادر الخطر في البنوك والمؤسسات المالية.

المحور الثالث: أمن المعلومات المصرفية والمالية.

المحور الرابع: نصائح وتوجيهات أمن أنظمة المعلومات بالنسبة للعملاء والمستخدمين.

المحور الأول: الجرائم الإلكترونية في البنوك والمؤسسات المالية

إن خطر النشاط الإلكتروني الإجرامي هو أحد المواضيع الأكثر أهمية في مجال أمن المعلومات للسنوات القليلة الفائتة، وسنتطرق في هذا المحور الأول إلى:

1_ حجم الجرائم الالكترونية عالميا:

_سنة 2011: كانت الفاتورة الإجمالية لجرائم [1] أمن المعلومات عالميا وعربيا في 2011 وحده تقدر بحوالي 388 مليار دولار أميركي [2]. أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فقدرت بحوالي 114 مليار دولار [3]. ومعنى ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين، والتي قدرت بحوالي 288 مليار دولار، واقتربت من قيمة السوق العالمية للمخدرات عموما اين وصلت إلى 411 مليار دولار، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة "اليونيسيف" بحوالي 100 ضعف، حيث وصلت ميزانيتها الى 3.65 مليار دولار، كما تعادل هذه الخسائر ما تم إنفاقه خلال 90 عاما على مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في 38 عاما.

وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة، تأثر بها 589 مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 9% من إجمالي سكان العالم [4].

ووفقً لنتائج تجارب قدمها تقرير "نورتون لجرائم الإنترنت سنة 2012 ما يزيد عن 13 ألف مستخدم بالغ في 24 دولة، قام بحساب التكاليف المباشرة المرتبطة بجرائم الإنترنت الاستهلاكية العالمية في الولايات المتحدة والتي بلغت نحو 110 مليار دولار أمريكي* على مدى الأشهر 12 الماضية [5].

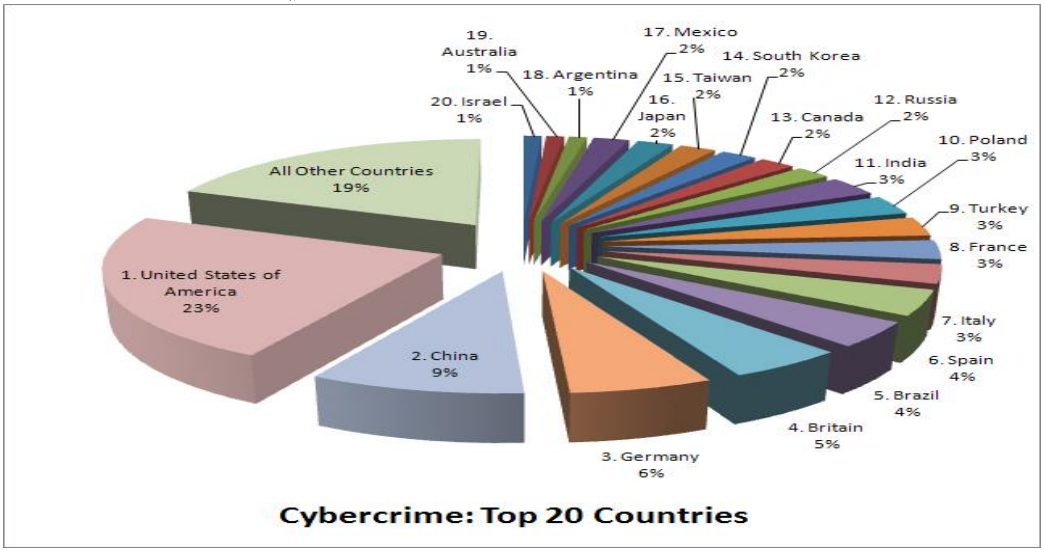
وأكد التقرير سقوط 18 شخص بالغ كل ثانية كضحيةً لجرائم الإنترنت أي ما يعادل 560 مليون ضحية في السنة و1,5 مليون ضحية وأكثر في اليوم، ما يؤدي لسقوط أكثر من مليون ونصف شخص ضحية لجرائم الإنترنت كل يوم على المستوى العالمي، حيث يبلغ متوسط الخسارة في التكاليف المالية المباشرة ما يعادل آنذاك 197 دولار أمريكي لكل ضحية في جميع أنحاء العالم، وتبلغ تكلفة جرائم الإنترنت الاستهلاكية ما يعادل تكلفة أسبوع واحد من الاحتياجات الغذائية لأسرة مكونة من أربعة أشخاص في الولايات المتحدة.

وفي الأشهر 12 الماضية، عانى حوالي 556 مليون بالغ حول العالم من جرائم الإنترنت، وهو عدد يفوق كامل سكان الاتحاد الأوروبي. ويمثل هذا الرقم 46 بالمائة من عدد البالغين على الإنترنت ممن سقطوا ضحية لجرائم الإنترنت في الأشهر الاثني عشر الماضية، وتأتي هذه النتائج متساوية مع نتائج عام 2011 45 بالمائة [6].

وقد توزعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار، وجرائم الاحتيال والنصب والاصطياد (الحصول على معلومات بنكية سرية)، والجرائم المتعلقة باختراق الهواتف المحمولة*.

كما يظهر مسح سنة 2012 زيادة في عدد الأشكال "الجديدة" لجرائم الإنترنت مقارنة بعام 2011، كتلك الموجودة على شبكات التواصل الاجتماعي أو الأجهزة النقالة، وهي إشارة على بدء مجرمي الإنترنت بتكثيف جهودهم على هذه المنصات ذات الشهرة المتزايدة. وقد سقط واحد من بين خمسة بالغين على الإنترنت (21 بالمائة) ضحايا لجرائم الإنترنت على شبكات التواصل الاجتماعي أو الأجهزة النقالة، وسقط ما نسبته 39 بالمائة من مستخدمي شبكات التواصل الاجتماعي ضحايا لجرائم الإنترنت [7]. والشكل الموالي وضح توزيع الجرائم الإلكترونية حول العالم.

الشكل رقم (01): توزيع الجرائم الإلكترونية حول العالم في 20دولة



Source : Enigmasoftware :" **Top 20 Countries Found to Have the Most Cybercrime",** **(http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/)**.

من خلال الشكل أعلاه يتضح أن الجرائم الإلكترونية في العالم ي عشرين دولة تتصدر الولايات المتحدة الامريكية القائمة بنسبة 23% والصين بـ 9 % ثم ألمانيا بـ 6 % ويتوقع مستقبلا أنه سيستمر نمو التطوير التكنولوجي والقدرة على مهاجمة وشل المواقع الإلكترونية بشكل مذهل، حيث تتزايد نسب المستخدمين الذين يتعرضون لجرائم إلكترونية عاما بعد عام، مع تزايد النطاقات الخطرة التي تحتوي على ملايين المواقع المشبوهة التي قد تزرع برامج ضارة في أجهزة المستخدمين.

هذا وتستخدم العديد من المصطلحات في جرائم نظم المعلومات والتي يكثر تداولها واستخدامها من قبل القارئ، منها: قرصنة البرامج، أحصنة طروادة، المقتحم، الفيروس، المتسلل Hakers، جريمة الإنترنت [8].

_سنة 2022: وقد وفرت الانتشار المستمر للحياة الافتراضية أرض خصبة لمجرمي الإنترنت – أكثر من 415 مليونًا البالغون في 10 دول (Australia, Brazil, France, Germany, India, Italy, Japan, New Zealand, United Kingdom, United States) واجهوا جرائم الإنترنت في 12 شهرًا الماضية (2021)، هذه الحوادث المالية و آثار التموج العقلي على أولئك الذين يعانون منها. من بين أولئك الذين عانوا من جرائم الإنترنت في الماضي عام، تم قضاء ما مجموعه 4.4 مليار ساعة في محاولة حل المشكلات التي تم إنشاؤها [9].

