ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

التهديدات السيبرانية –الهندسة الاجتماعية انموذجا–

- Cyber threats - social engineering as a model

محمد دحماني*
طالب دكتوراه، جامعة عمارثليجي الاغواط، كلية الحقوق والعلوم السياسية،
مخبر الحقوق والعلوم السياسية
mo.dahmani@lagh-univ.dz

تاريخ إرسال المقال: 01/ 08/ 2023 تاريخ قبول المقال: 14/ 08/ 2023 تاريخ نشر المقال: 15/ 09/ 2023

الملخص:

اليوم، يعيش العالم في عصر رقمي يتسم بالتطور التكنولوجي السريع وانتشار الاتصالات الإلكترونية، ومع هذا التطور، ظهرت تحديات جديدة تهدد أمن المعلومات والخصوصية، وتشكل التهديدات الإلكترونية جزءًا من هذه التحديات بجميع أشكالها المختلفة، تمثل الهندسة الاجتماعية أخطر هذه الأنواع، فهي شكل جديد من أشكال التهديد، تختلف عن طبيعة التهديدات التقليدية للأفراد والمجتمعات، بناءً على المنهج الوصفي التحليلي، وقد سلطت هذه الدراسة ونتائجها الضوء على ظاهرة السيبرانية التهديدات من خلال استخدام ما يسمى بالهندسة الاجتماعية، وفي نفس الوقت، إصدار التشريعات المتعلقة بالاستخدامات المختلفة للفضاء السيبراني

الكلمات المفتاحية: التهديدات السيبرانية، الهندسة الاجتماعية، الفضاء السيبراني، الامن السيبراني، الاختراق

Abstract: Today, the world lives in a digital age characterized by rapid technological development and the proliferation of electronic communications. With this development, new challenges have emerged that threaten information security and privacy, and electronic threats form part of these challenges in all their various forms. Social engineering represents the most dangerous of these types, as it is a new form of threat, different from the nature of traditional threats to individuals and societies, based on the descriptive analytical approach. This study and its results shed light on the phenomenon of cyber threats through the use of what is called social engineering, and at the same time, the issuance of legislation related to the different uses of cyberspace.

Keywords: cyber threats, social engineering, cyberspace, cybersecurity, penetration

* المؤلف المرسل

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

مقدمة:

ازداد تعقيد عالم اليوم وأصبح أصغر مما كان متوقعًا في عملية الاتصال والتواصل والتأثير، حيث هناك العديد من الطرق التي يمكن لأي فرد في هذا العالم استخدامها لتحقيق ما يريده ويطمح إليه، ويسعى كل فرد في هذا الكون إلى استخدام وسائل اتصال سهلة غير معقدة ، على العكس من ذلك ، أدى إلى تعقيد العلاقات الاجتماعية وبدأ يهيمن عليها السلبية في التواصل والفكر بسبب ما يحدث بين مستخدمي الوسائل الرقمية التي اجتاحت العالم ، والتي لم تتوقف عند حد معين، لكنها بدأت تخترق العقول البشرية بكل قوتها وتقنياتها في التعقيد ، بحيث انتقلت من التأثير الإيجابي إلى التأثير السلبي على الأفراد والجماعات والمجتمع بشكل عام ، ومع التبني الهائل والسريع للإنترنت واستخدام التقنيات الذكية، والأجهزة الإلكترونية ظهرت ظاهرة جديدة بكل جوانبها السلبية والإيجابية، وهي من بين التقنيات المستخدمة في جميع جوانب عمليات الأمن الشخصي والاجتماعي والوطني والتهديد السيبراني تسمى الهندسة الاجتماعية والتي تعتبر من أقوى التقنيات وأسرع التقنيات التي يستخدمها المهاجمون في الفضاء السيبراني، مما سبق ، يمكن طرح السؤال الرئيسي التالي.

