التصيد الاحتيالي في القطاع المالي بين الآثاروطرق الوقاية

د. سناء العايب

laibsana89@gmail.com

جامعة الأميرعبد القادرللعلوم الإسلامية قسنطينة

ملخص:

نهدف من خلال هذا البحث إلى التعرف على التصيد الاحتيالي كنوع من الهجمات السيبرانية ، من خلال التعرف على بعض الجوانب المفاهيمية المتعلقة به، وكذا إبراز أثره على القطاع المالي خلال السنوات الماضية وصولا إلى أزمة كوفيد-19.

وقد خلصت الدراسة إلى أن هذه المخاطر لا تعترف بالحدود الإقليمية ولا بدرجة تطور أي بلد، كما ان القطاع المالي يعد الأكثر استهدافا نظرا لسهولة اختراقه وترابط مؤسساته، وفي هذا الإطار حثت الهيئات الدولية على ضرورة تكثيف الجهود الجماعية وتوحيد العمل من أجل نشر ثقافة مكافحة الجريمة السبرانية، بغرض تسهيل تبني الأطر التنظيمية التي تضبطها.

الكلمات المفتاحية: التصيد الاحتيالي ، الهجمات السبرانية، الخطر السبراني ، القطاع المالي.

Abstract:

The present article aims to determine the impact of phishing on financial sector, by getting an overview of phishing, 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.

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. In this context the international authorities insist on the collective work to enhance the Cyber-risk awareness culture**.**

Keywords: Phishing, cyber attacks, cyber risk, financial sector

مقدمة:

تعتبر التكنولوجيا المالية 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 التكنولوجيا المالية لا تقتصر فقط على الجوانب الإيجابية، إذ تواجه الحكومات تحديات كبيرة تتمثل في مخاطر سوق التكنولوجيا المالية، ويعتبر الأمن السيبراني من أكبر المخاطر المتزايدة بنسبة 78% تليه المخاطر التشغيلية 54 %، حماية المستهلك 27%، الاحتيال والتزوير 18% (World Bank, 2020) .

لقد أتاح كوفيد 19 فرصًا أكبر للاحتيال في الدفع الرقمي، حيث شهدت شركات التكنولوجيا المالية في المتوسط زيادة بنسبة 15٪ في انتهاكات الأمن السيبراني، وقد تنوعت الهجمات السيبرانية بتنوع وتطور التقنيات المستخدمة فيها، ولعل أبرز هذه الهجمات ما يسمى بالتصيد الاحتيالي، الذي يعتمد على 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.

وتأسيسا لما سبق تأتي اشكالية الدراسة على النحو التالي:

ما هو أثر التصيد الاحتيالي على القطاع المالي؟ وما هي سبل مواجهته؟

- **الأسئلة الفرعية:**
  1- لماذا يعد القطاع المالي الأكثر استهدافا؟
  2- هل يرتبط التصيد الاحتيالي بالدول ذات التكنولوجيا المتطورة؟
  3- لماذا تفشل سياسات الحد من هجمات التصيد الاحتيالي ؟

- **الفرضيات:**
  1- يعد القطاع المالي الأكثر استهدافا لكونه يشكل قطاعا حيويا في أي اقتصاد بالإضافة إلى سهولة اختراقه.
  2- يرتبط التصيد الاحتيالي بدرجة تطور كل بلد .
  3- العمل الفردي يفشل أمام قوة هجمات التصيد الاحتيالي

- **أهداف الدراسة**
  - ✓ وضع إطار مفاهيمي شامل للتصيد الاحتيالي
  - ✓ التعرف على آثار هذا النوع من الهجمات على القطاع المالي.
  - ✓ معرفة أسباب استهداف القطاع المالي من طرف المتصيدين المحتالين
  - ✓ التعرف على دور الهيئات المالية الدولية في مواجهة هذه الهجمات أو التقليل منها.

- **المنهج المتبع:** 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.

أولا: مفاهيم عامة حول التصيد الاحتيالي

1- تعريف التصيد الاحتيالي:

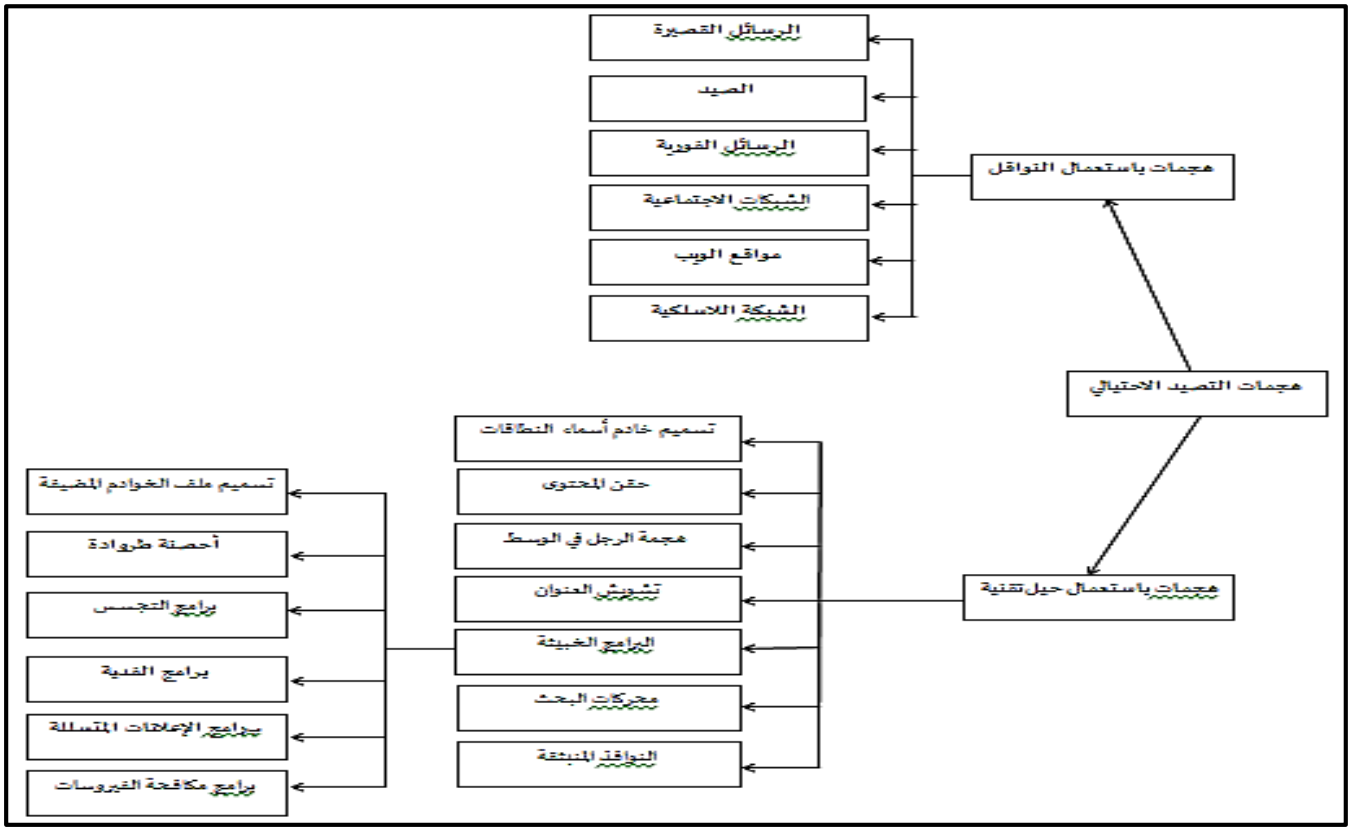
يعد التصيد الاحتيالي أحد أقدم أنواع الهجمات السبرانية ، ويعود تاريخه إلى التسعينيات. على الرغم من وجودها منذ عقود، إلا أنها لا تزال واحدة من أكثر الهجمات الإلكترونية انتشارا وضررا، وقد عرف على أنه: "إنها تقنية هندسة اجتماعية تهدف إلى التأثير على الهدف للكشف عن معلوماته الشخصية، مثل البريد الإلكتروني أو كلمة المرور أو أي معلومات مالية أخرى يمكن للمتسلل من خلالها السيطرة على الأرصدة المستهدفة". **(Alabdan, 2020, p. 01)**

