مجلة الدراسات المالية والمحاسبية والإدارية
ISSN 2352-9962 / E-ISSN 2572-0147
المجلد 08، العدد 03- ديسمبر 2021

OEB Univ. Publish.

تسيير المخاطر السبرانية في القطاع المالي من المنظور الدولي

cyber risk management in the financial sector from an international perspective

د.سناء العايب*
جامعة الأمير عبد القادر للعلوم الإسلامية laibsana89@gmail.com

تاريخ التسليم: 2021/05/03، تاريخ المراجعة: 2021/10/09، تاريخ القبول:2021/12/29

الملخص

نهدف من خلال هذا البحث إلى التعرف على الخطر السبراني، من خلال عرض بعض الجوانب المفاهيمية المتعلقة به، وكذا إبراز أثره على القطاع المالي خلال السنوات الماضية وصولا إلى أزمة كوفيد-19، بالإضافة إلى الممارسات الدولية (الفنية والكمية) لمواجهته.

وقد خلصت الدراسة إلى أن هذه المخاطر لا تعترف بالحدود الإقليمية ولا بدرجة تطور أي بلد، كما أن القطاع المالي يعد الأكثر استهدافا نظرا لسهولة اختراقه وترابط مؤسساته، بالإضافة إلى أن عملية القياس صعبة في ظل نقص البيانات.

الكلمات المفتاحية: الخطر السبراني، مخاطر التشغيل، القطاع المالي، القيمة المعرضة للمخاطر السبرانية.

Abstract

The present article aim to determine the impact of cyber risk on financial sector, by getting an overview of cyber risk, as it is defined by specialized literature, and perform an analysis of attacks reported in the financial sector over the last view years until the covid-19 crisis, in addition to the approved international practices (technical, quantitative) to confront it.

Based on the results of the analysis, we find that the hackers chose financial institutions as easy targets due to the fact that they can spread the attack quickly through the interconnected financial system, and because most of the financial institutes still use legacy digital systems. The measurement process still hard in light of the lack of data.

Keywords : Cyber risk, operational risk, financial sector, cyber value at risk.

*المؤلف المراسل

1. مقدمة:

تعتبر التكنولوجيا أحد أهم العوامل التي ساهمت في تغيير العالم وإعادة تشكيل معالمه، فقد مكنت من تحسين كفاءة السوق، وتقديم خدمات أكثر كفاءة وأسرع، وتحسين الشمول المالي وتعزيز تجربة العملاء. غير أن استخدام هذه التكنولوجيا لا يقتصر فقط على الجوانب الإيجابية، وما فرضته أزمة بل ذهب العديد من الأفراد والمؤسسات إلى توظيفها فيما يخدم توجهاهم اللامشروعة، وبهذا ظهرت عمليات الاحتيال التي شملت كل القطاعات الحساسة التي من شأنها توفير معلومة، قد تمثل ثروة عند هذه الفئة.

ولكون القطاع المالي أحد هذه القطاعات الحساسة فقد شهد العديد من الهجمات السبرانية التي تنوعت بتنوع وتطور التقنيات المستخدمة فيها، والتي تهدف إلى اقتناص الضحية والاستيلاء على بياناتها السرية (المالية والشخصية) وهذه العملية قد تنتهي في أغلب الأحيان بانتحال شخصية الضحية والقيام بعمليات احتيال أخرى، مما يجعل العملية متواصلة ومتكررة، الأمر الذي جعل من حماية البيانات وأمنها أحد أهم المواضيع المطروحة على طاولة الهيئات الدولية المالية خصوصا في السنوات الأخيرة، وما فرضته أزمة كوفيد-19.

وعليه تطرح اشكالية الدراسة على النحو التالي:

كيف أثرت المخاطر السبرانية على القطاع المالي؟ وما هي سبل مواجهتها؟

- **الأسئلة الفرعية:** - لماذا يعد القطاع المالي الأكثر استهدافا؟
  - لماذا يصعب قياس المخاطر السبرانية؟
- **الفرضيات:** - يعد القطاع المالي الأكثر استهدافا لكونه يشكل قطاعا حيويا في أي اقتصاد بالإضافة إلى سهولة اختراقه.
  - عدم توفر البيانات يصع عملية قياس المخاطر السبرانية.
- **أهداف الدراسة:** نهدف من خلال هذه الدراسة إلى جملة من الأهداف كما يلي:
  - ✓ وضع إطار مفاهيمي للخطر السبراني والتعرف على طرق انتقاله.
  - ✓ التعرف على تداعيات هذا النوع من المخاطر على القطاع المالي.
  - ✓ معرفة أسباب استهداف القطاع المالي.
  - ✓ التعرف على صعوبات قياس الخطر السبراني.

- **منهجية الدراسة:** بغرض الإجابة على الأسئلة المطروحة والوصول إلى الأهداف المتبناة، تم اعتماد المنهج الوصفي عند التطرق لمختلف الجوانب المفاهيمية المتعلقة بالموضوع، كما تم اعتماد المنهج التحليلي في تحليل البيانات الموظفة في الدراسة.
- **محاور الدراسة:** بهدف الإلمام بجوانب الموضوع والإجابة على التساؤلات المطروحة تم تقسيم الدراسة إلى ثلاثة محاور كما يلي:
  - مفاهيم أساسية متعلقة بالمخاطر السبرانية.
  - تداعيات المخاطر السبرانية على القطاع المالي.
  - تسيير المخاطر السبرانية.

2. مفاهيم أساسية متعلقة بالمخاطر السبرانية:

تسعى البنوك والمؤسسات المالية إلى تطوير نماذج أعمالها وفق ما تمليه التطورات التكنولوجية، ووفقا لهذا فإن المخاطر المصاحبة لها في تطور مستمر، ولعل أبرزها المخاطر السبرانية التي فرضتها بيئة الأعمال الرقمية. وفيما يلي نعرض بعض الجوانب المفاهيمية المتعلقة بها.

1.2 تعريف المخاطر السبرانية:

من أجل تحديد تعريف **للخطر السبراني** لابد من تحليل مكونات هذا المصطلح، حيث أن مصطلح **الخطر** كما هو معروف يعبر عن حالة عدم اليقين، التي تنطوي على احتمالات خسارة أو نتيجة غير مرغوب فيها، أما مصطلح **السبراني** الذي يعني إلكتروني، فقد أصطلح على كل ما هو متعلق بالشبكات الإلكترونية الحاسوبية وشبكة الأنترنيت.

يمكن القول أن الخطر السبراني يعبر عن نجاح هجوم في الفضاء السبراني، وبالتالي إلحاق الضرر بسرية وسلامة وتوافر المعلومات وتحقق الخسارة.