الاشكالية: ما المقصود بالهندسة الاجتماعية في التهديدات السيبرانية وفيما تتمثل؟

ويتفرع عن هذا السؤال المركزي السؤالين التاليين:

أ. ما مفهوم التهديدات السيبرانية والهندسة الاجتماعية في الفضاء السيبراني؟

ب. ما مضامين الهندسة الاجتماعية في التهديدات السيبرانية؟

فرضية الدراسة:

تنطلق فرضية الدراسة من رؤية مفادها أن التهديدات السيبرانية لها جملة من الاشكال والطرق، تقع في فضاء مشترك واحد وهو الفضاء السيبراني وتعد الهندسة الاجتماعية من اخطرها.

أهمية الدراسة:

يكتسب موضوع الدراسة أهمية بالغة بالنظر لمدى حداثته، وضرورة البحث فيه وتكمن أهميته في:

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

• يعد موضوع الأمن السيبراني واستراتيجيات مواجهة التهديدات السيبرانية من أهم الموضوعات في الساحة الدولية، حيث برزت التهديدات الإلكترونية في مقدمة اهتمامات الباحثين والمهنيين، وهي من أهم الموضوعات اليوم في البحوث الأمنية والاستراتيجية.

• يتعلق الأمر بالحصول على فهم واضح للعلاقة بين التهديدات السيبرانية والهندسة الاجتماعية.

أهداف الدراسة :

يمكن تحديد أهداف البحث من حيث متغيرات الموضوع نفسه، وهي التهديدات السيبرانية على مستويات مختلفة، نظرًا لانتشار التقنيات الحديثة وقلة الوعي بين افراد المجتمع و نظرًا لمخاطرها وتأثيراتها، فقد تطرق الباحث إلى تحديد إحدى التقنيات التي يستخدمها المهاجمون السيبرانيون، حيث تتنافس التهديدات المتقلبة مع تطبيقات الأمن لأن عدم وجود أحدها يؤدي إلى تنفيذ الآخر، والغرض الرئيسي من هذه الدراسة هو تحديد مفهوم التهديدات السيبرانية وتأثيراتها المختلفة، وتأثير الهندسة الاجتماعية على الأمن الفردي والمجتمعي.

منهج الدراسة:

يعتمد الباحث في هذه الدراسة على المنهج الوصفي التحليلي الشائع الاستخدام في العلوم الاجتماعية والإنسانية بشكل عام، وفي العلوم السياسية بشكل خاص، والذي من خلاله يتم تحديد سمات وجوانب الظاهرة قيد الدراسة ووصفها بشكل موضوعي صريح، وجمع الأدلة والحقائق والبيانات، واستخدام أدوات وتقنيات البحث العلمي، وتحليل البيانات، ويتم وصفها واستخدامها على نطاق واسع في البحث لتفسير وتوصيف ظاهرة التهديدات الإلكترونية، فضلاً عن طبيعة ونوعية العلاقة بين الهندسة الاجتماعية والتهديدات السيبرانية.

هيكل الدارسة:

قسمنا هذه الدراسة إلى مبحثين رئيسيين هما:

المبحث: مفهوم التهديدات السيبرانية والهندسة الاجتماعية

المبحث الثاني: مضامين الهندسة الاجتماعية في التهديدات السيبرانية

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

الخاتمة: تضمنت نتائج الدراسة

المبحث الأول: المبحث الأول: مفهوم التهديدات السيبرانية والهندسة الاجتماعية

تعد التهديدات السيبرانية والهندسة الاجتماعية من الظواهر الخطيرة للغاية، حيث يمكن أن تؤدي إلى تداعيات وخيمة على المستوى الشخصي والمؤسساتي والوطني.

من خلال هذا المبحث سوف نتطرق في المطلب الاول منه، إلى مفهوم التهديدات السيبرانية والذي تضمن ثلاثة عناصر مترابطة مع بعضها البعض، أما المطلب الثاني فقد تم التطرق إلى مفهوم وطريقة عمل الهندسة الاجتماعية.