كما تعرفه **Kaspersky** على أنه: " نوع من الاحتيال عبر الإنترنت يسعى إلى الحصول على بيانات اعتماد المستخدم عن طريق الخداع. يتضمن سرقة كلمات المرور وأرقام بطاقات الائتمان وتفاصيل الحساب البنكي وغيرها من المعلومات السرية" **(kaspersky, 2021)**.

2- هجمات التصيد الاحتيالي:

تنفذ هجمات التصيد الاحتيالي إما عن طرق نواقل أو عن طرق حيل تقنية يبتكرها المهاجمون ويعتمدونها في الوصول للبيانات السرية الخاصة بالضحية، والتي قد تنتهي بانتحال شخصية الضحية. الشكل الموالي يوضح أنواع هذه الهجمات .

الشكل رقم (01): أنواع هجمات التصيد الاحتيالي



المصدر: أنجز من طرف الباحثة وبتصرف بالاعتماد على **(Alkhali, Hewage, Nawaf, & Khan, 2021, p. 13)**

2-1- التصيد الاحتيالي باستعمال النو اقل:

- **الرسائل القصيرة:** يعمل التصيد الاحتيالي عبر الرسائل القصيرة على تعزيز الرسائل النصية بدلاً من البريد الإلكتروني لتنفيذ هجوم التصيد الاحتيالي. يرسل المهاجمون نصوصًا من مصادر تبدو مشروعة (مثل الشركات الموثوقة) تحتوي على روابط ضارة. قد يتم إخفاء الروابط كرمز قسيمة (خصم 20٪ على طلبك التالي!) أو عرضًا للحصول على فرصة للفوز بشيء مثل تذاكر الحفل**(security, 2021)** .

- **الصيد:** التصيد هو نسخة الهاتف من التصيد الاحتيالي أو عملية احتيال الصوت ، وقد 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 وخداع الضحايا لتحويل الأموال إليهم **(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 أن: تم اختراق حسابك يرجى ادخال تفاصيل تسجيل الدخول) **(Alabdan, 2020, p. 08)**
- **الشبكات الاجتماعية:** منذ بداية القرن 21، تطورت وسائل التواصل الاجتماعي بشكل كبير **(Twitter و Facebook و LinkedIn)** 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. تعد هذه الطبيعة لمشاركة التفاصيل الشخصية عبر الإنترنت مصدرا ممتازا للمحتالين لتحديد مجموعات الأهداف وربما الاقتراب من الضحايا.
- **مو اقع الويب:** تعد مواقع الويب الاحتيالية مصدرا آخر لهجمات التصيد الاحتيالي. تبدو هذه المواقع شرعية وتستخدم لجمع التفاصيل الشخصية للضحايا عندما يحاول الضحية تسجيل الدخول، ونظرا لأن المستخدمين العامين للإنترنت يميلون أكثر إلى الاعتقاد بأن هجمات التصيد 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 هجمات التصيد الاحتيالي.
- **الشبكة اللاسلكية (Wi-Fi):** يتم اختيار نقطة اتصال عامة معينة لأن هدفا معينا يزور بانتظام ويستخدم شبكة **Wi-Fi** يمكن أن يتخذ التصيد الاحتيالي لشبكة **Wi-Fi** عدة أشكال. يتضمن النموذج المعتاد تثبيت برامج ضارة على جهاز الضحية لجمع بيانات الاعتماد أو إعادة التوجيه إلى مواقع مخادعة. وهناك طرق أخرى لتتبع هذه الشبكات لسرقة المعلومات الشخصية التي يتم إرسالها من قبل الأشخاص الذين يستخدمون نقطة الاتصال العامة.

2-2- تقنيات التصيد الاحتيالي:

2-2-1- تسميم خادم اسماء النطاقات (DNS poisoning): يسمى كذلك الزرعة الخبيثة (**Pharming**)، ويقوم على تخريب خادم أسماء النطاقات **(Domain Name Server)** 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 من صحة العملية، وعليه فهود يقاد مباشرة نحو العنوان المزيف وبالتالي الاستيلاء على البيانات السرية والمالية للضحية (الغثبروبن هيشة، 2009، صفحة 60).

2-2-2- 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 يمكن حقن المحتوى الضار في موقع شرعي بثلاث طرق أساسية **(Alkhali, Hewage, Nawaf, & Khan, 2021, p. 15):**

- ✓ يستغل المقرصن ثغرة أمنية ويخترق خادم الويب.
- ✓ يستغل المقرصن ثغرة في البرمجة النصية عبر الموقع (XSS) وهي عيب برمجي يمكّن المهاجمين من إدراج نصوص برمجية من جانب العميل في صفحات الويب ، والتي سيتم عرضها من قبل زوار الموقع المستهدف.
- ✓ يستغل المقرصن ثغرة أمنية في إدخال لغة الاستعلام الهيكلية (SQL)، والتي تسمح للقراصنة بسرقة المعلومات من قاعدة بيانات موقع الويب عن طريق تنفيذ أوامر قاعدة البيانات على خادم بعيد.

2-2-3- هجمة الرجل في الوسط (Main in the Mddle Attack):

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 المضي قدمًا في سرقة بيانات الاعتماد ومعلومات الحساب والبيانات المالية واستخدام الموارد المصرح بها للمستخدم **(Alabdan, 2020, p. 20)**.

2-2-4- 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.