في المتوسط ، أكثر من 550 مليون مستهلك على مستوى العالم تعرضت لجريمة إلكترونية؛ 415 مليون يقولون إنهم كانوا ضحية خلال الـ 12 شهرًا الماضية. تعرض أكثر من نصف المستهلكين لجرائم إلكترونية، وأكثر من 1 من كل 3 سقطوا ضحية. وأكثر من 81 مليون مستهلك تعرضوا لسرقة الهوية العام الماضي. من أولئك الذين تعرضوا لسرقة الهوية، تم إخطار 2 من كل 5 حولها من قبل مصدر خارجي. ومن أجل 81 مليون بالغ على مستوى العالم كانوا ضحايا للهوية السرقة في عام 2021، جميعهم تقريبا من ذوي الخبرة المالية[10].

2_ تدمير أنظمة المعلومات الخاصة بالمؤسسات المالية: لتدمير نظام معلومات الخاص بالبنك والمؤسسة المالية سواء كليا أو جزئيا لابد من اختراقه أولا، ولكي تتم عملية الاختراق لابد من وضع برنامج يتم تصميمه خصيصا لهذه العملية، ويعتبر برنامج حصان طروادة Trojan Horse * من البرامج الخطيرة التي تستخدم في عمليات اختراق نظام المعلومات الخاص بالمؤسسات المالية، وتكمن خطورة هذا البرنامج في كونه يتيح للمخترق أن يحصل على كلمة السر Pass Word للدخول في هذا النظام [11].

ويعتبر أي تعد أو تخريب وسوء استعمال للحاسب ومعداته أو ما يتصل به أو وسائل التخزين تهديد لأمن المعلومة أو الوثيقة الإلكترونية. وازدادت الخطورة على أمن المعلومات بتطور تقنية الاتصالات بين مراكز المعلومات في العالم وشبكاتها المتطورة لتشكل شبكة هائلة لتناقل المعلومات والبيانات ومعالجتها. الشيء الذي فتح المجال للعابثين من المخربين وقراصنة المعلومات للوصول إلي المعلومات والبيانات والعبث بها أو سرقتها أو تخريبها.

3_ الانتقال من الفيروسات إلى الجرائم الإلكترونية: في الماضي، كانت الحواسيب تتعرض بشكل عام لهجمات الفيروسات والبرامج الدودية. الهدف الرئيسي لهذه الفيروسات هو الانتشار؛ إلى جانب ذلك هناك برامج صممت لتلحق الضرر بالملفات والحواسيب. بإمكان وصف هذا البرامج الخبيثة بـ Cyber Vandalism أو التخريب الإلكتروني[12]. ومن أحدث واخطر الفيروسات عالميا على سبيل الذكر لا الحصر.

_ برامج Flame: اكتشف هذا البرنامج الخبيث بفضل جهود خبراء كاسبرسكي لاب، الذين قاموا بالتحري عنه بطلب من الإتحاد الدولي للاتصالات*، وكالة الأمم المتحدة المعنية بتكنولوجيا المعلومات والاتصالات. وقد شخّص البرنامج الخبيث، الذي أطلق عليه Worm.Win32.Flame بواسطة المنتجات الأمنية من **كاسبرسكي لاب**، وهو مصمم ليقوم بالتجسس الإلكتروني. إذ بإمكانه سرقة المعلومات القيمة، بما فيها البيانات حول الأنظمة المستهدفة، الملفات المخزنة، معلومات الاتصال وحتى المحادثات الصوتية. وينتمي Stuxnet وDuqu إلى سلسلة واحدة من الهجمات التي أثارت القلق حيال الحرب الإلكترونية في العالم أجمع. ويبدو أن Flame هو مرحلة أخرى في هذه الحرب وإنه من الهام أن نتفهم أن مثل هذه الأسلحة الإلكترونية قد تستخدم بسهولة ضد أي بلد. وبخلاف الحروب التي تستخدم فيها الأسلحة العادية، تكون الدول المتطورة هي الأكثر تعرضا للاستهداف في هذه الحالة.

_ برامج التجسس Spyware : يمكن تعريف برامج التجسس Spyware بأنها برامج يتم تحميلها على أجهزة الكمبيوتر بهدف جمع معلومات حول العميل أثناء تصفحه لشبكة الإنترنت. وعادة، يتم تحميل هذه البرامج بموافقة المستخدم أو دون موافقته أثناء تحميل إحدى الألعاب أو البرامج...الخ، والتي تعرض عليه تحديث الكمبيوتر أو زيادة سرعة معالجه أو تحسين أدائه. وتسعى برامج التجسس عادة إلى الحصول على كلمات السر، والمعلومات الشخصية، ورقم بطاقة الائتمان. وتاريخ تصفح الإنترنت.. الخ. كما يمكن أن تستعمل في الإطلاع على ملفاتك الشخصية، وتستخدم لفحص الملفات على القرص الصلب. كما أنها يمكن أن تؤدي الى البطء في جهاز الكمبيوتر الخاص بالعميل او المستخدم أو تعطله نظرا لحاجتها إلى مساحة كبيرة من الذاكرة عن طريق استهلاك موارد النظام، مما يؤدي إلى عدم استقرار النظام أو تعطله.

_ الاحتيال والتصيد (رسائل الفيشنج Phishing): الفيشنج عبارة عن رسائل بريد الكترونية ذات طابع احتيالي تدعي أنها صادرة عن مؤسسات وشركات معروفة بهدف تضليل المتلقي وإقناعه بضرورة الكشف عن المعلومات الخاصة به لاستعمالها في أغراض الاحتيال. وترد مثل هذه الرسائل إلى بريد المتلقي عادة، وتطلب منه زيارة أحد المواقع الهامة وإعطاء معلومات شخصية وحساسة مثل كلمات السر ورقم البطاقة الائتمانية أو الحساب المصرفي المالي.

ان مثل هذه المواقع زائفة ولا علاقة لها البنك والمؤسسة المالية الرسمية التي أعلنت عن مثل تلك المواقع على الرغم من تشابهها في الكثير من الصفات والشكل التصميمي والبرمجي. وبعد أن يقدم المتلقي تلك المعلومات والتفاصيل، يتم تحويلها وإرسالها إلى الشخص المحتال للاستفادة منها، وتوجيه المتلقي بعد ذلك إلى الموقع الصحيح.

إذن الفيشنج أو"التصيّد" هو عملية الاحتيال على الإنترنت، هي طريقة لسرقة الهوية والتي تحاول الاحتيال على المستخدم لكشف معلوماته الشخصية أو المالية على الإنترنت. وعادة المحتالون يستخدمون مواقع مزيفة، أو رسائل البريد الإلكتروني الخادعة التي تحاكي أنشطة الأعمال والعلامات التجارية من أجل سرقة بياناتك الشخصية، مثل: اسم المستخدم، وكلمة السر، وأرقام بطاقات الائتمان، ومعلومات الفواتير.

_ برامج Crimeware: هو نوع من البرامج الإجرامية التي يتم تحميلها خفية إلى الحواسيب. أغلب هذه البرمجيات هي أحصنة طروادة Trojan Horse *. وهناك أنواع كثيرة من أحصنة طروادة التي صممت لأغراض مختلفة. فمثلا هناك أدوات لرصد كل مفتاح تضغط عليه لدى الطباعة، بعضها تلتقط صورة صفحات الموقع لدى تصفحك مواقع البنك على الإنترنت، بعضها تحمل إلى جهازك شيفرات ضارة وغيرها تمكن المخترقين من دخول نظام التشغيل في جهازك. إن القاسم المشترك لكل منها هو قدرتها على سرقة البيانات الخاصة بالعميل مثل كلمات السر وإرسالها إلى مجرمي الإنترنت. وإن المعلومات التي يحصل عليها مجرمو الإنترنت تمكنهم من سرقة أمواله.

_ هجمات البرمجيات الضارة Ransomware: في السنوات الماضية ترك مرتكبي الجرائم الإلكترونية أساليب برمجيات الخداع القديمة مثل الاحتيال عبر البرامج المضادة للفيروسات المزيفة للتحول إلى هجمات الاحتيال المالي عبر هجمات البرمجيات الضارة Ransomware، ويتوقع أن يستمر هذا الوضع، بل ويصبح أكثر انتشاراً على مستوى العالم وبلغات متعددة، وهو ما يمثل تهديداً متزايداً لأمريكا اللاتينية، حيث تقوم هجمات الاحتيال المالي عبر البرمجيات الضارة Ransomware بإغلاق الحاسوب أو الجهاز أو الخدمات وتحفظ البيانات المرهونة أو حتى أنها تهدد بالدعوة القضائية إذا لم يقوم المستخدم بالدفع، فهي هجمات غاية في الخداع والمراوغة، حيث يتم دمجها بعمق داخل الحاسوب أو الجهاز وبعد ذلك يكون من المستحيل تقريباً على المستخدم العادي أن يستعيد السيطرة على النظام أو البيانات الخاصة به.