المطلب الأول: مفهوم التهديدات السيبرانية

إن العلاقة بين مفهومي "الأمن" و "التهديد" هي علاقة نفوذ متبادل، وأي محاولة لشرح الأمن يجب أن تبدأ بتحديد مصادر التهديد، حيث ان الدراسات الأمنية ركزت في الماضي على خطر الغزو العسكري، كأهم مصادر التهديد الأمني ، لكن الدراسات الحديثة ذهبت إلى وجود مصادر وأنواع أخرى من التهديد، من خلال هذا المطلب سنتناول النقاط التالية:

في العنصر الأول تم التطرق الى الفضاء الإلكتروني بأنه المجال الذي تحدث فيه جميع أنواع وأشكال الأعمال الإلكترونية، وفيما يتعلق بالعنصر الثاني، تمت مناقشة مفهوم الأمن السيبراني وأهم جوانبه وأهدافه، وأخيرًا، تم تعريف التهديدات السيبرانية وتم ذكر بعض أنواع هذه التهديدات ومجالات تطبيقها.

الفرع الاول: الفضاء السيبراني

الفضاء السيبراني كمجال جديد للعلاقات الدولية يمكن أن يتجاوز الحدود الوطنية ويملك قاعدة شاملة للسلطة للجهات الفاعلة الحكومية وغير الحكومية على حد سواء، وبالتوازي مع أنشطة المواطنين، يمثل امتدادًا للنشاط البشري أو طبيعة عسكرية، حتى في المجالات الدولية الأخرى، الأرض، البحر، الجو، الفضاء، إلخ.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

نشأ مصطلح "الحاكميات" في عمل نوربرت وينر، الذي قدم تعريف مصطلح "الحاكمية" في منتصف القرن العشرين، مشيرًا إلى أن التفاعل بين الإنسان والآلة يؤدي إلى خلق بيئات اتصال بديلة، ويشكل هذا الهيكل الأساسي لمفهوم الفضاء السيبراني. [1]

في أوائل الثمانينيات، صاغ الكاتب ويليام جيبسون مصطلح الفضاء الإلكتروني في رواياته عن المستقبل، واصفًا الفضاء الإلكتروني بأنه هلوسة متعاطفة يمارسها يوميًا بلايين المستخدمين في جميع البلدان، وإنه تعقيد لا يمكن تصوره.[2]

وبالتالي، فإن الفضاء السيبراني بالنسبة له ليس فضاء بيانات ثابتًا، لكن قنوات الاتصال الخاصة به تربط العالم الحقيقي وتسمح لمستخدمي هذا الفضاء بطرق التفاعل مع ذلك العالم، على الرغم من وضع العبارة في سياق الخيال العلمي، إلا أنها أصبحت تستخدم على نطاق واسع بين الأكاديميين والمتخصصين في هذا المجال، خاصة مع ظهور وانتشار الإنترنت وانتشار الرقمنة.

في أوائل التسعينيات، وضع جون بيري بارلو العبارة كمفهوم معاصر في سياق وصفه للعلاقة بين أجهزة الكمبيوتر والشبكات السلكية واللاسلكية. [3].

الفضاء الإلكتروني هو عالم افتراضي من صنع الإنسان يعتمد على أنظمة الكمبيوتر وشبكات الإنترنت وكميات هائلة من البيانات والمعلومات والأجهزة.

أما القاموس العسكري لوزارة الدفاع الأمريكية، فيعرّف الفضاء الإلكتروني بأنه: جبل جليد، وبدلاً من الاعتماد كليًا على البيئة المحوسبة التي توفرها شبكات المعلومات، فإن كمية المعلومات الرقمية التي تغطي مجموعة واسعة من المفردات مثل سرعة نقل البيانات والوصول إلى الشبكة، بالإضافة إلى المعالجات التي تتعامل مع تدفق البيانات في بيئة الفضاء الإلكتروني.[4]

يتكون الفضاء السيبراني من عناصر مادية مثل الكابلات والمحولات والبنية التحتية للمعلومات والمحتوى الأخلاقي (البرمجيات) الذي يعكس شكل المعلومات في الفضاء السيبراني، والمكون الثالث هو عملية الاتصال بين المعلومات والأشخاص، والتفاعل بين البرمجيات والأجهزة، ومدى ملاءمتها لتصورات المستخدم البشري وقيمه وسلوكياته[5].

---

[1] عادل عبد الصادق ، **أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني** ، مكتبة الإسكندرية وحدة الدراسات المستقبلية ، الاسكندرية، 2016, ص 7.