2-2-5- البرامج الخبيثة (Malware Attack):

كما يوحي الاسم ، يعد هذا نوعا من هجمات التصيد الاحتيالي التي يتم إجراؤها عن طريق تشغيل برامج ضارة على جهاز المستخدم ، ويتم 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**. ينتشر من خلال حملات التصيد الاحتيالي وتشمل نواقل الهجوم الرئيسية حقن الويب وتسجيل إدخال لوحة المفاتيح (للحصول على كلمات المرور ولصقها في حقول النموذج) ، واستغلال نظام مشاركة سطح المكتب

لحوسبة الشبكة الافتراضية (**VNC**). في عام 2018، وسعت برامج **Panda** الضارة أهدافها لتشمل تبادل العملات المشفرة ومواقع التواصل الاجتماعي **(Alkhali, Hewage, Nawaf, & Khan, 2021, p. 14)**. هناك العديد من الأشكال المستندة إلى البرامج الضارة كما يلي:

- **تسميم ملف الخوادم المضيفة (hosts file poisoning):** يشبه هذا الأسلوب إلى حد ما أسلوب تسميم خادم أسماء النطاقات، غير أنه يعتمد على تسميم ملف الخوادم المضيفة 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 العميل يقوم أولا بالبحث عن العنوان العشري لاسم الخادم في ملفات الخوادم قبل الاستعلام عن العنوان العشري لخادم أسماء النطاقات، وكما هو الحال في تسميم خوادم أسماء النطاقات يقوم المخربون بتسميم ملف خوادم المضيفة ف جهاز الضحية، وذلك بوضع سجل جديد لربط اسم نطاق معين بعنوان عشري لموقع مزيف (الغثبروبن 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, December 2020, p. 03)** مثل **key loggers and screen loggers** يتم إنشاء هذه البرامج لتسجيل ضغطات المفاتيح وإنشاء سجلات لكل شيء يكتب على لوحة مفاتيح الكمبيوتر ، ويمكن استخدام هذه البرامج للتحكم في الأجهزة أثناء استخدامها **(Kaspersky، 2021).**
- **برامج الفدية (Ransomware)**: تنتج عن نوع من البرامج الضارة أو البرام 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 عادةًكبرامج مكافحة فيروسات، تبدأ هذه البرامج بعد مرور بعض الوقت في مهاجمة نظام المستخدم. ثم يتعين على المستخدم أن يدفع للمجرمين لإزالة مثل هذه الفيروسات **(Manisha M & al, 2015, p. 745)**

2-2-6- محركات البحث (Search Engine Phishing):

تعتمد هذه الطريقة على إنشاء مواقع إلكترونية للبيع بالتجزئة **(Retail)** 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 (الغثبروبن هيشة، 2009، الصفحات 71-72).

2-2-7- النو افذ المنبثقة (The Pop Up Attack):

تعتبر الرسائل المنبثقة كونها تطفلية ، واحدة من أسهل الأساليب لإجراء عمليات الخداع في التصيد الاحتيالي. لأنها تسمح للمتسللين بسرقة تفاصيل تسجيل الدخول عن طريق إرسال رسائل منبثقة للمستخدمين وتوجيههم في نهاية المطاف إلى مواقع ويب مزورة، وضمن هذا النوع نجد **التصيد الاحتيالي أثناء الجلسة** الذي يعمل من خلال عرض نافذة منبثقة أثناء جلسة الخدمات المصرفية عبر الإنترنت ، ويطلب من المستخدم إعادة كتابة اسم المستخدم وكلمة المرور الخاصة به بعد انتهاء صلاحية الإصدار. يقوم المستخدم بإدخال تفاصيله ، دون أن يتوقع أن تكون النافذة المنبثقة عملية احتيال حيث قام بالفعل بتسجيل الدخول إلى مواقع البنك، كما نجد **دعم فني منبثق** وهو عملية احتيال أخرى منبثقة على نطاق واسع، فعند تصفح الإنترنت، يمكن أن يتلقى المتصفح فجأة رسالة منبثقة تفيد بأن نظامه مصاب ويحتاج إلى الاتصال بالبائع للحصول على الدعم الفني. **(Deloitte, December 2019, p. 10)**

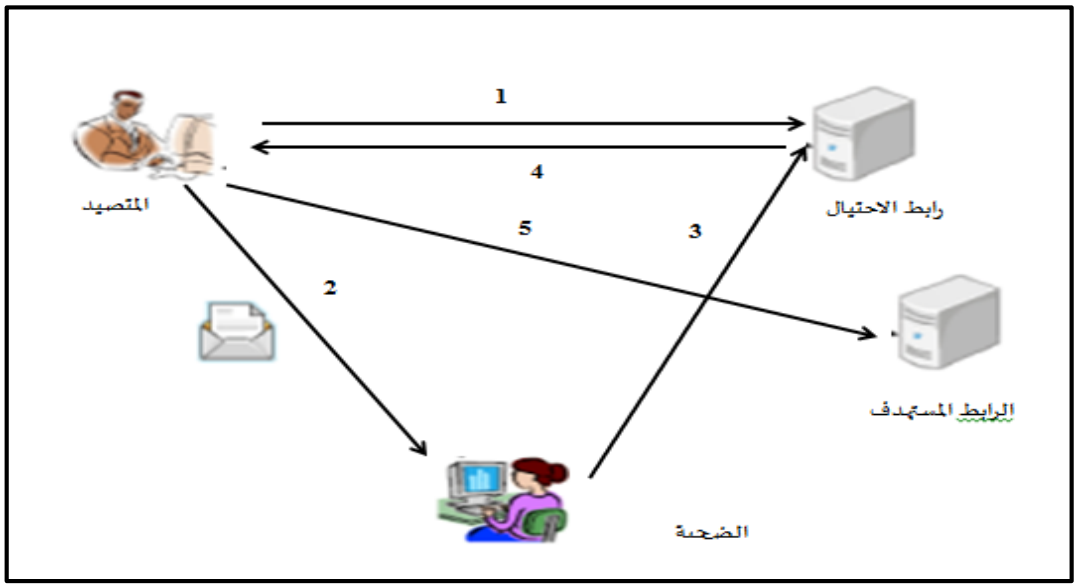
هجمات التصيد الاحتيالي لا تنفذ من قبل شخص واحد، بل مجموعة من الأشخاص المتخصصين في مجالات مختلفة تخدم عملية الهجوم ونجاحه. تتمثل هذه المجموعة فيما يلي **(الغثبروبن هيشة، 2009، صفحة 49)**:

- **المرسلون (Mailers):** هم مرسلو الرسائل غير المرغوبة (**Spammers**) أو المخربون (**Hackers**)، الذين لديهم القدرة على إرسال عدد هائل من الرسائل غير المرغوبة بهدف الاحتيال.
- **المجمعون (Collectors):** هم المخربون الذين جهزوا المواقع الإلكترونية المزيفة لغرض الاحتيال، وتحويل الضحايا إليها من قبل الرسائل البريدية غير المرغوبة، بعدها تطلب منهم هذه المواقع تزويدهم ببيانات سرية كاسم المستخدم ورقم المرور أ رقم البطاقة الائتمانية (المجمعون هم عملاء متكررين عند المرسلين وهم يدفعون مبالغا مادية مقابل إرسال الرسائل غير المرغوبة).
- **المحصلون (Cashers):** يمثلون الفئة التي تقوم بأخذ البيانات السرية المسروقة من قبل المجمعين، ومن ثم استغلالها، وينفذ الاستغلال بعدة طرق كإنشاء بطاقات ائتمان مزيفة، أو بطاقات حسابات بنكية مزيفة تستخدم للسحب النقدي المباشر من أجهزة الصراف الآلي، أو الشراء/البيع بواسطتها. تقوم هذه الفئة بالدفع المادي المباشر للمجمعين لقاء البيانات السرية المسروقة، أو بإعطائهم نسبة من المسروقات النقدية المحصلة.