أما عن مفهوم هذا الخطر في القطاع المالي فقد اعتبرته لجنة بازل أحد أشكال المخاطر التشغيلية **(Aldasoro & al, January 2021,p03)** باعتبار أنه ناتج عن العنصر البشري، ويعرف على أنه خطر الخسارة الناتجة عن الحوادث الرقمية الداخلية والخارجية أو أطراف ثالثة، بما في ذلك السرقة وإتلاف المعلومات وأصول التكنولوجيا، والاحتيال الداخلي والخارجي **(Curti & al, July 14th, 2020, p. 04)**

2.2 أنواع المخاطر السبرانية:

مصطلح الخطر السبراني يعبر عن نجاح تنفيذ الهجمة السبرانية مهما كانت طريقة تنفيذها، ومن أجل فهم أفضل لهذه الهجمات لابد من التفريق بين التقنيات المستعملة في تنفيذ الهجمات، والقنوات التي يتم عبرها تمرير التقنية لتنفيذ الهجوم.

1.2.2 قنوات انتقال الهجمات السبرانية:

- **الرسائل القصيرة:** يعمل التصيد الاحتيالي عبر الرسائل القصيرة على تعزيز الرسائل النصية بدلا من البريد الإلكتروني لتنفيذ هجوم التصيد الاحتيالي. يرسل المهاجمون نصوصا من مصادر تبدو مشروعة (مثل الشركات الموثوقة) تحتوي على روابط ضارة. قد يتم إخفاء الروابط كرمز قسيمة خصم أو عرضا للحصول على فرصة للفوز بشيء مثل تذاكر الحفل(**security, 2021**) .
- **التصيد:** تم تصميم التصيد لخداع الضحايا لمشاركة المعلومات الشخصية، مثل أرقام **PIN** وأرقام الضمان الاجتماعي ورموز أمان بطاقات الائتمان وكلمات المرور والبيانات الشخصية الأخرى. غالبا ما يبدو أن مكالمات التصيد الصوتي تأتي من مصدر رسمي مثل بنك أو مؤسسة حكومية، يقوم هؤلاء المخترقون بإنشاء ملفات تعريف هوية المتصل وهمية (تسمى "انتحال هوية المتصل") مما يجعل أرقام الهواتف تبدو شرعية. في الآونة الأخيرة، أصبح القراصنة قادرون على انتحال شخصية الناس من خلال تقليد الأصوات باستخدام الذكاء الاصطناعي **(Deloitte, December 2019, p. 08).**
- **الرسائل الفورية:** في الوقت الحالي تطورت أشكال الرسائل الفورية بعد دمجها مع وسائل التواصل الاجتماعي، وبالتالي أصبح سهلا على المحتالين جذب الضحايا وحثهم على كشف تفاصيلهم وبياناتهم الشخصية (مثلا إرسال رسالة فورية مفادها أنه تم اختراق حسابك يرجى إدخال تفاصيل تسجيل الدخول) **(Alabdan, 2020, p. 08)**
- **الشبكات الاجتماعية:** تطورت وسائل التواصل الاجتماعي بشكل كبير سمح للأفراد بالتواصل ومشاركة خبراتهم مع أفراد آخرين الذين يشاركونهم نفس الاهتمامات أو آفاق الحياة أو الهوايات. ومع ذلك، فإن الاستخدام الرئيسي لهذه المنصات هو متابعة منشورات هويات العالم الحقيقي لتحديد مجموعات الأهداف وربما الاقتراب من الضحايا.
- **مواقع الويب:** تبدو هذه المواقع شرعية وتستخدم لجمع التفاصيل الشخصية للضحايا عندما يحاول الضحية تسجيل الدخول، ونظرا لأن المستخدمين العامين للإنترنت يميلون أكثر إلى الاعتقاد بأن الهجمات يتم تنفيذها بشكل أساسي من خلال رسائل البريد الإلكتروني

وخدمات المراسلة الأخرى ، فإنهم يميلون إلى أن يكونوا أقل وعيا بالأمان عند زيارة مواقع الويب، مما يجعلهم عرضة لهذه الأنواع من الهجمات السبرانية.

- **الشبكة اللاسلكية (Wi-Fi):** يتم اختيار نقطة اتصال عامة معينة لأن هدفا معينا يزور بانتظام ويستخدم الشبكة. يتضمن النموذج المعتاد تثبيت برامج ضارة على جهاز الضحية لجمع بيانات الاعتماد أو إعادة التوجيه إلى مواقع مخادعة.

2.2.2. التقنيات المستعملة في تنفيذ الهجمات السبرانية:

أما عن التقنيات المستعملة في تنفيذ الهجمات السبرانية فهي متعددة متنوعة وفقا لدرجة التطور التكنولوجي، وهي كما يلي:

- **تسميم خادم أسماء النطاقات (DNS poisoning):** يسمى كذلك الزرعة الخبيثة **(Pharming)**، ويقوم على تخريب خادم أسماء النطاقات الذي يعتبر أحد المكونات الأساسية للشبكة العالمية، والذي من مهمته الربط بين اسماء النطاقات وعناوينها العشرية مثلا بنك السلام وله عنوان عشري (213.230.10.197)، وعبر التلاعب بهذا العنوان فإن الضحية لا يشعر بهذا لكونه متأكد من صحة العملية، وعليه فهو يقاد مباشرة نحو العنوان المزيف وبالتالي الاستيلاء على البيانات السرية والمالية للضحية **(الغثبر و بن هيشة، 2009، صفحة 60)**.
- **حقن المحتوى (Content Injection):** يشير إلى إدخال محتوى زائف في موقع شرعي. يمكن أن يوجه هذا المحتوى الضار المستخدم إلى مواقع ويب مزيفة ، مما يدفع المستخدمين إلى الكشف عن معلوماتهم الحساسة للهاكر أو قد يؤدي إلى تنزيل برامج ضارة في جهاز المستخدم **(Alkhali & al, 2021, p. 15)**
- **هجمة الرجل في الوسط (MIM):** يعترض مستخدم ضار البيانات التي يستخدمها مقدم الخدمة والطرف المستخدم ويعيد تكوينها. ثم يواصل المهاجم الاتصال بمزود الخدمة متظاهرا بأنه الطرف المستخدم. يمكن للمهاجم بعد ذلك انتحال شخصية المستخدم **(Alabdan, 2020, p. 20).**
- **تشويش العنوان (Address Obfuscation):** غالبا ما تتم كتابة رسائل البريد الإلكتروني المغشوشة بشعور من الإلحاح، لإعلام المستلم بأنه تم اختراق حساب شخصي ويجب عليه الرد على الفور، والهدف هو الحصول على إجراء معين من الضحية مثل النقر فوق رابط ضار يؤدي إلى صفحة تسجيل دخول مزيفة. بعد إدخال بيانات اعتمادهم، يقوم الضحايا للأسف بتسليم معلوماتهم الشخصية مباشرة إلى أيدي المحتالين.