[2] انديرا عراجي ، **القوة في الفضاء السيبراني: فصل عصري من التحدي والاستجابة** ، رسالة لنيل شهادة دراسات عليا في العلوم السياسية والإدارية، كلية الحقوق والعلوم السياسيه، لبنان،2016 , ص 08.

[3] انديرا عراجي، نفس المرجع ، ص 08

[4] عادل عبد الصادق ، مرجع سبق ذكره, ص11

[5] عادل عبد الصادق ، نفس المرجع,, ص 12

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

أصبح الفضاء الإلكتروني أحد العوامل الرئيسية المؤثرة في النظام الدولي، ليس فقط لأنه يؤثر على القيم السياسية، ولكن أيضًا لأنه يوفر أداة تكنولوجية مهمة في عملية تعبئة العالم وتعبئته، عسكري، اجتماعي.... الخ.

أصبح من الواضح أن أي شخص لديه آليات لاستخدام الفضاء الإلكتروني سيكون قادرًا على تحقيق أهدافه والتأثير على سلوك الجهات الفاعلة التي تستخدم هذه البيئة.

وحتى وقت قريب، كان يُنظر إلى الفضاء الإلكتروني على أنه مصطلح يشير إلى القضايا السياسية الثانوية والظروف الاجتماعية والاقتصادية التي لا تؤثر في المقام الأول على استقرار أي بلد، ومع ذلك، فقد أصبحت اليوم قضية سياسية أكثر تعقيدًا، مثل إغلاق الإنترنت أو تسريب المستندات خلال فترة عدم الاستقرار المحلي، الحكومات السرية والهجمات الإلكترونية كلها أمثلة على كيف لا يمكن تجاهل وجود الفضاء السيبراني وإمكاناته. [6]

الفرع الثاني: الامن السيبراني

1. تعريف الامن السيبراني

يُعرّف الأمن السيبراني بأنه: "أمن الشبكات وأنظمة المعلومات والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، لذلك فهو مجال متعلق بالإجراءات والمعايير الوقائية التي يجب اعتمادها والالتزام بها من أجل التعامل مع التهديدات"، انتهاك لـــمنع، أو على الأقل الحد من تأثيره" .

يعرّف Richard A. Kemmerer الأمن السيبراني بأنه "وسيلة لتقليل مخاطر الهجمات على البرامج أو أجهزة الكمبيوتر أو عناصر التحكم، بما في ذلك الوسائل والأدوات المستخدمة."

محاربة القرصنة واكتشاف الفيروسات ووقفها" [7]

بناءً على الغرض منه، يضمن الأمن السيبراني حماية الموارد البشرية والمالية المتعلقة بتكنولوجيا الاتصالات والمعلومات والقدرة على تخفيف الخسائر المتكبدة في حالة المخاطر والتهديدات، وعملياتها ووظائفها ونظم معلوماتها والمعلومات الواردة فيها محمية من مصادر الضرر.

2. أبعاد الأمن السيبراني:

[6] انديرا عراجي ،مرجع سبق ذكره ، ص 14

[7] لامية طالة, **التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها**،مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد04, العدد 02، 2020، ص ص 60- 61.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

يؤثر الأمن السيبراني على جميع القضايا العسكرية والاقتصادية والاجتماعية والسياسية والإنسانية ويحدد بوضوح جوانب الأمن السيبراني من أجل تحقيق نظام أمني متكامل يعمل على حماية الأمن القومي من جميع التهديدات السيبرانية، وتشمل الجوانب الاتية:[8]

أ. الجوانب العسكرية:

الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يتيح تبادل وتدفق المعلومات والأوامر، وهذه هي الفكرة التي يتم من خلالها إنشاء الشبكات وتطويرها للوصول إلى الإنترنت والأهداف البعيدة، ومع ذلك، فهذه نقطة ضعف خاصة إن لم تكن محمية بشكل كاف من التطفل، والتي يمكن أن تؤدي إلى تدمير قواعد البيانات العسكرية، وتعطيل الاتصالات بين الوحدات القيادية والعسكرية، والقدرة على التحكم في بعض قواعد البيانات.