3 – آلية هجوم التصيد الاحتيالي:

الدافع وراء هجوم التصيد الاحتيالي هو التلاعب بالضحية لتقديم معلومات سرية عنه. لتنفيذ مثل هذا الهجوم، يقوم المهاجم أو المخادع بمحاكاة بإنشاء موقع ضار باستخدام موقع ويب للتصيد الاحتيالي. سيجمع موقع التصيد الاحتيالي هذا كل المعلومات عن الهدف ويقدمها للمهاجم. عادة ، لا تستطيع الأهداف التمييز بين المواقع الأصلية ومواقع التصيد الاحتيالي مما يتسبب في وقوعها في الفخاخ التي وضعها المخادع.

الشكل رقم (02): خطوات التصيد الاحتيالي



Source : (Shankar, Shetty, & Nath K, 2019, p. 2172)

يبدأ المهاجم العملية بالتخطيط للهجوم. تتضمن هذه الخطوة تحديد موقع الويب الشرعي الذي يجب تقليده والضحية التي يجب جمع معلوماتها. يتبع بالتخطيط، إنشاء بريد إلكتروني يجب أن يبدو أصليًا حتى يتم إغراء الضحية بتقديم البيانات الجزء الثالث هو إرسال البريد الإلكتروني المؤلف إلى الهدف متبوعًا بجمع المعلومات عن الضحية إذا تم خداع الضحية من قبل المخادع. باستخدام معلومات الضحية، يرتكب المهاجم جرائم إلكترونية مثل الاحتيال على بطاقة الائتمان والسرقة وما إلى ذلك.

وبشكل أدفق يمكن توضيح خطوات التصيد الاحتيالي فيما يلي: **(Shankar, Shetty, & Nath K, 2019, p. 2172):**

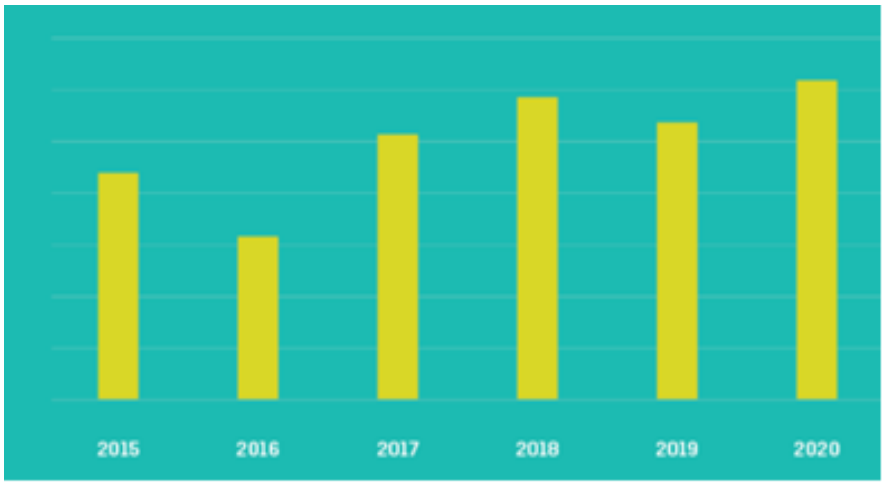
- ✓ **الخطوة 1:** يصمم المخادع بريدًا إلكترونيًا بمساعدة موقع ويب للتصيد الاحتيالي بحيث يبدو أنه حقيقي وشرعي.
- ✓ **الخطوة 2:** يرسل المهاجم هذا البريد الإلكتروني المؤلف إلى الضحية.
- ✓ **الخطوة3:** الضحية غير قادرة على التمييز بين رسائل البريد الإلكتروني الحقيقية ورسائل البريد الإلكتروني المخادعة، تميل إلى فتح البريد الإلكتروني. ثم يوجهها البريد الإلكتروني إلى موقع التصيد. تقوم الضحية بإدخال بيانات اعتماد تسجيل الدخول الخاصة بها في صفحة الويب متجاهلة حقيقة أنه موقع ضار.

- ✓ **الخطوة 4:** يقدم موقع التصيد الاحتيالي بيانات اعتماد تسجيل الدخول للمهاجم.
- ✓ **الخطوة 5:** يقوم المخادع باستخدام البيانات التي حصل عليها من موقع التصيد الاحتيالي ، بتسجيل الدخول إلى موقع الويب الضحية، وبالتالي الوصول إلى جميع المعلومات الخاصة بالضحية، ما يعني أن عملية التصيد قد اكتملت

ثانيا: أثر هجمات التصيد الاحتيالي على القطاع المالي

على غرار القطاعات الحيوية الأخرى، شهد القطاع المالي في عصر التحول الرقمي عدة أزمات مالية ساهمت في إعادة النظر حول أسبابها والمسؤول عنها. نسعى من خلال هذا العنصر لإبراز أثر التصيد الاحتيالي (باعتباره أحد أشهر الهجمات السبرانية) على القطاع المالي .

الشكل رقم (03): هجمات التصيد الاحتيالي خلال الفترة (2015-2020)



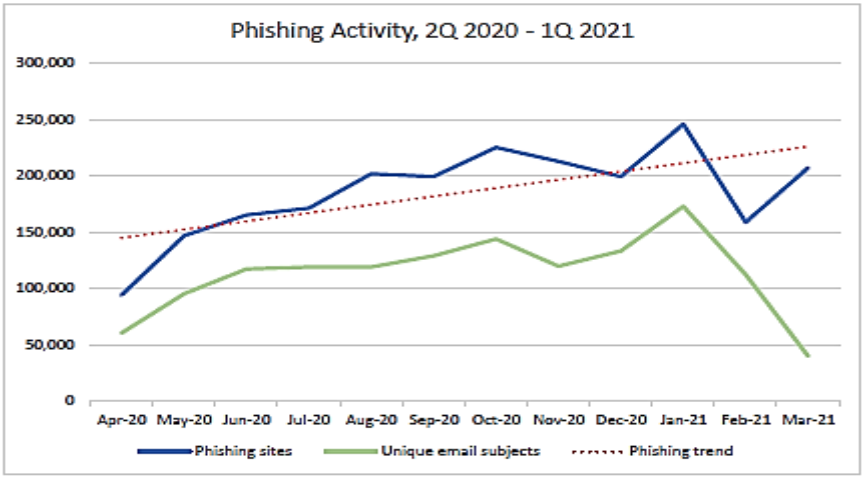
Source: (Warburton, 2020, p. 04)

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 بُعد 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)**.