- **البرامج الخبيثة (Malware Attack):** يتم تنزيل البرامج الضارة على جهاز الضحية، إما بإحدى حيل الهندسة الاجتماعية أو تقنيا عن طريق استغلال الثغرات الأمنية في نظام الأمان (على سبيل المثال، نقاط ضعف المتصفح). برنامج **Panda** الضار هو أحد البرامج الضارة الناجحة التي اكتشفتها شركة **Fox-IT Company** في عام 2016. يستهدف هذا البرنامج الضار أنظمة تشغيل **Windows**. **(Alkhali & al, 2021, p. 14)**. وهي كما يلي:

❖ **تسميم ملف الخوادم المضيفة (Hosts File poisoning):** يشبه هذا الأسلوب إلى حد ما أسلوب **DNS**، غير أنه يعتمد على تسميم **HF** الموجود في جهاز الضحية، حيث أن هذا الملف يربط بين أسماء النطاقات وعناوينها العشرية، ويمكن التحكم به محليا من خلال جهاز المستخدم، فعند طلب موقع ما، فإن جهاز الضحية يقوم أولا بالبحث عن العنوان العشري لاسم الخادم في ملفات الخوادم قبل الاستعلام عن العنوان العشري لـ **DNS**، وبنفس الطريقة يقوم المخربون بتسميم **HF**، وذلك بوضع سجل جديد لرابط اسم نطاق معين بعنوان عشري لموقع مزيف **(الغثبر و بن هيشة، 2009، صفحة 62)** .

❖ **أحصنة طروادة:** هو برنامج كمبيوتر ضار مصمم لسرقة المعلومات الحساسة والسرية المخزنة أو المعالجة من خلال الأنظمة البنكية عبر الإنترنت **(Bulueliv, 2019, p. 20)**. هو برنامج غير مرئي للمستخدم يعمل عندما يقوم المستخدم بتسجيل الدخول إلى أي موقع ويب مهم أو إجراء أي معاملات ويجمع جميع المعلومات التي ملأها المستخدم ونقلها إلى المهاجم **(Syiemlieh, Khongsit, & Sharma, 2015, p. 02)**.

❖ **برامج التجسس (Spyware):** هي برامج ضارة يتم تثبيتها على كمبيوتر المستخدم دون أن يتمكن المتسلل المعرفي من الوصول إلى جميع الملفات والملفات المخزنة في النظام **(Adharsh & Dhatchina, 2020, p. 03)** مثل **key loggers and screen loggers** والتي يتم انشاؤها لتسجيل ضغطات المفاتيح وإنشاء سجلات لكل شيء يكتب على لوحة مفاتيح الكمبيوتر، ويمكن استخدامها للتحكم في الأجهزة أثناء استخدامها **(Kaspersky، 2021)**.

❖ **برامج الفدية (Ransomware):** تنتج عن نوع من البرامج الضارة المصممة لرفض الوصول إلى نظام الكمبيوتر أو البيانات حتى يتم دفع فدية. يمكن لمثل هذا الهجوم على مؤسسة مالية أن يتسبب في ضرر نقدي **(Asia, RSBP for Central, 2020, p. 02)**.

❖ **برامج الإعلانات المتسللة (Adware):** هي تهديد أمني يستخدم عادة لتجميع بيانات التسويق أو عرض الإعلانات من أجل تحقيق إيرادات **(Yilamaz & Zavrak, 2015, p. 5599)** .

❖ **برامج مكافحة الفيروسات (Scareware):** يجبر بعض مجرمي الإنترنت المستخدمين على تنزيل برامج معينة. بينما يتم تقديم مثل هذه البرامج عادةً كبرامج مكافحة فيروسات، تبدأ هذه البرامج بعد مرور بعض الوقت في مهاجمة نظام المستخدم. ثم يتعين على الضحية أن يدفع للمجرمين لإزالة مثل هذه الفيروسات **(Manisha M & al, 2015, p. 745).**

- **محركات البحث (Search Engine):** تعتمد هذه الطريقة على إنشاء مواقع إلكترونية للبيع بالتجزئة على الشبكة العالمية لمنتجات وهمية، حيث يتم إدخال هذه المواقع للفهرسة في محركات البحث أيضا بمنتجات مختلفة، وبأسعار منافسة للسوق لجذب الباحثين عن مثل هذه المنتجات، وعند زيارة المستخدمين لها بغرض شراء منتج معين فإنه ومن أجل إتمام عملية الشراء يطلب منه تعبئة نموذج إلكتروني ببيانات سرية، وذلك إما لإنشاء حساب في ذلك الموقع، أو للتحويل المالي، فيقع المشتري ضحية لذلك الموقع، والذي قد تستخدم بياناته لاحقا في انتحال شخصيته **(الغثبر و بن هيشة، 2009، الصفحات 71-72).**
- **حجب الخدمة الموزعة (Denial-of-service DOS):** هو نوع من الهجوم حيث يتم إغلاق الشبكة أو الخدمات مما يمنع الوصول إلى الخدمة للمستخدمين المعنيين، وذلك من خلال إرسال كمية زائدة من المعلومات وبالتالي إرسال بريد عشوائي **(SPAM)** لتعطيل حركة المرور العادية للشبكة، وبالتالي حرمان المستخدمين الشرعيين من الوصول إلى المعلومات. في الغالب يستهدف هذا الهجوم المنظمات الربحية الكبيرة، على الرغم من أن هذا النوع من الهجوم لا يسبب فقدان أو سرقة المعلومات الحيوية، إلا أن الضرر يتطلب الكثير من المال والوقت للتخفيف **(Acharya & Joshi, 2020, p. 4661).**
- **النوافذ المنبثقة (The Pop Up):** تعتبر الرسائل المنبثقة كونها تطفلية، واحدة من أسهل الأساليب لإجراء عمليات الخداع. لأنها تسمح للمتسللين بسرقة تفاصيل تسجيل الدخول عن طريق إرسال رسائل منبثقة للمستخدمين وتوجيههم في نهاية المطاف إلى مواقع ويب مزورة. **(Deloitte, December 2019, p. 10).**

من خلال ما تم عرضه مسبقا يمكن القول أن المخاطر السبرانية تتلخص في نوعين إما التحايل على العميل أو المؤسسة المالية من خلال إحدى التقنيات السابقة وتنفيذها في إحدى القنوات المذكورة، أو انتحال شخصية العميل أو المؤسسة المالية لتأدية أغراض تخدم المهاجم الذي يكون داخلي أو خارجي، وفيما يلي شرح موجز لكليهما:

- ✓ **التصيد الاحتيالي:** إنها تقنية هندسة اجتماعية تهدف إلى التأثير على الهدف للكشف عن معلوماته الشخصية، مثل البريد الإلكتروني أو كلمة المرور أو أي معلومات مالية أخرى يمكن للمتسلل من خلالها السيطرة على الأرصدة المستهدفة" **(Alabdan, 2020, p. 01).**
- ✓ **الانتحال المالي:** في الغالب يحدث هذا الخطر بعد نجاح تنفيذ الهجمة، وهو يعبر عن الاستيلاء على البيانات السرية والمالية للعميل، وانتحال شخصيته من أجل القيام بسحوبات مالية من رصيده أو حتى التحايل على مؤسسات مالية للحصول على التمويل. وفي هذا الصدد يجب التفريق بين أربعة أنواع من المهاجمين **(WEF & Deloitte, 2015, p. 12):**