_ هجمات حجب الخدمة الموزعة Distributed Denial of Service **: تجدر الإشارة هنا إلى أن هجوم حجب الخدمة الموزعة DDoS، الذي يستهدف أحد البنوك التي توفر الخدمات المصرفية الإلكترونية، ليس أكثر من مجرد إزعاجٍ يتمثل في تعطيلٍ مؤقتٍ لصفحة الويب التابعة للبنك. التي تؤثر سلباً على مراكز البيانات والشبكات والتطبيقات.

فمثلاً، كشف التقرير السنوي الذي تصدره أربور نتوركس عن أمن البنية التحتية العالمي أن ربع جميع مزودي خدمات الاتصالات يتعرضون لهجمات حجب خدمة موزعة. لكن المدهش أن ما يقرب من ثلثهم لا يعرفون أصلاً بحدوث تلك الهجمات لأنهم لا يعتمدون على حل أمني مناسب.

على سبيل المثال: في عام 2011، كان هناك عدد 1.596.905 من هجمات ما يعرف بـ DDoS "**هجمات حجب الخدمة الموزعة**" مقارنة بعددها عام 2012 حيث بلغ 120.321.372.[13].

وعلى العموم هنا العديد من التهديدات التي يتعرض لها البنك والمؤسسة المالية ناهيك عن التي ذكرمناها فهناك: Email spam، spoofing، Pharming، War walking، War driving، ....[14]. وهناك كذلك Vishing ، Cross-site scripting (XSS)، Cyber Squatting، Bot Networks، SMS spoofing:، Email bombing، Sending malicious codes through email:، Insider threats[15].

المحور الثاني: تحديات ومصادر الخطر في البنوك والمؤسسات المالية

من أجل تحقيق القدر الأكبر من الحماية، يجب معرفة مصادر الخطر على أمن المعلومات وتجنبها، ومن أهم هذه المصادر: عموما تسريب كلمات السر، الفيروسات وبرامج التجسس، الاستدراج، سرقة الهوية[16]، وهي بالنسبة للبنك تحديات يومية يحاول التقليل منها وإضعافها بمختلف الطرق والأساليب.

1_ مصادر الخطر في البنوك والمؤسسات المالية: عديدة ومتنوعة ومن بينها:

_ الخطر الأول: تسريب كلمات السر: كلمة السر للتعريف بالعميل أو ما يسمى المستخدم في الوسائل الإلكترونية، وباقترانها باسم المستخدم تكون هي الهوية الإلكترونية التي تصرح له بالدخول إلى أنظمة الحاسب الآلي والشبكات، ومجالات استخدامها عديدة على سبيل المثال (الإنترنت، الصراف الآلي، الهاتف المصرفي..).

_ الثاني: الفيروسات وبرامج التجسس: الفيروسات هي برامج حاسوبية تتسلل للأجهزة دون علم المستخدم، الهدف منها تدمير الملفات أو تعطيل النظام أو بعض أجزائه أو سرقة بعض البيانات أو المعلومات، وتنتشر تلك الفيروسات [17] بطرق عديدة، منها: مواقع الإنترنت والبريد الإلكتروني، والوسائط المتنقلة مثل: الأقراص المدمجة CD والمرنة Floppy Disk وشرائح الذاكرة Memory Stick وغيرها.

وتعرف على أنها برامج تتسلل في أجهزة المستخدم أو العميل الغرض منها التجسس عليه وتقوم بعملية رصد على ما يتم في تلك الأجهزة من عمليات. وهي قادرة على سرقة المعلومات والأرقام السرية المستخدمة على الجهاز المستهدف

_ الخطر الثالث: الاستدراج: تتم بإرسال بريد إلكتروني مضلل للمستخدمين والعملاء بهدف التحايل عليهم بانتحال شخصية مصرفية أو شركة أو مسؤولي بطاقات ائتمان ومطالبة العميل بإرسال معلوماته لأن هناك مشكلة في حساب العميل أو في النظام، عندها تتم عملية الخداع وتتم سرقة المعلومة، وقد يصل التضليل إلى إقامة مواقع مزورة مشابهة للموقع الرسمي للبنك يتم من خلالها خداع العميل ومحاولة استدراجه ليكشف عن معلوماته.

_ الخطر الرابع: سرقة الهوية: ذلك بالحصول على معلومات العميل الشخصية واستخدامها، حيث يتم انتحال شخصيته والقيام بأي عملية مصرفية أو أي جريمة أخرى تعود بالفائدة على الفاعل، مثال ذلك سرقة معلومات البطاقة الائتمانية مثل: رقمها وتاريخ انتهائها ثم القيام بعمليات مصرفية عليها.

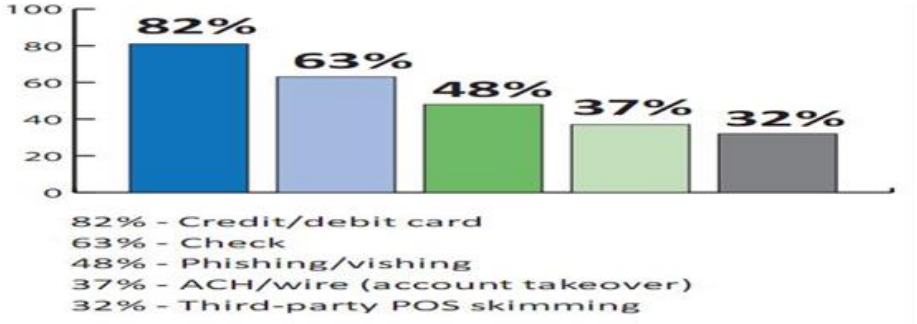
2_ تحديات أمن المعلومات في البنوك والمؤسسات المالية: يتمثل مصدر تحديات أمن أنظمة المعلومات الرئيسية التي تؤثر على امن المعلومات والبنوك والمؤسسات المالية فيما يلي:

_ زيادة أدوات ثغرات المهاجمة: تحتوي أدوات ثغرات المهاجمة على برامج خبيثة، والتي سريعاً ما تقوم بالتعرف على نقاط الضعف الإلكترونية ومهاجمتها، ثم تبدأ في الانتشار.

_ زيادة في تهديدات أمن أنظمة المعلومات التي تخص أجهزة المحمول: إن تبني تقنية NFC * أو ما يعرف بالتواصل قريب المدى لأنظمة الدفع عن طريق أجهزة المحمول هي ما تجعل من برامج أجهزة المحمول هدفاً شديد الجاذبية للجرائم الإلكترونية ذات التوجه المالي.

_ زيادة التطوير التكنولوجي للتهديدات سنة 2010: حيث أن البنوك من جميع الأحجام تستمر في نقل الخدمات والبنية الأساسية إلى الإنترنت والحوسبة السحابية. فسوف تتصاعد مشاكل هجمات حجب الخدمة الموزعة على العديد من برامج العمل، حيث أن لديها القدرة على شل البنية الأساسية بأكملها بشكل سريع للبنك والمؤسسة المالية. والشكل لموالي يوضح نسبة الجرائم الإلكترونية في وسائل الدفع المصرفية.

الشكل رقم (02): نسبة الجرائم الإلكترونية في وسائل الدفع المصرفية



Source : John P Mello Jr: "**Phishing in Top 3 Fraud Threats for 2010",** 20 January, 2011, (http://www.allspammedup.com).

من خلال الشكل أعلاه يتضح لنا أن نسبة الغش في وسائل الدفع سنة 2010 كانت كبيرا جدا في بطاقات القرض والخصم بنسبة 82%، ثم في الشيكات بنسبة 63%، ثم عمليات التصيد بنسبة 48% لتحتل المرتبة الأخيرة سرقة بيانات نهائيات نقاط البيع بنسبة 32%.