وتجدر الإشارة إلى أن الولايات المتحدة الأمريكية والمملكة المتحدة وأستراليا صنفت في منطقة التعرض المنخفض والمعتدل، لكنها شهدت نسبة عالية من الانتهاكات السبرانية، 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، فخلال استطلاع (أجري وفق مؤشر التعرض للخطر السبراني) تم إجراؤه على مختلف بلدان العالم وجد أن **(Frisby, 2020)** :

- **أفريقيا:** مصنفة في مجموعة التعرض العالي بـ 0.643 نقطة (إثيوبيا هي أكثر البلدان تعرضا بـ 0.866نقطة، موريشيوس هي أقل البلدان تعرضاً بـ 0.200 نقطة).
- **آسيا والمحيط الهادئ:** مصنفة في مجموعة التعرض المعتدل مع 0.483 نقطة (أفغانستان هي الدولة الأكثر تعرضا بـ1.000نقطة، أستراليا هي أقل البلدان تعرضًا بـ 0.131 نقطة)
- **أمريكا الجنوبية:** مصنفة في مجموعة التعرض المعتدل بـ 0.541 نقطة (فنزويلا هي الدولة الأكثر تعرضا بـ 0.807. نقطة؛ أوروغواي هي أقل البلدان تعرضا بـ 0.348 نقطة).
- **أمريكا الشمالية:** مصنفة في مجموعة التعرض المعتدل بـ 0.207 ص (السلفادور هي أكثر البلدان تعرضا بـ 0.517 نقطة؛ الولايات المتحدة هي أقل البلدان تعرضا بـ 0.145 نقطة).
- **أوروبا:** مصنفة في مجموعة التعرض المنخفضة مع 0.207 نقطة (أرمينيا هي الدولة الأكثر تعرضا بـ 0.655 نقطة؛ وفنلندا هي أقل البلدان تعرضا بمعدل 0.110 نقطة).

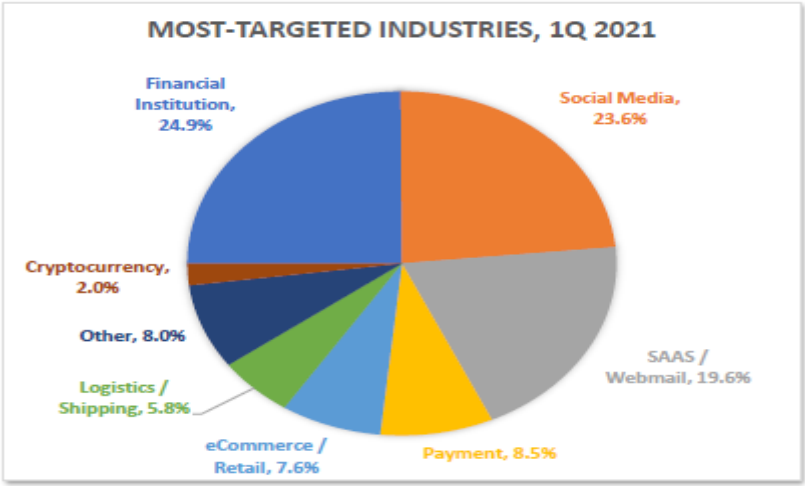
الشكل رقم (04): التصيد الاحتيالي خلال فترة كوفيد-19 (الربع$_2$ 2020-الربع$_1$ 2021)



Source: (APWG, 8 June 2021, p. 04)

يوضح الشكل السابق أعلاه تطور ونمو هجمات التصيد الاحتيالي الناجحة والمبلغ عنها خلال الربع الثاني من سنة 2020 وإلى غاية الربع الأول من سنة 2021، حيث نلاحظ تزايد الهجمات بشكل مستمر من بداية الجائحة خلال الربع الثاني من سنة 2020 وإلى غاية جانفي 2021 حيث يعتبر المحتالون أن فترة الوفاء فرصة لتكثيف أنشطتهم الإجرامية من خلال استغلال ضعف الموظفين الذين يعملون من المنزل والاستفادة من اهتمام الناس القوي بالأخبار المتعلقة بفيروس كورونا (مثل المواقع الإلكترونية الخبيثة المزيفة ذات الصلة بفيروس كورونا). اعتبار آخر مهم هو انخفاض تكاليف خرق البيانات المالية للضحايا. ونظرا لهذه الاعتبارات فقد تزايد حجم المواقع المسروقة خلال جانفي 2021.

الشكل رقم (05): الصناعات الأكثر استهدافا من طرف المتصيدين خلال فترة الكوفيد-19



Source: (APWG, 8 June 2021, p. 05)

أصبح القطاع المالي هو القطاع الأكثر استهدافا على مستوى العالم، على الرغم من انخفاض حجم الهجوم بنسبة 46% في منطقة آسيا والمحيط الهادئ، وقد اتسمت الهجمات ضد التمويل بالاستخدام المكثف لبرامج التجسس وأجهزة تسجيل المفاتيح، فضلاً عن الهجمات القائمة على التطبيقات **(NTT, 2018, p. 05)** .

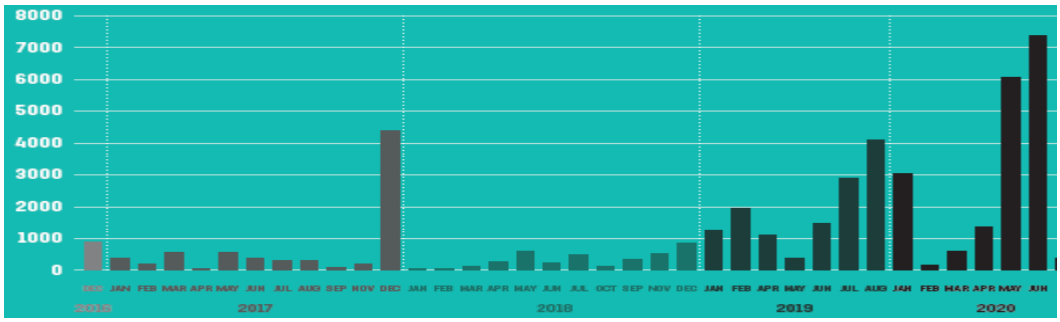
تبقى المؤسسات المالية الهدف الأكبر لهجمات التصيد الاحتيالي بشكل خاص، حيث وفي ظل أزمة كوفيد -19 وصلت نسبة الهجمات إلى ما يقارب 25% من إجمالي الهجمات ، والبارز في الأمر ومع تنامي سوق العملات المشفرة تزايدت عمليات الاحتيال عبرها باعتبار أن هذه العملات مجهولة المصدر ويشوبها الكثير من الغموض، فقد منع نظام 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 المحتالون بنشاط على إنشاء صفحات تسجيل دخول وهمية لخدمات العملة المشفرة على أمل الحصول على بيانات اعتماد المستخدم.