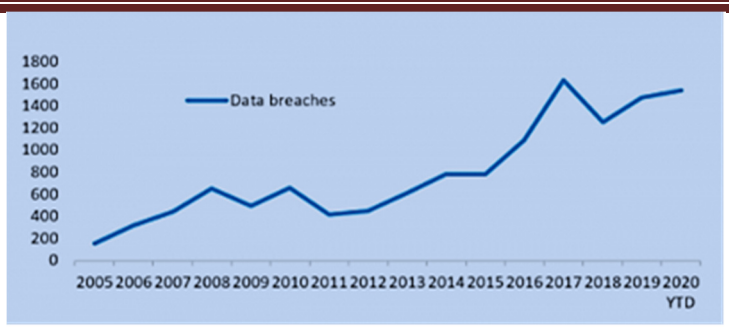
- **مجرمو الأنترنيت:** الذين يرتكبون جرائم سبراني تهدف إلى تحقيق أرباح من خلال سرقة البيانات الشخصية والمعلومات السرية للمؤسسة المالية وهم الأكثر ريادة.
- **الهاكرز (قراصنة الأنترنيت):** وهم المتسللون الذين يتصرفون بناء على معتقدات دينية أو إيديولوجية اجتماعية وسياسية.
- **الجواسيس:** والذين لديهم أهداف تتوافق مع مصالح البلد الذي يخدمونه.
- **التهديدات الداخلية:** التي يكون مصدرها موظفي المؤسسة المالية (عاملون بدوام كامل أو مؤقت)، وهنا يمكن أن يكون الخطأ مقصود أو غير مقصود.

3. تداعيات المخاطر السبرانية على القطاع المالي:

تتزايد الخسائر المالية الناتجة عن الهجمات السبرانية مع رقمنة العمليات المتقدمة، وقد وصلت إلى ذروتها في عام 2019 بنحو 3500 مليون دولار. هذه الأرقام لا تمثل سوى الحوادث المبلغ عنها، حيث أن أكثر من 90٪ من الحوادث لا يتم الإبلاغ عنها لتجنب الإضرار بالسمعة **(Fal, 2020, p. 10)** .

تتوقع دراسة من **cyber security Venture** أن تزداد تكاليف الهجمات السبرانية العالمية بنسبة 15٪ سنويا على مدى السنوات الخمس المقبلة، لتصل إلى 10.5 مليار دولار سنويًا بحلول عام 2025 **(Morgan, january 21, 2021, p. 01).**

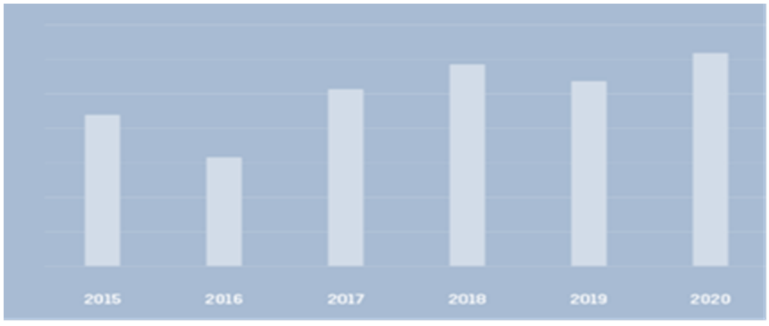
الشكل رقم (01): تنامي الهجمات السبرانية



Source : (Bouveret, June 2018, p. 08)

خلال الفترة (2005–2017)، تعرض القطاع المالي لهجمات سبرانية واسعة النطاق، وازدادت حدتها بسبب زيادة استخدام الإنترنت وانتشارها، فضلا عن التوسع في استخدام المدفوعات الرقمية وانتشار شركات التكنولوجيا المالية. الملاحظ أن الهجمات تتزايد وتتناقص بوتيرة طبيعية، لكن اعتبر عام 2017 الأسوء وذلك وفقا لما رود في تقرير صادر عن **(OTA)**، حيث بلغ عدد الهجمات الناجحة والمبلغ عنها ما يقارب 160000 عام 2016 هجمة ناتجة عن استخدام برامج الفدية، وبلغت خلال سنة 2017 حدود 350000 هجمة ناجحة، منها 134000 ناتجة عن برامج الفدية (Seal, 2018)، هذه الهجمات تسببت في شل 300000 جهاز كومبيوتر في 150 دولة، بتكلفة 3.75 مليون دولار بزيادة 5% عن عام 2016 (Loeb, 2018). أقر الخبراء أن 92% من هذه الهجمات كان بالإمكان تفاديها باتباع ممارسات أمنية سليمة. تعكس الإحصائيات عدم كفاية الرقابة على الهجمات السبرانية، وضعف حوكمة المخاطر، والاعتماد على الآليات القديمة التي يسهل اختراقها.

الشكل رقم (02): هجمات التصيد الاحتيالي خلال الفترة (2015–2020)

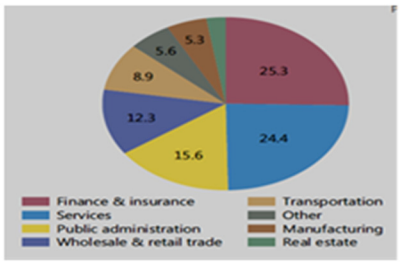


Source: (Warburton, 2020, p. 04)

بلغ العدد الإجمالي لاكتشافات التصيد الاحتيالي في عام 2019 ما يعادل 467.188.119 حالة، 51.4٪ منها كانت هجمات متعلقة بالتمويل. ارتفع الرقم في عام 2020 بنسبة 15٪ مقارنة بالعام الماضي. 37.2% منها كانت متعلقة بالتمويل، في الولايات المتحدة الأمريكية كانت 52٪ من جميع الهجمات ناتجة عن العمل عن بعد مما سهل عمليات القرصنة خاصة للمؤسسات التي تفتقر إلى الاستعداد لمواجهة المتسللين (**SecureList, 2020**). في المملكة المتحدة، يمثل التصيد الاحتيالي 28٪ من جميع الحالات المبلغ عنها خلال الفترة من أفريل 2019 – مارس 2020 ، وفقا لبيانات (**OAIC**)، بلغ عدد عمليات التصيد الاحتيالي 36 ٪ من جميع أحداث القرصنة التي تتعلق بسرقة بيانات الاعتماد (الأكثر أولية) (**Warburton, 2020, p. 04**).

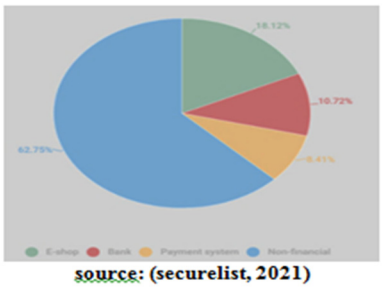
كان من المتوقع أن تنخفض حدة هذه الهجمات خلال عام 2020، لكن أزمة كوفيد-19 قلبت كل الموازين، ووضعت المؤسسات المالية أمام تحديات كبيرة فرضها تغير نمط العمل (العمل من المنزل **WFH**) والتحديات التشغيلية الأخرى.