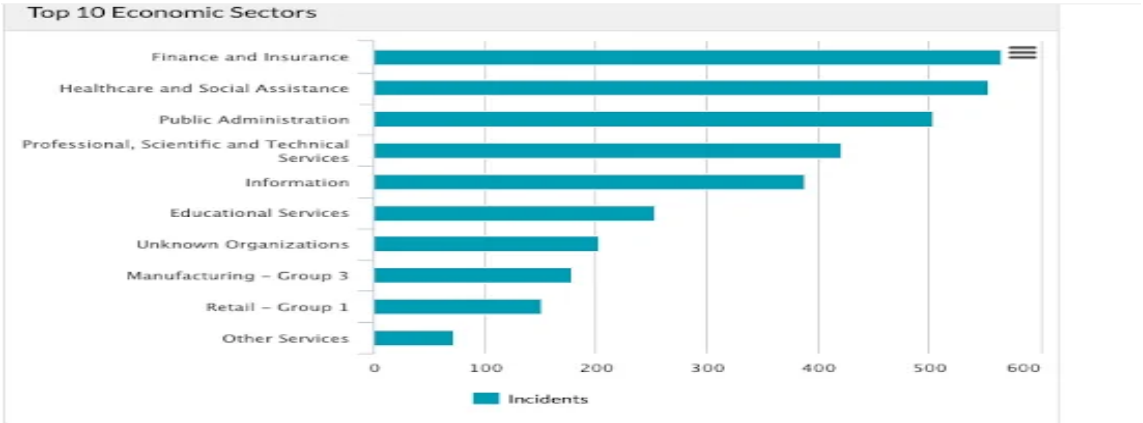
وحول حدود نمو النقود الإلكترونية فان انتشار طرق الغش والتزوير وجرائم المعلوماتية تعد العائق الرئيسي لانتشار النقود الإلكترونية. وهذا يلقي مسئولية كبيرة على المؤسسات المصدرة لبطاقات الائتمان الذكية والشيكات الإلكترونية وكافة اشكال النقود الإلكترونية لوضع نظام أمان فعال غير قابل لاختراق مجرمي المعلوماتية وقراصنة المعلومات [18].

وعليه فإن التطور الكبير الذي شمل مجالات التعاملات الإلكترونية بشكل عام والمصرفية منها بشكل خاص، واكبه للأسف، تطور غير مسبوق في أساليب الاحتيال المالي وعمليات الاختراق الإلكتروني، وتنبهت المؤسسات المالية والمصرفية على مستوى العالم إلى خطورة هذا الأمر وبادرت إلى اتخاذ إجراءات أمنية وتدابير احترازية لحماية أنظمتها التقنية، ومنع الوصول غير المشروع إلى المعلومات الخاصة بها وبعملائها.

_تهديدات المصارف والمؤسسات المالية 2022: إن عدد الهجمات عبر برامج أحصنة طروادة المصرفية لسرقة بيانات الدفع، تضاعف في عام 2022 مقارنة بعام 2021، حيث وصل إلى ما يقرب من 20 مليون هجوم. هذا العام، بالإضافة إلى هذه الحملة النشطة لسرقة بيانات الاعتماد المصرفية، لم يقف مجرمو الإنترنت ساكنين وطوروا مخططات احتيال جديدة. في يوم الجمعة الأسود على وجه الخصوص، استخدم المحتالون نوعًا جديدًا من مخططات التصيد لأول مرة لاستغلال خدمات "Buy Now Pay Later" (BNPL) هذه بعض النتائج التي توصل إليها تقرير "كيف تعرض العملاء للخداع في موسم الجمعة السوداء في عام 2022 الصادر عن Kaspersky والذي يهدف إلى توعية المستخدمين بالبقاء آمنين خلال موسم التخفيضات.

هذا وتستشهد تحليلات المخاطر الإلكترونية، التي تستوعب معلومات عن الانتهاكات التي تم الكشف عنها علنًا، بأن كيانات التمويل والتأمين هي القطاع الأكثر تعرضًا للاختراق في عام 2022. اعتبارًا من 9 ديسمبر 2022، تعرضت كيانات التمويل والتأمين في جميع أنحاء العالم لـ 566 انتهاكًا للبيانات، والتي بلغت حتى الآن لأكثر من 254 مليون سجل مسرب. يُعزى ما يقرب من 57 في المائة من هذه الخروقات إلى القرصنة العامة.بينما يمكن أن يُعزى حوالي 6.5 في المائة إلى Skimming (سرقة بيانات بطاقات الصراف الآلي). الشكل الموالي يوضح ذلك:

الشكل رقم (03):أهم 10 قطاعات اقتصادية تأثرت بانتهاكات البيانات (2022) وفقًا لتحليلات المخاطر الإلكترونية



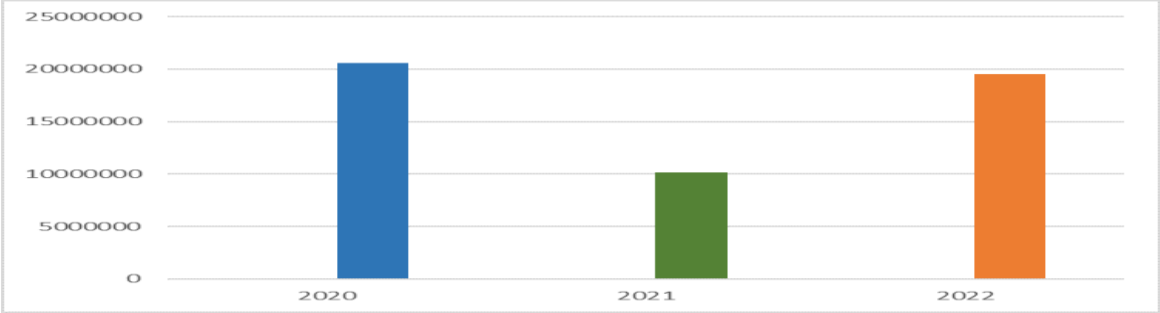
Source: flashpoint **:"Flashpoint Year In Review: 2022 Financial Threat Landscape",** (https://flashpoint.io).

لقد كانت جميع انتهاكات سرقة بيانات بطاقات الصراف الالي ناتجة عن الاجهزة المادية المثبتة على أجهزة الصراف الآلي، بدلاً من السرقة الإلكترونية. تُصنف هجمات Skimming، التي تنطوي على استخدام برنامج نصي ضار يتم حقنه في مواقع التجارة الإلكترونية المخترقة لسرقة معلومات بطاقة الدفع، على أنها قرصنة عامة في مجموعة البيانات هذه.

_ سرقة لبيانات باستخدام احصنة طروادة: تُستخدم أحصنة طروادة المصرفية على نطاق واسع في ترسانة مجرمي الإنترنت الذين يستفيدون من موسم المبيعات. بمجرد أن يتصفح المستخدم في متجر على الإنترنت، يحفظ حصان طروادة جميع البيانات التي يدخلها المستخدم في نماذج موقع الويب. وهذا يعني أن مجرمي الإنترنت يمكنهم الوصول إلى رقم بطاقة الائتمان أو الخصم وتاريخ انتهاء الصلاحية وCVV وبيانات اعتماد تسجيل الدخول إلى موقع الضحية. بعد الحصول على هذه المعلومات، قد يستخدمها المهاجمون لتفريغ الحساب المصرفي للمستخدم، أو استخدام تفاصيل بطاقتهم في عمليات الشراء أو بيع البيانات في متاجر الويب المظلمة.

بعد الانخفاض السريع في عدد الهجمات باستخدام أحصنة طروادة المصرفية في عام 2021، عاد مجرمو الإنترنت إلى هذا النوع من التهديد بقوة متجددة. ففي عام 2022، تضاعف عدد الهجمات مقارنة بنفس الفترة الزمنية في عام 2021. من يناير إلى نوفمبر. وفي نفس الوقت ننوه الى ان منتجات Kaspersky تمنع ما يقرب من 20 مليون هجوم. والشكل الموالي يوضح ذلك:

الشكل رقم(04):العدد الإجمالي لهجمات التروجان المصرفية، 2020-2022 (جانفي - أكتوبر)



Source: kaspersky Lab : "**Black Friday report: banking credentials theft doubled in 2022**", (https://www.kaspersky.com).