بالرغم من كون شركات التكنولوجيا المالية تعمل على تمكين المستهلكين والشركات من تحويل الأموال وإدارة الاستثمارات والوصول إلى الموارد المالية الشخصية والإقراض رقميا، لا سيما من خلال الأجهزة المحمولة، إلا أنها باتت هدفا مثاليا للقرصنة، فخلال سنة 2017 سجلت خسائر قدرت بـ 95 مليون دو لار راح ضحيتها كل من مؤسسة (**Tether**) ومؤسسة (**NiceHsh**)، وخلال جانفي إلى غاية أفريل سنة 2018 تم تسجيل خسائر بقيمة 737 مليون دولار منيت بها ثلاث مؤسسات مجتمعة (**Coincheck, BitGrail, Coinsecure**)، وهذا يعني أن تطور الوسائل الحمائية يتبعه تطور تقنيات الهجمات السبرانية **(Bouveret, June 2018, p. 09)**.

كان عام 2020 بالتأكيد عاما فريدا، حيث ارتفعت نسبة التصيد المالي إلى ما يقرب من 30% (بزيادة تقدر بـ 8% عن سنة 2019)، وصل التصيد البنكي إلى 10.72%فقط من الإجمالي. أما المتاجر الإلكترونية، فقد سجلت 7.57%في عام 2019 لتتضاعف ثلاث مرات تقريبا لتصل إلى 18.12%. يربط خبراء **Kaspersky** هذه التغييرات بإجراءات الإغلاق بسبب الوباء - في المنزل معظم الوقت ، لجأ الناس إلى التسوق عبر الإنترنت والترفيه الرقمي. وبالتالي ، أدى الطلب المتزايد من

المستخدمين إلى زيادة "العرض" من مجرمي الإنترنت. وتجدر الإشارة إلى أنه على الرغم من أن التسوق عبر الإنترنت أثبت أنه المجال الأكثر جاذبية للمحتالين ، إلا أن أنظمة الدفع لم تكن مغرية للغاية بالكاد وصلت حصتها إلى 8.41% على الرغم من التوسع الذي عرفته المدفوعات الرقمية غير التلامسية والذي فرضته طبيعة الوباء.

الشكل رقم (06): عدد بطاقات الائتمان المسروقة خلال الفترة (2015-2020)



Source: (Warburton, 2020, p. 16)

وبالحديث عن التصيد البنكي نجد أن 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.

الجدول رقم (01): أهم 10 دول أصيبوا بالبرامج الضارة البنكية التي تعمل بنظام Android في عام 2020

البلد	النسبة
اليابان	%2.83
تايوان	%0.87
إسبانيا	%0.77
إيطاليا	%0.71
تركيا	%0.60
كوريا	%0.34
روسيا	%0.25
طاجاكستان	%0.21
بولندا	%0.17
أستراليا	%0.15

source : (securelist, 2021)

يبين الجدول أعلاه أهم عشرة دول تعرضت أنظمتها البنكية للاحتيال عبر استخدام برامج ضارة تعما بنظام الأندرويد، ومعظم هذه الدول صنفت ضمن المناطق الأقل تعرضا للهجمات السبرانية، فمثلا أستراليا بالرغم من أنها الدولة الأقل تعرضا للهجمات السبرانية ضمن منطقة آسيا والمحيط الهادي إلا أنها شهدت تصيدا بنكيا بنسبة 15% وهذا ما يعزز فكرة أن هذه الهجمات لا تعترف بالحدود الإقليمية ولا بدرجة تطور البلد، وإنما يعمد القائمون عليها على اقتناء ضحايا يمكن من خلال تحقيق ثروات هائلة.

فيما نجد دول أخرى غابت عن هذا التصنيف بفضل تركيزها على الاستثمار في مجال الأمن السبراني، الذي شهد سوقه نموا كبيرا، حيث بلغت قيمته 167.13 مليار دولار أمريكي في عام 2020 ومن المتوقع أن يسجل معدل نمو سنوي مركب قدره 10.9% من 2021 إلى 2028. ويمكن أن يعزى نمو السوق إلى التطور المتزايد للهجمات الإلكترونية **(Grand View Reaserch, 2021)**

بالموازاة مع ذلك ، بلغ الإنفاق على الأمن السبراني 131 مليار دولار في عام 2020 ، ومن المتوقع أن يصل إلى 174 مليار دولار بحلول عام 2022 ؛ ويرجع هذا التوسع إلى وعي المنظمات بالحاجة إلى إيجاد طرق أكثر فاعلية لضمان حماية وسرية البيانات ضد الهجمات المستقبلية.

ثالثا: ممارسات الوقاية من هجمات التصيد الاحتيالي

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 ، وخلق مجموعة من الفرص للمشاركين في الصناعة، وضمن هذا العنصر نبرز أهم الجهود المبذولة لمواجهة هجمات التصيد الاحتيالي.

1- طرق عامة للوقاية من هجمات التصيد الاحتيالي:

ربما يتم تصنيف دراسات مكافحة التصيد وفقا لهدفها ، في مجموعتين كبيرتين هما تلك التي تهدف إلى التخفيف من رسائل البريد الإلكتروني المخادعة ، وتلك التي تهدف إلى تخفيف الهجمات على مواقع الويب. تلك الموجهة نحو مواقع الويب يمكن تصنيفها بشكل أساسي إلى ثلاث فئات مختلفة: (1) تركز على عنوان **URL** لموقع الويب ؛ (2) تركز على محتوى **HTML** ؛ (3) تركز على السلوك **(Bevavedes & al, 2020, p. 53)**. ويمكن أن نوجز أهم طرق حماية المعلومات فيما يلي:

- اقتناء أحد البرامج الأمنية الموثوقة والتي تكون مكافحة الفيروسات جزءا من عملها.
- استخدام برنامج مدير كلمات المرور **Password Manager**
- الالتزام بالتحديث لنظام التشغيل الأسبوعي وكذلك برامج الحماية.

- تحديث جميع البرامج والانتباه من البرامج المقرصنة والمجانية.
- البحث عن أي تحديث متوفر لجميع البرامج الموجودة على الجهاز.
- استخدام كلمة مرور قوية لكل حساب.

بالرغم من حجم الوعي والإدراك الذي وصلت إليه الدول، والذي تجلى في تركيزها على تطوير سوق الأمن السبراني والإنفاق عليه إلا أن الامر استدعى تدخل الهيئات الدولية التي عملت على توحيد الجهود لمواجهة الجريمة السبرانية.