الشكل رقم (03): الحوادث السبرانية المتعلقة بـ Covid-19 حسب القطاع



Source: (Aldasaro & al, 14 january 2021, p. 06)

الشكل رقم (04): توزيع الحوادث السبرانية حسب القطاعات المالية خلال Covid-19



source: (securelist, 2021)

توضح الإحصائيات المدرجة مدى تأثر كل قطاع على حدة خلال فترة كوفيد -19 ، ووجد أن القطاع المالي هو الأكثر تضررا بنسبة 25.3٪، يليه قطاع الخدمات بنسبة 24.4٪ من إجمالي عدد الهجمات المبلغ عنها. وفقا لتقرير صادر عن **Keeper security**، فإن 70٪ من الهجمات المبلغ عنها حقيقية وتم تنفيذها بنجاح. ترجع الشركات المتضررة هذه الهجمات إلى الظروف المتعلقة بالوباء (**Muncaster, 2021**)

وقد تأثرت بشكل خاص شركات الدفع وشركات التأمين والمؤسسات الائتمانية، حيث وجدت دراسة استقصائية بين المؤسسات المالية أجراها مركز تبادل وتحليل معلومات الخدمات المالية (**FS-ISAC**) ارتفاعا كبيرا في التصيد الاحتيالي والمسح المشبوه والنشاط الضار ضد

صفحات الويب لموظفي **WFH** للوصول إلى الشبكة، فقد شهدت هذه المؤسسات أقوى زيادة في عمليات الاختراق، حيث نمت الهجمات المرتبطة بـ **Covid-19** من أقل من 5000 أسبوعيا في فيفري إلى أكثر من 200000 أسبوعيا في أواخر أفريل، وارتفعت بشكل أكبر بنحو الثلث في ماي وجوان مقارنة بشهري مارس وأفريل، وقد أبرز الاستطلاع أنه في 45٪ من الحالات، طغى فريق **WFH** على البنية التحتية، كما أنه في ثلث الحالات لم يتم إعداد خطط تكنولوجيا المعلومات الخاصة باستمرارية الأعمال لفريق **WFH**. أفاد خمس الشركات المالية أن أنشطة تشغيل شبكتها قد توقفت أثناء الوباء**(Aldasaro & al, 2021, p. 06)**

وعن التصيد البنكي نجد تراجع للبطاقات المسروقة في عام 2016، حيث كان لدى 97.2% من جميع البطاقات أسماء كاملة مرتبطة بها. في عام 2020، انخفض هذا الرقم إلى 84.9% وبالمثل، انخفضت صلاحية البطاقة أيضا. وخلال السداسي الثاني من نفس السنة أين شهد العالم ذروة الوباء تزايد عدد البطاقات المسروقة (سرقة بيانات اعتماد البطاقة) وبالتالي العمل المنزلي سهل على المتصيدين سرقة بيانات البطاقات المالية وانتحال شخصيات أصحابها لاستعمالها في عمليات دفع عن بعد خاصة بهم وبفواتير حقيقية موجهة لعناوين مزيفة **(Warburton, 2020, p. 16)**. إن هذه الهجمات ساهمت وبشكل كبير في تدني جودة الأصول البنكية (وفقا لاستطلاع أجرى على 15 دولة أوروبية)، كما أن نسبة رأس المال (الشريحة الأولى) من المتوقع أن تنخفض بمقدار 485 نقطة في نهاية عام 2023 **(JCESO, 2021, p. 06)**.

مع تنامي سوق العملات المشفرة تزايدت عمليات الاحتيال عبرها باعتبار أن هذه العملات مجهولة المصدر ويشوبها الكثير من الغموض، فقد منع نظام مكافحة التصيد الاحتيالي لدى مؤسسة **APWG** 410 786 محاولة لإعادة توجيه المستخدمين إلى مواقع التصيد الاحتيالي التي تحاكي محافظ العملات المشفرة والمبادلات والأنظمة الأساسية. يعمل المهاجمون بنشاط على إنشاء صفحات تسجيل دخول وهمية لخدمات العملة المشفرة على أمل الحصول على بيانات اعتماد المستخدم.

وتجدر الإشارة إلى أن الولايات المتحدة الأمريكية والمملكة المتحدة وأستراليا صنفتا في منطقة التعرض المنخفض والمعتدل وفقا لمؤشر التعرض للخطر السبراني **(CSI)** **(Frisby, 2020)**، لكنهما شهدتا نسبة عالية من الانتهاكات السبرانية، بالإضافة إلى ذلك وخلال سنة 2021 صنفت أستراليا من بين العشر الدول الأكثر تضررا من البرامج الضارة البنكية، الأمر

الذي يقودنا إلى نتيجة مفادها أن الخطر السبراني لا يتعلق بالحدود الإقليمية أو درجة التنمية لكل بلد، بل يرتبط بتطور بآليات القرصنة والمركز المالي للضحية.

4. تسيير المخاطر السبرانية:

مع تنامي الهجمات السبرانية ونجاح أغلبها، ركزت الحكومات على حماية مؤسساتها وهياكلها المالية، وهذا من خلال اتباع ممارسات فنية تمليها التعاملات الرقمية، بالإضافة إلى التركيز على الإنفاق في مجال الأمن السبراني. وبالتالي أصبح هذا الموضوع محل جدل ونقاش على المستوى الدولي من أجل بحث سبل وآليات تعزيز البنية التحتية الأمنية الداخلية.

1.4. مبادئ تسيير المخاطر السبرانية:

يبدو أن الإجراءات التي يتخذها كل بلد هي إجراءات عامة لتعزيز الأمن القومي وليس لحماية الأنظمة المالية. ويرجع ذلك إلى حقيقة أن الأمن السبراني غير مدرج في سياسات إدارة المخاطر. الشيء الذي يوضح صعوبة الوصول إلى بيانات الخسارة المتعلقة بالمخاطر السبرانية، حيث يتم التعامل معها على أنها مخاطر تشغيلية وفي هذا السياق نشرت لجنة بازل في ديسمبر 2018 مجموعة من مبادئ الحوكمة السبرانية كما يلي **(BCBS, December 2018, pp. 11-15):**

- ✓ إدراج إستراتيجية تسيير المخاطر السبرانية ضمن سياسات تسيير المخاطر التي يضعها مجلس الإدارة.
- ✓ تصر اللجنة على تعيين مسؤول أمن المعلومات السبرانية **(CISO)** الذي يقدم تقاريره إلى مسؤول المخاطر الإلكترونية **(CRO)**.
- ✓ لا تتضمن معظم البنوك متطلبات خاصة للتعامل مع مهارات القوى العاملة في مجال الأمن السبراني. لذلك، حثت اللجنة على نشر الوعي بالمخاطر السبرانية، وتعزيز ثقافة تسيير المخاطر المشتركة في الصناعة البنكية.