يجذب موسم المبيعات حتما انتباه المتسوقين وتجار التجزئة. ومع ذلك، فهو أيضًا وقت مفضل لمجرمي الإنترنت، الذين لا يترددون في جني الأموال من العملاء عبر الإنترنت. ينشئ مجرمو الإنترنت عروضًا مثيرة مزيفة وتنتهي صلاحيتها بسرعة، لذلك يجب على المستخدم الإسراع في الحصول على البضائع مجانًا أو بأقل سعر. هذا هو المكان الذي يلتقط فيه مجرمو الإنترنت العملاء، الذين يتوقون إلى الهدايا المجانية ولا ينظرون بعناية إلى الموقع الذي يدخلون فيه بياناتهم: التصيد الاحتيالي أو الموقع الأصلي.

ظهرت أحصنة طروادة المصرفية الجديدة التي تتنكر في شكل تطبيقات جوال مشروعة. بعض أشهر محللي أحصنة طروادة الذين لاحظوا في عام 2022 هم [19]:

_Xenomorph: عبارة عن حصان طروادة مصرفي تم اكتشافه في الأصل في فبراير 2022. تم إخفاء هذا البرنامج الضار داخل تطبيق "مدير يومي" يبدو شرعيًا داخل متجر تطبيقات الهاتف المحمول.

_Sova: عبارة عن حصان طروادة جديد نسبيًا للخدمات المصرفية عبر الهاتف المحمول تمت ملاحظته لأول مرة في عام 2021. منذ ملاحظته الأولى، لاحظ الباحثون الأمنيون أن البرامج الضارة يتم تطويرها وترقيتها باستمرار. في 10

سبتمبر، أصدر فريق الاستجابة لطوارئ الكمبيوتر في الهند (CERT-In) تحذيرًا استشاريًا للمواطنين ضد حملة إلكترونية جارية تستخدم Sova. يشير التحذير إلى أن Sova ظهرت لأول مرة للبيع داخل المجتمعات غير المشروعة.

_Teabott : هو حصان طروادة مصرفي يعمل كلوغر Keylogger [20] من خلال سرقة بيانات الاعتماد. ظهر Teabot في البداية في ماي 2021 مستهدفًا ضحايا أوروبيين ، على الرغم من أنه توسع منذ ذلك الحين ليشمل أيضًا أهدافًا في هونغ كونغ وروسيا والولايات المتحدة. تشمل أهداف Teabot التطبيقات المصرفية والتشفيرية والتطبيقات ذات الصلة بالاستثمار.

المحور الثالث: أمن المعلومات المصرفية والمالية

تعد المعلومات ومراكزها من أهم ركائز الوثائق الإلكترونية وأمنها وتزداد أهميتها بزيادة أهمية المعلومات التي تحتويها، وزيادة الاعتماد عليها في تيسير الكثير من الأعمال الاقتصادية والأمنية ومدي الاستفادة منها هذا بالإضافة إلي الأبعاد الأمنية والأهمية الاقتصادية للمعلومات المصرفية والمالية.

1_ تعريف أمن المعلومات: يعرف أمن المعلومات على أنه:

_ مجموعة الإجراءات والتقنيات المعنية بحماية المعلومات والمحافظة عليها من الضياع أو التسريب أو العبث بمضمونها، ويتم ذلك باستخدام الأدوات والوسائل الملائمة.

_ العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

_ المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

نستنتج من خلال التعاريف السابقة أن الهدف من أي برنامج أمن لنظام المعلومات حماية معلومات البنك والمؤسسة المالية المعنية، وتقليل المخاطر التي قد تؤثر علي توافر المعلومات وسريتها وسلامتها بمستوي مقبول ومحدد. ويتضمن برنامج أمن المعلومات الجيد توافر عنصرين رئيسيين، يتمثلان في تحليل المخاطرة وإدارة المخاطرة [21].

2_ المبادئ الأساسية لأمن المعلومات: يسعى المختصون في أمن المعلومات إلى ضمان تحقيق المبادئ التالية:

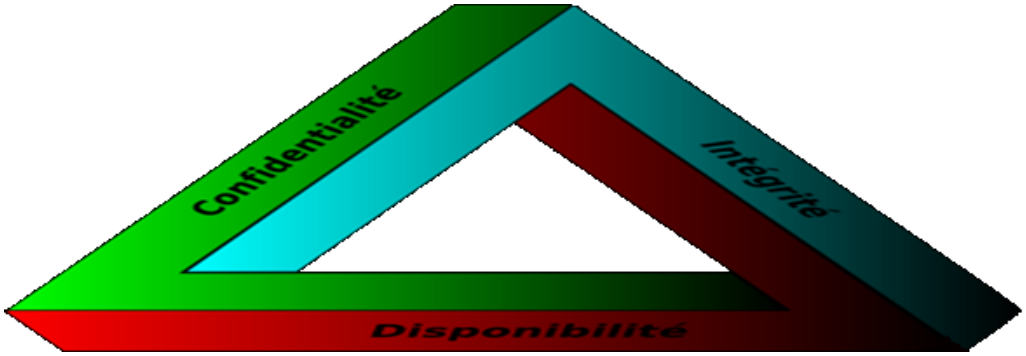
_ **سرية المعلومة Confidentiality** : حيث تحجب المعلومات عن الشخص غير المصرح له.

_ **صحة المعلومة Integrity:** حيث يتم التأكد من سلامة المعلومة والمحافظة عليها من العبث أو التغيير غير المصرح به.

_ **توافر المعلومة Availability:** حيث يمكن للأشخاص المصرح لهم الحصول المعلومة عند الطلب بسهولة.

تطلق عليها بالفرنسية Critères de sensibilité [22]، وهناك من يضيف، (Authenticity)، (Non-repudiation)، (dentification)، (Authorization)، (Accountability) و(auditability). والشكل الموالي يوضح معايير أمن المعلومات المتفق عليها عالميا.

الشكل رقم (05): معايير أمن المعلومات المالية والمصرفية



المصدر: من إعداد الباحثين.

3_ إدارة المخاطر المعلوماتية والجرائم الإلكترونية في البنوك والمؤسسات المالية: سنتطرق في هذا العنصر إلى:

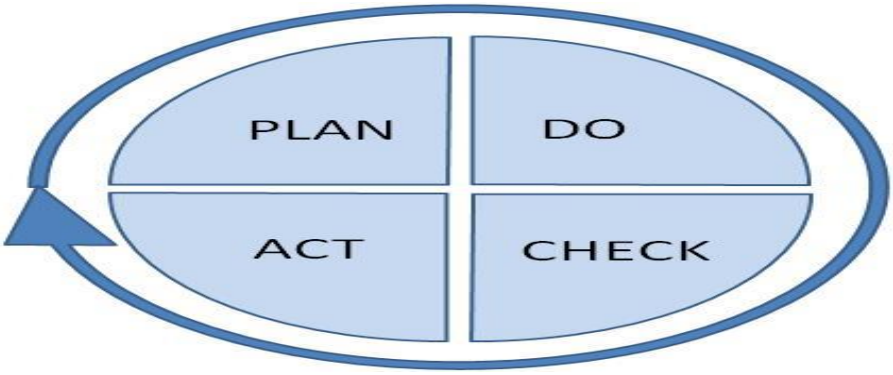
_ إدارة المخاطر: هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها المنظمة أو الشبكة المعلوماتية في تحقيق أهدافها، والحد والتقليل من نقاط الضعف إن وجدت، لتأخذ في الحد من المخاطر إلى مستوى مقبول، على أساس قيمة للموارد المعلومات إلى المنظمة".

_ عملية إدارة المخاطر هو تكرار العمليات الجارية ويجب أن يتكرر إلى ما لا نهاية لأن بيئة العمل المتغيرة باستمرار، والتهديدات الجديدة والضعف تظهر كل يوم.

نستنتج أن ادارة المخاطر على العموم هي اختيار التدابير المضادة (الرقابة)، ويجب أن توازن بين الإنتاجية، والتكلفة، وفعالية التدابير المضادة، وقيمة الموجودات وحماية البيانات في البنوك والمؤسسات المالية.