1- منظمة التعاون الاقتصادي والتنمية (OECD):

تقترح منظمة التعاون والتنمية في الميدان الاقتصادي أن تضع البلدان الأعضاء المبادئ التوجيهية المتعلقة بالسياسات لإدارة الأمن السبراني على المستويات المؤسسية. يجب أن تؤكد المبادئ التوجيهية على ما يلي : **(Hamid Uddin & al, Auguste 2020, p. 55)**

- ✓ خلق الوعي بالمخاطر السبرانية وعواقبها.
- ✓ تحديد الأطراف المسؤولة عن شبكات نظام المعلومات.
- ✓ تحديد الفريق المسؤول للكشف عن التهديدات السبرانية ومنع الحوادث.
- ✓ ضمان المساءلة والأخلاقية معايير الأطراف المشاركة في إدارة الأمن السبراني.
- ✓ تطوير نظام أمني ضمن معايير الديمقراطية.
- ✓ تطوير نظام شامل لتقييم المخاطر لالتقاط التهديدات الأمنية من كل من التقنية (ضعف النظام) والمصادر غير التقنية (ضعف العوامل البشرية والسياسة).
- ✓ اعتماد **"القلق الأمني"** كمجال تركيز في جميع المجالات داخل المؤسسة.
- ✓ تصميم إطار إدارة أمن شامل وديناميكي يعتمد على نهج تقييم المخاطر الاستباقي والتطلعي.
- ✓ ضمان استمرار إعادة تقييم وتعديل السياسات الأمنية جنبًا إلى جنب مع التهديدات الأمنية المتغيرة ونقاط الضعف.

2- جهود لجنة بازل (BCBS):

باعتبار مخاطر الأمن السبراني ناتجة عن العنصر البشري فهي تعد أحد **أشكال المخاطر التشغيلية (Aldasaro & al, 14 January 2021, p. 03)**، وبالتالي فإن عملية تسييرها ليست عملية مستقلة بذاتها، وإنما هي ممارسات موجودة فعلا ضمن سياسات وإجراءات تسيير المخاطر التي تعتمدها المؤسسات ، وقد قدمت العديد من الدول والهيئات الدولية البارزة عدة أعمال إرشادية تتضمن اجراءات وسياسات لضبط هذه المخاطر باعتبار أن صحة الاقتصاد في المستقبل تعتمد على الاقتصاد الرقمي الموثوق. هذا الحديث يقودنا إلى ما ورد في وثيقة لجنة بازل التي صدرت في ديسمبر 2018، والتي تتضمن ممارسات **لحوكمة الأمن السبراني** وفق خمسة مبادئ كما يلي **(BCBS, December 2018, pp. 11-15)**:

- **استراتيجية الأمن السبراني:** هذه الاستراتيجية متوقعة وغير مطلوبة، بمعنى لا توجد معايير للأمن الإلكتروني وإنما هي موجودة فعلا ضمن السياسات الموضوعة لتسيير المخاطر، تفرض السلطات القضائية متطلبات استراتيجية الأمن الإلكتروني باستخدام ثلاثة أنواع من الأساليب التنظيمية غير الحصرية للطرفين:
  - ✓ تقوم الجهة التنظيمية / السلطة بتنفيذ متطلبات استراتيجية الأمن الإلكتروني ، سواء كانت خاصة بقطاع معين أو عبر صناعات متعددة ، والتي يتعين على المؤسسات المالية الامتثال لها. هذا النهج شائع في اقتصادات السوق الناشئة مع التجانس النسبي في أنظمتها المصرفية.
  - ✓ تضع المؤسسات المالية استراتيجيات الأمن الإلكتروني الخاصة بها وفقًا لممارسات إدارة المخاطر المستندة إلى المبادئ. يقوم المنظمون بمراجعة هذه الاستراتيجيات كجزء من تقييمهم لممارسات إدارة المخاطر الشاملة للمؤسسة
  - ✓ النهج الثالث ، السائد في أوروبا ، يتضمن فحص ما إذا كانت الكيانات المالية لديها استراتيجية لتكنولوجيا المعلومات والأحكام الأمنية المصاحبة.
- **المسؤوليات والأدوار:** ينص هذا المبدأ على تحديد الأدوار وتقسيم المسؤوليات لتفادي تداخل العمليات والمصالح، حيث أن وضع سياسات تسيير المخاطر يكون من طرف مجلس الإدارة والإدارة العليا، التي تعين مسؤول المخاطر الذي يتولى تنفيذها، ومهمة تسيير مخاطر الأمن الإلكتروني تسند إلى مسؤول أمن المعلومات الذي يقدم تقارير دورية لمسؤول المخاطر الإلكترونية.
- **التوعية بمخاطر الأمن السبراني:** يعد الوعي بالمخاطر الإلكترونية من قبل الموظفين في البنوك الفردية وثقافة المخاطر المشتركة من المتطلبات الأساسية للحفاظ على المرونة الإلكترونية داخل أي قطاع، وفي هذا السياق ، نشر العديد من المنظمين إرشادات تؤكد على أهمية الوعي بالمخاطر وثقافة المخاطر للموظفين والإدارة على جميع المستويات، ومن خلال هذا المبدأ يطلب المنظمون تدريبا للتوعية بالأمن الإلكتروني خلال كل مرحلة من مراحل عملية التوظيف، بدءا من التوظيف وحتى إنهاء الخدمة.
- **البنية الشبكية والمعايير التنظيمية:** لا توجد متطلبات تنظيمية عامة للبنية والمعايير، ولهذا يوجد عدد قليل فقط من البلدان التي تهتم بالرقابة والإرشادات الإشرافية الأساسية الخاصة بهيكل الأمن الإلكتروني (سبيل المثال يحدد كتيب فحص تكنولوجيا المعلومات الأمريكي **FFIEC** أنه عند مناقشة بنية الشبكة، يجب على المشرفين التأكيد على أن المخططات حديثة ومخزنة بشكل آمن وتعكس بنية أمان دفاعية قوية. في المملكة العربية السعودية ، تخضع الممارسات التي تغطي بنية الأمن الإلكتروني لتقييم ذاتي دوري).
- **القوى العاملة في مجال الأمن السبراني:** تختلف مهارات وكفاءات القوى العاملة وأطرها التنظيمية ومجموعة الممارسات بشكل ملحوظ، تمتلك بعض الولايات القضائية معايير خاصة بتكنولوجيا المعلومات تتناول مسؤوليات القوى العاملة في مجال تكنولوجيا المعلومات ووظائف أمن المعلومات، مع إيلاء اهتمام خاص لتدريب وكفاءات القوى العاملة في مجال الأمن الإلكتروني. تغطي مجموعة ممارساتهم الإشرافية تقييم أقسام

الفريق وخبرات الموظفين (عمليات الفحص الأمني لمتخصصي الأمن الإلكتروني) لا تزال معظم الدول في المراحل الأولى من تنفيذ الممارسات الإشرافية لمراقبة مهارات القوى العاملة الإلكترونية.