وبدوره قام صندوق النقد الدولي في نوفمبر 2020 بطرح مجموعة من المبادئ المدعمة لما ورد في وثيقة لجنة بازل، وذلك على خلفية الخسائر الكبيرة التي تسببت فيها الانتهاكات السبرانية. وقد نصت هذه المبادئ في مجملها على يما يلي **(Maure & Nelson, Spring 2021):**

- ✓ مزيد من الوضوح حول الأدوار والمسؤوليات.
- ✓ يجب على البنوك والمؤسسات المالية أن تعمل ضمن إطار عمل **CS** الدولي الموحد، وأن تحث على التعاون المشترك لوقف الجرائم السبرانية.

- ✓ التركيز على القطاع المالي من خلال وضع أطر حماية أكثر فاعلية يوفر حماية أفضل للقطاعات الأخرى في المستقبل.

في ماي 2018 قدمت اللائحة العامة لحماية البيانات، والتي تضمنت مطلب **إخطار** الجهة التنظيمية ومالك البيانات بخرق البيانات، مع فرض عقوبات على المؤسسات التي لا تمتثل بغرامة تصل إلى 4% من دخلها الإجمالي.

2.4. تكميم (قياس) المخاطر السبرانية:

على مدار العام الماضي، بدأت الفرق التنفيذية وأعضاء مجلس الإدارة عبر العديد من الصناعات في طرح الأسئلة بقوة أكبر حول المخاطر التي تشكلها هجمات الأمن السبراني. لم يعودوا راضين عن المراجعات الفنية لضوابط الأمان الخاصة بهم ويطرحون أسئلة تتعلق بتأثير الأعمال لهجمات الأمن السبراني. ما مقدار المخاطر السبرانية لدينا؟ هل ننفق أكثر من اللازم أم لا؟ إلى أي مدى يمكننا تقليل المخاطر باستخدام ميزانية أمان المعلومات المقترحة؟ هل يجب أن نشتري التأمين الإلكتروني؟

أدت مثل هده الأسئلة إلى البحث عن آليات تمكن من تكميم المخاطر السبرانية وتسهيل قياسها، وقد تم التركيز على القيمة المعرضة للمخاطر والتي بدأ تطبيقها في سياق الأمن السبراني، حيث تم بذل العديد من الجهود لتكييفها مع الأساليب التي تم تطويرها خصيصا لتقييم المخاطر السبرانية. تقدم هذه النماذج الجديدة "إدارة عليا برقم خطر واحد واحتمال إحصائي لفهم مخاطر الأمن السبراني الإجمالية للمؤسسة". وقد اصطلح على هذا المقياس تسمية **CVaR**، وتتضمن هدفين رئيسيين **(Orlando, 2021, p. 04)**:

- ✓ مساعدة متخصصي المخاطر وأمن المعلومات في توضيح المخاطر السبرانية ماليا.
- ✓ تمكين المديرين التنفيذيين من اتخاذ قرارات فعالة من حيث التكلفة وتحقيق التوازن بين حماية المؤسسة وإدارة الأعمال.

يستند **Cy-VaR** إلى مفهوم القيمة المعرضة للمخاطر وهو مقياس للمخاطر اقترحه **JP Morgan** في عام 1995 باعتباره "خسارة أسوأ حالة متوقعة عند مستوى ثقة محدد". تعتبر القيمة المعرضة للمخاطر مقياسا رئيسيا للمخاطر، كما إنه شائع جدا لأنه بديهي وقيمه العددية أسهل في التفسير مقارنة بمقاييس المخاطر الأخرى. علاوة على ذلك، تم تحديده من قبل المنظمين في اتفاقيتي بازل 2 وبازل 3.

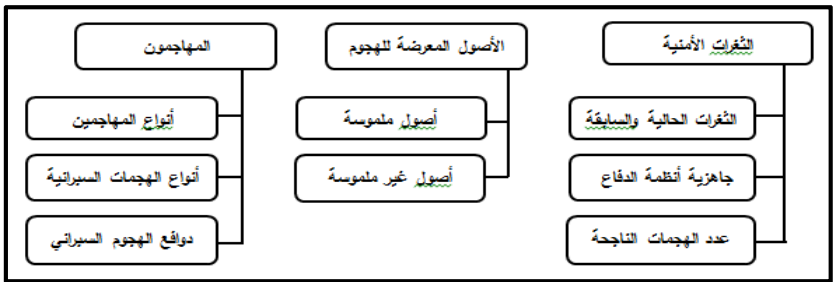
في صناعة الخدمات المالية، نمذجة القيمة المعرضة للخطر هي منهجية إحصائية تستخدم لتحديد مستوى المخاطر المالية داخل شركة أو محفظة استثمارية خلال إطار زمني محدد. يتم قياس القيمة المعرضة للخطر بثلاث متغيرات: مقدار الخسارة المحتملة، احتمال هذا القدر من الخسارة، الإطار الزمني.

وبالمثل، تستخدم نماذج القيمة المعرضة للمخاطر السبرانية الاحتمالات لتقدير الخسائر المحتملة من الهجمات السبرانية خلال إطار زمني معين، وهي عبارة عن نماذج تحاكي الواقع بغرض تحديد الخسارة الناتجة عن فقدان أحد الأصول أو مجموعة من الأصول مجتمعة، وتحديد الأثر الاقتصادي لهذه المخاطر، الذي لم يكن ممكنا في عمليات التقييم السابقة التي تعتمد على تجنب الهجمات. وبالتالي فهده الطريقة تعتمد على طريقة مونتي كارلو.

3.4. مكونات القيمة المعرضة للمخاطر السبرانية:

من أجل تقدير موثوق به للمخاطر السبرانية، لابد من الأخذ بعين الاعتبار الثغرات الأمنية (مواطن الضعف في نظام أمن المعلومات الخاص بالمؤسسة المالية والبنوك) وتحديدها بدقة، وكذا التعرف على المهاجمين المحتملين، والأصول المحتمل تعرضها للهجوم السبراني.