_ المراحل المتبعة في ادارة المخاطر الإلكترونية المصرفية: إن أهم الخطوات التي ينبغي أن تتخذها المؤسسة المالية أياً كان حجمها من أجل حماية المستخدم من الهجمات الإلكترونية هي معرفة أكثر أنواع هذه الهجمات المتنوعة وضوحًا وخطورة. ومن المهم أن تقوم بتعليم الموظفين كيفية التعرف على الفيروس والبرمجيات الخبيثة وتجنب جلبها إلى شبكة البنك والمؤسسة المالية دون قصد. وقد أظهر استطلاع حديث قامت به شركة **ديل سونيك وول** عن طريق زبائنها، أن نسبة 68 في المائة من إجمالي الشركات أشاروا في التقارير أن الموظفين لا يستطيعون التعرف على هجمات الاحتيال التي تصيب شبكة المؤسسة. والشكل الموالي يوضح كيفية حماية نظام المعلومات الإلكتروني المصرفي عموما.

الشكل رقم (06): حماية نظام المعلومات المصرفي والمالي



المصدر: من إعداد الباحثين

من خلال الشكل أعلاه والذي هو عبارة عن حلقة دائرية تعرف باسم (The Deming Cycle)[23]. يمكن القول أن أي خطر معلوماتي لابد من إدارته وفق أربعة خطوات:

_ تنفيذ عملية حماية المعلومات المصرفية يكون أولا من خلال تحديد السياسة الأمنية وتحديد هوية المخاطر ووضع أهداف السلامة.

_ ثم من الضروري وضع تدابير الأمن المحددة لتحقيق الأهداف التي تم وضعها مسبقا.

_ بعد التحقق من أن هذه التدابير تشمل القسم الأعظم من سلسلة أمن المعلومات وأمن النظام البنكي، لابد من المتابعة والمراقبة للتأكد من فعالية نظام الحماية الموضوع.

_ وأخيرا، تحليل النتائج وفقا لمستوى الأمن الذي يتحقق، وتحديد الموارد التي تتطلب تغييرات، ومن ثم متابعة تطور التهديدات الجديدة وتقديم تدابير السلامة.

واليوم تحرص الهيئات المالية من حيث الالتزام بمعايير الأمن والسلامة وتطبيق أفضل الممارسات Best Practices التي يمكن من خلالها تقليص المخاطر المرتبطة بمحاولات العبث بأنظمة البنوك والمؤسسات المالية المعلوماتية أو ببيانات العملاء ومعلوماتهم الشخصية.

المحور الرابع: نصائح وتوجيهات أمن أنظمة المعلومات بالنسبة للعملاء والمستخدمين

انطلاقا من حرص البنوك والمؤسسات المالية على ضمان أمن عملياتها وأنشطتها التي تتم عبر الإنترنت، فإنها تقدم لعملائها بعض النصائح الواجب اتباعها لتحقيق ذلك في العديد من الأمور.

1_ بخصوص أمن العمليات المصرفية الإلكترونية: تكون النصائح والتوجيهات على الشكل التالي:

_ أدخل مباشرة على موقع الإلكتروني للبنك باستخدام شريط الأدوات في المتصفح.

_ قبل الدخول إلى الموقع تأكد من أنك تتصفح الموقع الحقيقي البنك، ولا تتبع أي ارتباط يعرض عليك الدخول إلى موقع الإلكتروني للبنك، لتقليل احتمال تعرضك لهجمات القراصنة والبريد المتطفل Phishing.

_ استعمل برامج تصفح ذات ميزات أمان عالية، كتلك التي تقدم ميزة anti blocker واحرص على تحميل الإصدار 7.0 من برنامج إنترنت إكسبلورر أو أي إصدار أعلى منه.

_ تأكد من أن عنوان صفحة تسجيل الدخول يتغير من http:// إلى https://، ومن أن أيقونة الأمان التي تظهر وكأنها قفل بجوار الساعة تبدو في أسفل صفحة الموقع.

_ اضغط على أيقونة القفل بجوار الساعة للتأكد من إصدار شهادة التحقق لموقع البنك الإلكتروني.

_ بعد ذلك تأكد من أن كل التفاصيل الواردة في الشهادة تبين أنه قد تم إصدارها لموقع البنك الإلكتروني.

_ بعد الانتهاء من استخدام الموقع الالكتروني اونلاين، سجل خروجك من الموقع بشكل نظامي، ولا تقم فقط بإغلاق المتصفح وذلك بالضغط على الخروج من الموقع.

_ قم بتحديث حسابك المصرفي بالاتصال بمركز الاتصال إن تغيرت لديك أية معلومات كأرقام الهاتف الثابت أو الجوال.

_ سجل اشتراكك بخدمة الإشعارات عبر الجوال لتكون على علم بشكل مستمر بالعمليات التي تجري على حسابك المصرفي الإلكتروني أولا بأول.

_ راجع كشف حسابك بصورة دورية إما باستعمال الصراف الآلي أو بزيارة الموقع الإلكتروني الأصلي.

2_ بخصوص حماية كلمات السر والكمبيوتر الخاص بالعميل: تكون وصايا البنوك والمؤسسات المالية كالتالي:

_ استعمل كلمة سر قوية مؤلفة من 8 عناصر على الأقل ومبنية من تشكيلة من الأحرف والأرقام، ولا تستعمل كلمات سر بسيطة مثل اسم الأب أو الإبن أو الزوجة أو تاريخ الميلاد أو اسم دولتك ..الخ.

_ تذكر كلمة السر، ولا تحاول كتابتها في البريد الإلكتروني الخاص بك أو تخزينها في ذاكرة هاتفك المحمول.

_ اجعل اسم المستخدم وكلمة السر للبنك اونلاين مختلفة عن كلمات السر للمواقع الأخرى.

_ تأكد من أنك غير مراقب من قبل أي أحد بجوارك أثناء تسجيل الدخول وكتابة اسم المستخدم وكلمة السر أو رقم التعريف الشخصي الخاص بك أو إدخال أية معلومات ذات طابع شخصي.

_ احرص على ألا تجعل الآخرين يشاركونك فيها، حتى وإن كانوا موظفين في نفس البنك.

_ قم باختيار كلمات السر القوية المكوّنة على الأقل من 8 أحرف باستخدام مزيج من الأحرف الأبجدية والأرقام.

_ تجنّب كلمات سرّ سهلة التخمين مثل اسم الزوجة / الأطفال، تاريخ الميلاد، اسم حيوان أليف، اسم المدينة، ورقم سيارة.

_ احفظ كلمة السر الخاصة بك ولا تدونها في هاتفك الجوال أو البريد الإلكتروني.

_ يجب أن لا تكشف عن كلمة السر الخاصة بك / رقم التعريف الشخصي الخاص بك، إلى أي شخص حتى لو كان يدعي أنه أحد موظفي البنك.

_ لا تسمح لأي شخص أن يحتفظ أو يستخدم أو يعبث بكلمة السر الخاصة بك، المعطاة لك عن طريق جهاز رموز الأمان (توكن)، الذي ينتج كلمات السر الآمنة التي يقدمها لك البنك.

_ لا تكشف الرقم المتسلسل لجهاز رموز الأمان لأي أحد. وقم بإبقاء الجهاز في مكان آمن وبعيد عن متناول أي شخص .

أما بخصوص حماية جهاز الكمبيوتر فإنه يجب على العميل ما يلي:

_ تأكد من أن جهاز الكمبيوتر الخاص بك يحتوي على البرنامج المضاد للفيروسات، ومن أنه محدث باستمرار عبر الإنترنت وأن نظام التشغيل والمتصفح محدثين باستمرار وأنهما يمثلان آخر الإصدارات.

_ قم بتحميل الجدار الناري الشخصي Firewall لمنع الأشخاص غير المرخص لهم من الدخول إلى الكمبيوتر الخاص بك.

_ تأكد من تحديث الجدار الناري الشخصي Firewall بصورة مستمرة بما في ذلك ميزات الأمان وتحميل أحدث الإصدار البرمجية منه.

_ لا تختر ميزة الحفظ التلقائي Auto Save في المتصفح لتخزين اسم المستخدم أو كلمة السر عند الدخول إلى الحساب المصرفي الإلكتروني.