3- صندوق النقد الدولي (IMF):

في نوفمبر 2020 ، أصدر **CEIP** تقريرا بعنوان "**الإستراتيجية الدولية لحماية أفضل للنظام المالي العالمي من التهديدات السبرانية**". تضمن التقرير الذي تم تطويره بالتعاون مع المنتدى الاقتصادي العالمي، أربعة مبادئ **(Maure & Nelson, Spring 2021)**

- **أولا**، مزيد من **الوضوح** حول الأدوار والمسؤوليات مطلوب. لم يقم سوى عدد قليل من البلدان ببناء علاقات محلية فعالة بين سلطاتها المالية ، وإنفاذ القانون ، والدبلوماسيين ، والجهات الحكومية الأخرى ذات الصلة ، والصناعة. يعيق التجزؤ الحالي التعاون الدولي ويضعف القدرة الجماعية للنظام الدولي وقدرات التعافي، الاستجابة.
- **ثانيا**، **التعاون الدولي** ضروري وعاجل نظرا لحجم التهديد وطبيعة النظام المترابطة عالميا، لا تستطيع الحكومات الفردية والشركات المالية وشركات التكنولوجيا الحماية بفعالية من التهديدات الإلكترونية إذا كانت تعمل بمفردها.
- **ثالثا**، سيؤدي **الحد من التجزئة** إلى تحرير القدرة على معالجة المشكلة. هناك العديد من المبادرات الجارية لتحسين حماية المؤسسات المالية ، لكنها تظل معزولة. تتكرر بعض هذه الجهود مع بعضها البعض ، مما يؤدي إلى زيادة تكاليف المعاملات. العديد من هذه المبادرات ناضجة بدرجة كافية ليتم مشاركتها وتنسيقها بشكل أفضل وإضفاء المزيد من التدويل عليها.
- **رابعا**، يمكن أن تكون **حماية النظام المالي الدولي نموذجا للقطاعات الأخرى**. النظام المالي هو أحد المجالات القليلة التي يكون للدول فيها مصلحة مشتركة واضحة في التعاون ، حتى عندما تكون التوترات الجيوسياسية عالية. يوفر التركيز على القطاع المالي نقطة انطلاق ويمكن أن يمهد الطريق لحماية أفضل للقطاعات الأخرى في المستقبل

خاتمة:

هدفت هذه الدراسة إلى إبراز أثر التصيد المالي على القطاع المالي، وبدراسة المفاهيم المتعلقة بهذا النوع من الهجمات السبرانية، وجد أنه يضم العديد من التقنيات التي تختلف وتتنوع باختلاف الهدف وغاية مستعملها.

يعتبر القطاع المالي هشا للغاية في مواجهة هجمات التصيد الاحتيالي، نظرًا لأن المتسللين يمكنهم نشر الهجوم بسرعة من خلال النظام المالي المترابط ، ولأن معظم المؤسسات المالية لا تزال تستخدم الأنظمة الرقمية القديمة، فقد تم اكتشاف 91% من الهجمات في البنوك ، كان أكثر من 68% هجمات تصيد خلال عام 2020، أغلب هذه الهجمات تعتمد على برامج التجسس والبرامج الضارة.

معظم الدول التي تم اختراقها، لم يتم تصنيفها بالضرورة ضمن المجموعة الأكثر تعرضا، وكذلك أمريكا الشمالية التي تعرضت لأكثر من 52% من إجمالي الهجمات خلال عام 2020، فهذا يعني أن الهجمات الإلكترونية لا تتعلق بالحدود الإقليمية أو درجة التنمية. لكل بلد ، بل يرتبط بآليات القرصنة.

لا تزال الخسائر الناتجة عن الهجمات السبرانية تتزايد في ظل عدم وجود سياسات موحدة للأمن السبراني على المستوى العالمي ، وفي هذا الإطار تصر **BCBS** وصندوق النقد الدولي على العمل الجماعي لتعزيز ثقافة الوعي بالمخاطر السبرانية، حيث أن العمل الفردي مكلف للغاية ، والاستمرار في الإنفاق على تعزيز حماية البيانات في ظل التطور التكنولوجي هو في حد ذاته عبء مالي .

قائمة المراجع:

1. Adharsh, M., & Dhatchina, M. (December 2020). Cyber Attacks in banking industry. cyber attacks in banks. Bournemouth Project: cyber crime in banking.
2. 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), 01-39.
3. Aldasaro, I., & al. (14 January 2021). Covid-19 and cyber risk in the financial sector. Bulletin N 22, Bank of International Settlement, Basel.
4. Alkhali, Z., Hewage, C., Nawaf, L., & Khan, I. (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.
5. APWG. (8 June 2021). Phishing Activity Trends Report, 1st Quarter 2021. Anti-Phishing Working Group, San Francisco.
6. Asia, RSBP for Central. (2020). COVID-19: cybersecurity challenges for financial institutions.
7. BCBS. (December 2018). Cyber-resilience: Range of practice. Bank for International Settlement, Basel.
8. Bevavedes, E, Fuertes, W., Sanchez, S., & Sanchez, M. (2020). Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review. Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies,. 152, pp. 51-65. Singapore: Springer.
9. Bouveret, A. (June 2018). cyber security for the financial sector: A Framework for Qauntitave Assesment. Working paper, IMF.
10. Bulueliv. (2019). cyber threat intelligence for Banking &Financial services. spain: Bulueliv.
11. Deloitte. (December 2019). Understanding phishing techniques. Singapore: Deloitte; , Touche Enterprise Risk Services.
12. Frisby, J. (2020, JUNE 02). Cyber security Exposure Index (CEI). Retrieved 02 24, 2021, from Passwordmanagers.co: http://passwordmanagers.co
13. Grand View Reaserch. (2021, April). Cyber Security Market Size, Share & Trends Analysis Report By Component, By Security Type, By Solution, By Services, By Deployment, By Organization, By Application, By Region, And Segment Forecasts,

2021 - 2028. Consulté le April 27, 2021, sur Grand View Reaserch: http://www.grandviewreaserch.com

14. Hamid Uddin, M., & al. (Auguste 2020). Cyber security hazards and financial system vulnerability: asynthesis of literature. Risk Management N22.

15. Kaspersky. (2021). What is Kstroke Logging and Keyloggers. Consulté le 08 13, 2021, sur Kaspersky: http://www.Kaspersky.com

16. kaspersky. (2021). what is phishing. Retrieved August 10, 2021, from kaspersky: http://www.Kaspersky.com

17. 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).

18. Maure, T., & Nelson, A. (Spring 2021). the global cyber threat. IMF.

19. NTT, S. (2018). Global Threat Intelligence Report. Buenos Aires.

20. SecureList. (2020, April 16). Consulté le 03 05, 2021, sur Financial Cyber threats in 2019: https://securelist.com/financial-cyberthreats-in-2019/96692/

21. securelist. (2021, Mach 31). Financial Cyberthreats in 2020. Consulté le August 10, 2021, sur securelist: https://securelist.com/financial-cyberthreats-in-2020/101638/

22. security, p. (2021, April 12). 11 Types of Phishing + Real-Life Examples. Retrieved August 13, 2021, from panda security: https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/

23. Shankar, A., Shetty, R., & Nath K, B. (2019). A Review on Phishing Attacks. International Journal of Applied Engineering Research, 14(09), 2171-2175.

24. 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.

25. Warburton, D. (2020). 2020 phishing and fraud report. F5Labs, Seattle.

26. Yilamaz, S., & Zavrak, S. (2015). Adware: Are view. International Journal for Computer Science and Information Technology, 06(06).

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