الشكل رقم (05):مكونات القيمة المعرضة للمخاطر السبرانية



Source: (WEF & Deloitte, 2015, p. 12)

- **الثغرات الأمنية:** وهي الثغرات التي لم يتم اصلاحها، والتي قد تنتج عن خطأ في التنفيذ، الذي قد يؤدي إلى حادث غير متوقع يؤثر على نظام المعلومات. هذا الحدث يمكن أن ينتج بسبب خطأ واحد أو سلسلة من الأخطاء، والتي يتسبب فيها غالبا المستخدمون سواء عن قصد أو غير قصد، وبالتالي يمثلون الحلقة الأضعف لهجوم سبراني ناجح. إن تقييم الثغرات الأمنية للمؤسسة المالية يعتمد على قدرتها السابقة في مواجهة هجومات ناجحة، وعلى مستوى جاهزة وقدرة نظامها الأمني الذي يؤثر بدوره على أداء **CVaR.**

- **الأصول المعرضة للهجوم:** يجب على المؤسسة المالية تحديد الأصول المعرضة للهجوم السبراني والتكاليف الناتجة عن ذلك، وكما هو معروف تنقسم أصول المؤسسة إلى أصول مادية (ملموسة) والتي تشمل الأدوات المالية، النية التحتية، القدرة على منح القروض... وغيرها، أما الأصول المعنوية (غير الملموسة) فتمثل رأس المال الفكري، السمعة، الخبرة، الثقة...إلخ، تساهم هذه الأخيرة بنسبة 80% من قيمة المؤسسة (**Orlando, 2021, p. 06**)، بعد تحديد هذه الأصول يجب القيام بتقييمها حتى يسهل تصنيفها إلى فئات منفصلة تمكن من تحديد المخاطر السبرانية الشاملة، وتجدر الإشارة إلى أن عملية تقييم الأصول غير الملموسة تعد صعبا نوعا ما.
- **المهاجمون:** يجب إعداد ملف تعريفي للمهاجمين المحتملين ودوافعهم ونوع الهجوم المحتمل الذي يسعون لتطبيقه عبر تحديد القنوات الناقلة للهجوم والتقنيات المستعملة في تنفيذه، كما يجب التركيز على دوافع الهجوم والتي تختلف باختلاف نوع المهاجم الذي يمكن أن يخطئ (موظف بالمؤسسة المالية) وبالتالي فالهجوم ينتج عن إهمال منه كما يمك أن يون مقصودا والغرض منه إلحاق الضرر بالمؤسسة والاستفادة من ذلك، وهو ما يسعى إليه المهاجم الخارجي.

إن عملية تكميم المخاطر السبرانية توفر للمؤسسة المالية عدة مزايا لم تكن لتكون وقت اعتمادها الأدوات الفنية (تجنب المخاطر): وعليه يمكن حصر هذه الفوائد فيما يلي:

- ✓ اتخاذ قرارات سليمة.
- ✓ تعزيز موضوعية ودقة تقييمات المخاطر الخاصة بالمؤسسة المالية.
- ✓ إزالة الغموض عن الأمن السبراني لمجلس الإدارة والإدارة العليا.
- ✓ فهم فعالية استراتيجيات التخفيف من المخاطر واكتساب ميزة تنافسية.

4.4. تحديات اعتماد القيمة المعرضة للمخاطر السبرانية:

إن عملية تكميم المخاطر السبرانية وفقا لمقياس القيمة المعرضة للمخاطر، ليست بالأمر البسيط، فهي تحتاج مجموعة من العوامل حتى تكون نتيجة التقدير موثوقة، وهي كما يلي:

- **توافر البيانات:** من أهم التحديات التي تواجه المؤسسات المالية هو القدرة على تقدير احتمالات هجوم سبراني ناجح، والذي يتطلب أساليب قياسية تعتمد على افتراضات التوزيعات الاحتمالية لشدة وتواتر الأحداث السبرانية وكذا معايرة معلمات التوزيع للبيانات

الحقيقية في ظل توفر بينات تاريخية واسعة النطاق لرصد تكرارات الأحداث (WEF & Deloitte, 2015, p. 15). غير أن عدم توفر هذه البيانات يضع المؤسسة في فجوة بين تحقق الهجوم واكتشافه، وهذا راجع إلى غياب الوعي بالمخاطر السبرانية التي تعتبرها أغلب المؤسسات كأخطاء تقنية يمكن تلافيها، والواقع أنها تمثل نسبة كبيرة من المخاطر التشغيلية التي قد ينجر عنها مخاطر أخرى.

- **عدم وجود تعريفات قياسية للمخاطر**: ويتعلق الأمر بتابين الآراء في تحديد مفهوم لهذه المخاطر داخل المؤسسة المالية، فالبعض يعتبرها أوجه قصور وتهديدات يمكن تلافيها دون الإفصاح عنها (حماية سمعة المؤسسة)، والبعض الآخر يعتبرها مخاطر كبرى تهدد سير أعمال المؤسسة المالية، وبالتالي فإنه لا يوجد اعتراف صريح بهذه المخاطر. وفي هذا الصدد أوكلت لجنة بازل مهمة المخاطر السبرانية إلى شخص مستقل يرفع تقاريره إلى مسؤول أمن المعلومات، وهذا لتحري الدقة في تحديد هذه المخاطر وتعريفها.
- **دعم عدد محدود من السيناريوهات:** اعتمدت التطبيقات الأولى لنماذج القيمة المعرضة للمخاطر السبرانية على إجراء تحليلات فردية باستخدام جداول بيانات مفصلة. كانت مقارنة سيناريوهات المخاطر عملية معقدة للغاية وكثيفة الموارد، وكان تجميع سيناريوهات المخاطر للتقييمات على مستوى المؤسسة أمرا مستحيلا عمليا (Sanna, 2016).
- **الضغط:** دفع الضغط الأخير الذي فرضته مجالس إدارة المؤسسات والإدارة التنفيذية على لتحسين إعداد التقارير وتسيير المخاطر السبرانية العديد من المنظمات والمتخصصين في تسيير المخاطر لإنشاء منتديات يمكنهم من خلالها التعرف على الممارسات القياسية للمخاطر السبرانية ومشاركة حالات الاستخدام والحياة الواقعية والخبرة.

5. خاتمة:

مع ازدياد تواتر وشدة عمليات الاحتيال والجرائم السبرانية على مدار العقد الماضي، وجهت الشركات في جميع أنحاء العالم إنفاقها على تقنيات أمن المعلومات المتقدمة لتعزيز البنية التحتية الأمنية الداخلية. علاوة على ذلك، فإن الحاجة إلى الدفاع عن البنية التحتية الحيوية من التهديدات المستمرة المتقدمة شجعت الحكومات في جميع أنحاء العالم على إصلاح استراتيجيات الأمن السبراني الخاصة بها، غير أن العمل الفردي لم يكن مجديا، وخلق فرص تهديد أخرى، وهو ما شهده القطاع المالي الذي عرف موجة هجمات ساهمت في

مجملها في تقليص جودة أصول البنوك، فقدان ثقة العملاء، تدهور السمعة. ومن جملة النتائج المتوصل إليها ما يلي:

- ✓ يعد القطاع المالي الأكثر استهدافا بفعل ترابط أنظمته الرقمية. هذا الترابط شكل فرصا جديدة للتهديد، حيث يمكن أن يكون أمان نظام معين متعلق بنظام آخر، وبالتالي تتشكل قناة يمكن للمهاجم تمرير هجومه عبرها. هذا عدا عن قدم هذه الأنظمة وعجزها على مواجهة تقنيات الهجوم المتطورة.
- ✓ إن عدم الوعي والإهمال من طرف الموظفين ساهم في تفاقم الهجمات، خصوصا تلك التي فرضتها طبيعة العمل من المنزل.
- ✓ إن الممارسات الفنية المعتمدة في مواجهة المخاطر السبرانية تعد غير كافية في ظل تطور تقنيات الهجوم، وقابلية المهاجمين للتكيف مع التطورات الحاصلة في المجال الرقمي، وبالتالي صعوبة التنبؤ باستراتيجياتهم.
- ✓ الهجومات السبرانية لا تتعلق بدرجة تطور البلد، بل بمدى جاذبية الضحية، وهو ما أثبتته الاحصائيات، حيث تبين أن الولايات المتحدة الأمريكية وبالرغم من قوة أنظمتها الأمنية إلا أنها تعرضت لأكثر من 52% من إجمالي الهجمات خلال عام 2020.
- ✓ إن آثار الهجمات السبرانية الناجحة لا تقتصر فقط على أتلاف البنية التحتية الأمنية في القطاع المالي، بل امتدت آثاراها إلى تخفيض جودة أصول البنوك.
- ✓ إن عدم امتثال المؤسسات المالية لضوابط الافصاح خوفا على السمعة، جعل من عملية تقدير المخاطر السبرانية صعبة، خصوصا في ظل تبني مقياس القيمة المعرضة للمخاطر السبرانية والتي تعتمد على البيانات التاريخية لإعداد سيناريوهات تحاكي الواقع.
- ✓ عملية قياس المخاطر السبرانية تتطلب الأخذ في الاعتبار جميع الأصول، وبالنظر لطبيعة هذه الأصول، نجد البعض منها صعب القياس والتقدير وبالتالي النتائج تكون غير موثوقة.

6. قائمة المراجع:

1. الغثبر، خالد بن سليمان وبن هيشة، سليمان بن عبد العزيز. (2009). الإصطياد الإلكتروني (الأساليب والإجراءات المضادة) (الإصدار الطبعة الأولى). الرياض، السعودية: مكتبة الملك فهد الوطنية.

I Journal articles:

1. Acharya, S., & Joshi, S. (2020). Impact Of Cyber-Attacks On Banking Institutions In India: A Study Of Safety Mechanisms And Preventive Measures. Palarch's Journal Of Archaeology Of Egypt/Egyptology, 17(06), 15.
2. Yilamaz, S., & Zavrak, S. (2015). Adware: Are view. International Journal for Computer Science and Information Technology, 06(06).
3. Syiemlieh, P., Khongsit, G., & Sharma, U. (2015, January). Phishing-An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation. National Conference on Advances in Engineering, Technology & Management (pp. 01-08). IOSR Journal of Computer Engineering.
4. Manisha M, M., & al. (2015, December). Online Banking and Cyber Attacks: The Current Scenario. international Journal of advanced research in Computer Science and Software Engineering, 5(Issue 06).
5. Alabdan, R. (2020, september 30). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. l, vol 12(Issue 10), 01-39. future Internet Journa, 12(10).
6. Alkhali, Z., & al. (2021, March 09). Phishing Attacks: A Recent. (ASM Kayes, Ed.) Computer Security, a section of the journal Frontiers in Computer Science, 03(article 563060), 24.
7. Orlando, A. (2021, October 18). Cyber Risk Quantification: Investigating the Role of Cyber. (T. Kliestik, Ed.) Risks journal, 09(10), 13

II Reports:

1. Adharsh, M., & Dhatchina, M. (December 2020). Cyber Attacks in banking industry. cyber attacks in banks. Bournemouth Project: cyber crime in banking.
2. Aldasaro, I., & al. (14 january 2021, january 14). Covid-19 and cyber risk in the financial sector. Bulletin, Bank of International Settlement, basel.
3. Asia, RSBP for Central. (2020). COVID-19: cybersecurity challenges for financial institutions.
4. BCBS. (December 2018). Cyber-resilience: Range of practice. Bank for International Settlement, Basel.
5. Bouveret, A. (June 2018). cyber security for the financial sector:A Framework for Qauntitave Assesment. Working paper, IMF.
6. Bulueliv. (2019). cyber threat intelligence for Banking &Financial services. spain: Bulueliv.
7. Curti, F., & al. (July 14th, 2020). Cyber Risk Definition and Classification for Financial Risk Management. Federal Reserve Bank of Richmond, the Federal Reserve Bank of New York, or the Federal Reserve System., Richmond.
8. Deloitte. (December 2019). Understanding phishing techniques. Singapore: Deloitte; , Touche Enterprise Risk Services.
9. Fal. (2020). Cybersecurity in the time of COVID-19 and the transition to cyber immunity. spain: Facilitation of transport and trade in Latin America and Caribbean .

10. JCESO. (2021). Risk and vulnerabilities in the EU financial system. Joint Committee of European Supervison Authorities.
11. Maure, T., & Nelson, A. (Spring 2021). the glabal cyber threat. IMF.
12. Morgan, S. (january 21, 2021). Cyber warefare in the c-suite. Cyber security ventures, California.
13. Warburton, D. (2020). 2020 phishing and fraud report. F5Labs, Seattle.
14. WEF, & Deloitte. (2015). Partnering for Cyber Resilience /Towards the Quantification of Cyber Threats. World Economic Forum, Geneva.

III Internet websites:

1. Frisby, J. (2020, JUNE 02). Cyber security Exposure Index (CEI). Retrieved 02 24, 2021, from Passwordmanagers.co: http://passwordmanagers.co
2. Kaspersky. (2021). What is Kstroke Logging and Keyloggers. Consulté le 08 13, 2021, sur Kaspersky: http://www.Kaspersky.com
3. Loeb, L. (2018, Jan 30). Cybersecurity Incidents Doubled in 2017, Study Finds. Retrieved september 09, 2021, from securityintelligence: https://securityintelligence.com/news/cybersecurity-incidents-doubled-in-2017-study-finds/
4. Muncaster, P. (2021, 01 19). Most Financial Services Have Suffered COVID - Linked Cyber attacks. Retrieved 03 11, 2021, from Infosecurity Magazine: http://www.Infosecurity Magazine.com
5. Sanna, N. (2016, January 18). What Is a Cyber Value-at-Risk Model? Retrieved August 22, 2021, from fairinstitute: www.fairinstitute.org
6. Seal, T. (2018, Jan 26). Cyber attcks Doubled in 2017. Retrieved le september 09, 2021, from infosecurity: https://www.infosecurity-magazine.com/news/cyberattacks-
7. SecureList. (2020, April 16). Retrieved 03 05, 2021, from Financial Cyber threats in 2019: https://securelist.com/financial-cyberthreats-in-2019/96692/
8. security, p. (2021, April 12). 11 Types of Phishing Real-Life Examples. Retrieved August 13, 2021, from panda security: https://www.pandasecurity.com
9. Velieva, I., & Al. (2021, May 24). Cyber risk in new Era: The effect on bank ratings. Retrieved le June 18, 2021, from S& P Global Ratins: http://www.spglobal.com/ratings.