_ بعد الانتهاء من تصفح الموقع، قم بحذف الملفات المؤقتة Cookies وكذلك التاريخ History بالضغط على Tools ثم Internet Options للتخلص من أية دلائل أو إشارات إلى الموقع الذي يحتوي على حسابك المصرفي الإلكتروني وخاصة إن كنت تستعمل كمبيوتر ضمن مقهى إنترنت، أو كمبيوتر مشترك مع أشخاص آخرين.

_ عند استخدامك لويندوز، تأكد من تعطيل ميزة التشارك في الملفات وطباعتها. واحرص على عمل نسخ احتياطية من البيانات الخاصة بك، واستعمال أسلوب الترميز لحمايته.

_ التأكد من أن جهاز الكمبيوتر الخاص بك، تتوفر فيه أحدث برنامج لمكافحة الفيروسات، وأنه يتم تحديثها بشكل منتظم.

_ تأكد من أن نظام التشغيل للكمبيوتر الخاص بك، وكذلك برنامج المتصفح يتم تحديثها بأحدث التصحيحات الأمنية.

_ قم بمسح ذاكرة التخزين المؤقتة للمتصفح، وكذلك التاريخ بعد كل معاملة بحيث يتم إزالة معلومات حسابك، وخاصة إذا كنت تستخدم جهاز كمبيوتر مشترك، أو من مقاهي الإنترنت العامة.

_ قم بعمل نسخ احتياطية بشكل منتظم للبيانات الهامة.

_ فكر في استخدام تقنية التشفير لحماية البيانات الحساسة للغاية.

_ لا تستعمل أجهزة الكمبيوتر العامة أو التي يشترك فيها أكثر من شخص، ولا تستخدم أجهزة كمبيوتر عامة أو مشتركة.

_ تجنب الدخول إلى حسابك المصرفي عبر الإنترنت من خلال مقاهي الإنترنت أو أجهزة الكمبيوتر التي يشترك فيها أكثر

من شخص، ولكن إن اضطررت لذلك، فقم بتغيير كلمة السر الخاصة بك بأسرع طريقة ممكنة بعد انتهائك من جلسة التصفح.

_ ولزيادة الأمن أكثر، يطلب منك تغيير كلمة السر الخاصة بك على أساس منتظم.

3_ بخصوص الحماية في الشبكات اللاسلكية: تعطى للعميل النصائح التالية:

_ ضع كلمة سر للشبكة اللاسلكية الخاصة بك لحمايتها من أن تستعمل بشكل غير قانوني من قبل الآخرين، وقم بتعطيل البث الموجه لعنوان تلك الشبكة SSID-Service Set Identifier لمنع المتسللين والمتصفحين العشوائيين من الدخول إليها.

_ قم بتمكين ميزة الترميز عند نقل البيانات لحماية شبكتك اللاسلكية من التسلل، واسمح فقط لأجهزة الكمبيوتر المرخصة للدخول إليها فقط.

_ قم بتعيين كلمة سرّ لنقطة الاتصال اللاسلكية الخاصة بك، وامنع المستخدمين غير المصرح لهم من الدخول واستخدام الوصلة اللاسلكية.

_ قم بتعطيل البث لاسم الشبكة الخاصة بك (معرّف مجموعة الخدمات، SSID) من أجل منع المتصفحين العرضيين من الكشف والتوصيل مع الشبكة اللاسلكية الخاصة بك.

_ قم بتشغيل التشفير على نقل البيانات لحماية الشبكة اللاسلكية الخاصة بك. اسمح فقط للآلات المسجلة الخاصة بشبكة الاتصال اللاسلكية الخاصة بك.

4_ توصيات ونصائح عامة للعملاء والمستخدمين المصرفيين: على العموم من أجل حماية الأموال عند استخدام الخدمات البنكية الإلكترونية ينبغي عليك كعميل لأي بنك اتباع الإرشادات الأمنية التالية:

_ حماية الحاسبات الشخصية ببرامج أمنية أصلية (مكافحة فيروسات جدار أمني).

_ تحديث أنظمة التشغيل ومتصفح الإنترنت وبرامج الحماية بشكل دوري وآلي.

_ المسارعة في مراجعة البنك عند الشك في أي عملية بنكية وتغيير كلمة السر عند الشك في اكتشافها، مع استخدام كلمات سر يصعب توقعها وتغييرها بشكل دوري.

_ الحذر من وجود أشخاص على مقربة منك عند استخدام الصراف الآلي أو نقاط البيع أو عند استخدام شبكة الإنترنت في الأماكن العامة.

_ عدم الدخول إلى المواقع المشبوهة، حيث قد يتم تحميل برنامج في جهازك دون علمك.

_ تجنب الرد على رسائل البريد الإلكترونية المريبة والتي تطلب منك تحديث أو تأكيد معلوماتك البنكية أو الشخصية.

_ إبلاغ البنك عند الشك في تعرضك لأي عملية احتيال وذلك للسيطرة على المخاطر بأسرع وقت.

_ استخدام كلمة سر صعبة نسبياً بحيث تحتوي على حروف وأرقام، ويفضل تغييرها دورياً مع التأكد من حفظها وعدم كتابتها.

_ الحذر من إعطاء كلمة السر لأي شخص كان، حتى إن كان أحد موظفي القطاع المصرفي، أو الأقارب والأصدقاء.

_ عدم تخزين الأرقام السرية في متصفح الإنترنت آليا.

_ متابعة موقع البنك أو الأخبار للتحذير من أية مخاطر حديثة.

_ التأكد من أن أي رسالة بريدية إلكترونية تصلك على عنوانك بالبريدي الإلكتروني، هي مرسلة فعلا من البنك الذي تتعامل معه وذلك بالاتصال بالبنك.

_ تدقيق الكشوف البنكية والائتمانية بشكل دوري وإبلاغ البنك فوراً عند وجود عمليات مريبة.

_ المحافظة على البطاقات الائتمانية والإبلاغ الفوري حال فقدانها.

الخاتمة: بعد هذا العرض الوجيز نستنتج أن أمن المعلومات في القطاع البنكي والمالي يمثل منصة إستراتيجية لمناقشة التحديات الأمنية التي يواجهها القطاعين للتعرف على التحديات التي تواجهها البنوك والمؤسسات المالية كالاحتيال في الدفع والبطاقات والتهديدات التي تتعرض لها الخدمات المصرفية الالكترونية ومخاطر الصيرفة عبر الجوال.

وكنتيجة لبنوك الدرجة الأولى عالمياً في مجال الإنترنت البنكي من حيث نظم الأمن والحماية، تحصل البنوك على شهادة الآيزو ISO 27001 لأمن المعلومات المصرفية من منظمة الجودة العالمية ISO، وذلك نتيجة لامتلاكها وتطبيقها لسياسات تقنية رفيعة المستوي تتعلق بأمن أنظمة المعلومات، والتشغيل، والإجراءات المتعلقة بالتطبيقات الأمنية، بما في ذلك مواقع الأجهزة والبرامج. كما أن هذه خطوة تجعل البنك ينطلق بقوة في التطبيقات الجديدة التي ستغطي كافة مجالات نظم المعلومات بالبنك.

فعلى كبار موظفي القطاع المسؤولين عن تأمين وحماية البنى التحتية في مؤسساتهم المالية والاقتصادية. مع التركيز على مختلف الآليات وتعزيز الوعي وأفضل الممارسات لدى الخبراء والمهنيين الذين يعملون في هذا المجال. إضافة إلى توقيع مثلا اتفاقاً مع شركة NCR لتنفيذ عدد من المشاريع التكنولوجية البارزة، بما في ذلك الحلول المبتكرة للحماية من سرقة بيانات بطاقات الصراف الآلي Skimming، وذلك في إطار السعي لاستباق تحديات هذه الممارسة حيث يستخدم السارقون أجهزة الكترونية مخفية لسرقة البيانات الشخصية المخزنة على البطاقات وتسجيل الأرقام السرية وغيرها من المعلومات. وتجدر الإشارة كذلك إلى ضرورة العمل على تطبيق نظام أرقام الحسابات المصرفية الدولية (آيبان IBAN)، وذلك على حسابات عملاء المصرف. وذلك في سبيل إضافة مزيد من الأمان على عمليات التحويل وتسهيل معاملات الحوالات المصرفية الإلكترونية، والتي من شأنها أن تخفض من التأخير والتكاليف الإضافية المترتبة على استخدام أرقام خاطئة للحسابات.

ومن المتوقع ظهور أدوات لثغرات المهاجمة في السنوات القادمة تستهدف أنظمة ويندوز 8، وماك أو إس إكس، بالإضافة إلى أجهزة الهواتف المحمولة وخاصة تلك منها التي تعمل بنظام التشغيل أندرويد.

البنوك والمؤسسات المالية الجزائرية ستواجه تحديات كبيرة تستدعي الاستمرار في التحضير للعمل على تطبيق أفضل التقنيات والممارسات العالمية المتعلقة بأمن أنظمة المعلومات لمواجهة التهديدات وسد الثغرات الأمنية اذا ما اختارت تبني النمط الالكتروني في تقديم خدماتها المصرفية والمالية مستقبلا.

<u>الهوامش والاحالات:</u>

[1] أي سلوك سيئ متعمد يتسبب في الحاق الضرر بالضحية (أو يعرض الضحية إلى ضرر محتمل) أو ينتج عنه حصول الجاني (أو محاولته الحصول) على كسب أو فائدة لا يستحقها. فلكي نعرف جريمة نظم المعلومات فيجب أن نضيف الى هذا التعريف شرط ان تتضمن الجريمة: اتلاف المعلومات أو اساءة استخدامها. راجع: حسن طاهر داود، **جرائم نظم المعلومات**، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2010، ص. 23.

[2] اعتمد الباحثين في المعلومات الواردة بتقدير حجم جرائم المعلومات عالميا وعربيا على تقرير The Norton Cybercrime Report 2011 الصادر عن شركة **سيمانتك** العالمية المتخصصة في أمن المعلومات حول أوضاع جرائم المعلومات في عام 2011، والذي حمل عنوان "صورة إجمالية لأوضاع أمن المعلومات حول العالم.

[3] تقرير سيمانتك كوربوريشن **Norton Cybercrime Report 2011**، الصادر في سبتمبر 2011، (http://www.norton.com).

[4] نفس التقرير السابق.

* النتائج تقديرات استقرائية مبنية على نتائج من استطلاع رأي تم في 34 دولة بين الفئة العمرية من 18 إلى 64 سنة. وتعد التكلفة المادية للجرائم الالكترونية في السنة الماضية حوالي 111 مليار دولار أمريكي، وهي مبنية على عدد الضحايا في الشهور الـ12 الأخيرة في كل دولة (مضروبة) في 197 وهي التكلفة المتوسطة للخسائر من الهجمات الإلكترونية (لكل شخص بالدولار الأمريكي.

[5] تقرير سيمانتك كوربوريشن **Norton Cybercrime Report 2012**، الصادر في سبتمبر 2012، (http://www.norton.com).

[6] نفس التقرير السابق.

* يشار إلى أن أول اتفاقية للجرائم المعلوماتية وقعت ببودابست في 23 نوفمبر 2001، في حين وقع بروتوكولها الإضافي بستراسبورغ في 28 يناير 2003.

[7] نفس التقرير السابق 2012.

[8] حسن طاهر داود، مرجع سابق، ص. 25.

[9] Norton, **2022 *Norton* Cyber Safety Insights Report**, Global Results, anuary 2022.

[10] Idem.

[*] Tout le monde ou presque et même les plus jeunes connaissent aujourd'hui les variétés de virus qui sont les plus fréquents sur cyber espace. Les «**Trojan Horses** », « **Spywares** », « **Malwares** », « **dialers** ».

[11] Michelle Lafitte, **Les Systèmes d'Information dans les Etablissements Financières**, Presses de Jouve, Paris, France, 2000, P. 230.

[12] kaspersky Lab : "cyberthreats", (https://www.kaspersky.com).

[*] وسيستخدم الاتحاد الدولي للاتصالات شبكة ITU-IMPACT التي تضم 142 دولة وعدد من الشركات الكبرى المتخصصة في مجال الأمن الإلكتروني، بما فيها كاسبرسكي **لاب**، لإنذار الحكومات والأوساط التكنولوجية بوجود هذا التهديد الالكتروني وتسريع عملية التحليل التقني (http://me.kaspersky.com/news?id=7059).

[*] Un cheval **de** Troie (**informatique**) est un type de logiciel malveillant.

[**] **Denial-of-service attacks:** A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack).

[13] بغية الإطلاع على الوثيقة الخرائطية لإنتشار هجمات حجب الخدمة الموزعة عبر العالم، راجع الموقع الإلكتروني التالي:

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16461&view=map

[14] Kaustubh D, Gondhalekar, **Information Security Risk Management in Banks**, University of Wales, 9th February, 2007.

[15] Recommendations and Reports, **Report of the Working Group Working Group on information security, electronic banking, technology risk management and cyber frau,** Reserve Bank of India, Central Office Mumbai, January 14, 2011, P. 61.

[16] صقر بن ساعد العرابي الحارثي، **أمن المعلومات: نصائح وإرشادات لحماية عملياتك المصرفية**، العدد 6408 .الخميس 24 جمادى الأول 1432 هـ. الموافق 28 إبريل 2011، http://www.aleqt.com/2011/04/28/article_532209.html.

[17] هو عبارة عن برنامج له أهداف تدميرية يهدف إلى إحداث ضرر جسيمة بنظام الكومبيوتر. راجع:

_ علاء عبد الرزاق السالمي وحسين علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، دار وائل للنشر والتوزيع، بيروت، لبنان، 2004، ص.207.

[*] تقنية الإتصال في مجال قريب Near Field communication: لتوضيح فكرة هذه التقنية ننبه أنها شبيهة إلي حد كبير بتقنية البلوتوث Bluetooth، الموجودة في غالبية الهواتف والتي تعتمد على موجات الراديو للتواصل مع الأجهزة الأخرى، ولكن بعكس تقنية البلوتوث التي تحتاج

إلي تفعيلها على الجهازين المراد اقترانهم ببعضهما فإن تقنية الـ NFC لا تحتاج لتفعيلها على الجهاز، فقط قم بوضع الجهازين بجوار بعضهما وسوف يقوما بالاقتران في مدة من ثانية إلي عشر ثواني حسب المسافة بين الجهازين وهذه المسافة لا يمكن أن تزيد بحال من الأحوال عن 4 سم.

[18] من المؤسسات والمنظمات لفاعلة المقدمة للحلول الأمنية : Information Security Media Group. راجع الموقع الإلكتروني الرسمي: http://www.ismgcorp.com/.

[19] flashpoint :"Flashpoint Year In Review: 2022 Financial Threat Landscape", (https://flashpoint.io).

[20] برامج Keylogger هي برامج رصد لوحة المفاتيح. فهي تسجل وتعرض تقارير عن المفاتيح التي ضغطت عليها على لوحة المفاتيح في حاسوبك. ويمكنها أن تسجل كل ضربة على أي مفتاح، سواءً كان حرفاً أو رقماً أو زر "إدخال enter "أو ..Backspace إلخ. ويمكن أن يساعدك البرنامج على رؤية كل الكلمات التي استعملتها أو ضغطت عليها في حاسوبٍ معين نصبت عليه برنامج الرصد.

[21] محمد محمد الهادي. **توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية**. مجلة Cybrarians Journal. عدد 9، يونيو 2006.

[22] Représentation de la triade D, I, et C. Un quatrième est aussi souvent utilisé (sous différents noms) , Traçabilité, Imputabilité, ou Preuve , http://fr.wikipedia.org/wiki/Sécurité_de_information

[23] The Deming Cycle, refers to a four-part management method that preaches continuous improvement. The Deming cycle is made up of: Plan: Choose a process and set objectives Do: Implement the plan and begin collecting data on the results Check/Study: Analyze the results using statistical methods Act: Decide what changes to make in order to improve the process The Deming cycle and other similar continuous improvement models have been integrated into business and enterprise software. The Deming cycle is also referred to as plan do check act (PDCA), plan do study act (PDSA), the Shewhart cycle, the Deming circle and the Deming wheel. http://www.techopedia.com/definition/28058/deming-cycle