ب. الجانب الاقتصادي:

نظرًا لاستخدام أجهزة الكمبيوتر لتشغيل وتطوير الصناعات ودفع الاقتصاد، فقد أصبح الإنترنت أساس التجارة والتمويل والمعاملات الاقتصادية، وكل شيء مترابط من خلال شبكات الكمبيوتر

ت. الجوانب الاجتماعية:

يوجد أكثر من 4 مليارات مستخدم للإنترنت في جميع أنحاء العالم، منهم أكثر من 2.6 مليار يستخدمون مواقع الشبكات الاجتماعية، وهذا يجعل مواقع التواصل الاجتماعي أكثر تفاعل بشري كثافة، تاركة الباب مفتوحًا على مصراعيه لتبادل الأفكار والتجارب الإيجابية، وبدلاً من ذلك، تتعرض أخلاق المجتمع للخطر بسبب صعوبة مراقبة محتوى الإنترنت وتعرض المعلومات الشخصية لأنشطة القرصنة الخارجية التي قد تهدد السلام الاجتماعي للأمة.

ث. الجوانب القانونية:

يتطلب التطور التكنولوجي السريع الامتثال للقوانين القانونية من خلال تطوير الأطر والقوانين للعمليات القانونية وغير القانونية في الفضاء السيبراني.

ج. الجانب السياسي:

يعد التدخل الإلكتروني الروسي في الانتخابات الأمريكية أهم دليل على ضرورة وأهمية الأمن السيبراني في المجال السياسي، بخلاف التسريبات والتنازلات للوثائق السرية التي غالبًا ما تؤدي إلى أزمات

[8] محمد مختار،الأمن السيبراني مفاهيم المستقبل، مجلة اتجاهات الأحداث ،العدد 02، 2015، ص06.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

دبلوماسية بين الدول، ويُعتقد أن هناك علاوة على ذلك، أصبح الفضاء الإلكتروني بيئة خصبة للحملات لمختلف الجهات الفاعلة الدولية.

الفرع الثالث: التهديد السيبراني

1) تعريف التهديد السيبراني:

التهديد بالمعنى الاستراتيجي هو صراع المصالح والأهداف الوطنية، وإيجاد حل سلمي يوفر لكل أمة حد أدنى من الأمن السياسي والاقتصادي والاجتماعي والعسكري مقابل افتقارها، يُعرّف بأنه الوصول إلى مرحلة يكون فيها هو مستحيل ان القدرة على موازنة الضغوط الخارجية التي قد تعرض الأمن القومي للطرف الآخر للخطر من خلال إجبار الطرف الآخر في النزاع على استخدام القوة العسكرية.[9]

التهديد: وبحسب باري بوزان، فهو: "تهديد للمؤسسات الوطنية التي تستغل الفكر أو تثبت قدرات دولة ما لدولة أخرى، وأن أراضي ذلك البلد تتضرر أو تتضرر أو تدمر، ويمكن أن تكون مهددة بالغزو والاحتلال، والتهديدات يمكن أن تأتي من الخارج والداخل ".[10] "

السيبرانية: تأتي من كلمة cyber وتعني أي شيء يتعلق أو يتعلق بأجهزة الكمبيوتر وتكنولوجيا المعلومات والواقع الافتراضي. الكلمة مشتقة من Kybernetes اليونانية، والتي تعني الأمر أو التعليمات، وعلم التحكم الآلي، علم التحكم الآلي، علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والكائنات الحية.[11].

يعني التهديد السيبراني إساءة استخدام أجهزة الكمبيوتر وتكنولوجيا المعلومات لتخريب البنية التحتية للمعلومات الخاصة بالعدو وتدميرها، وكذلك تخريب شبكات الدفاع الجوي، وحرق أنظمة المعلومات الخاصة بمكتب البريد الإلكتروني لرئيس الدولة، وقد يتجسس أيضًا وفقًا لمنهجيات مدروسة، لذلك، فإن التهديد السيبراني أو الهجوم السيبراني يهدد الأمن الاجتماعي والأمن الاقتصادي القومي والأمن القومي والأبعاد العسكرية، ويتم استهداف التهديدات الإلكترونية لأنها تؤثر على الأبعاد الأخلاقية والمادية على جميع المستويات.[12].

---

[9] أحمد عبد الحليم، **أمن الخليج: إلى أين؟** ، اوراق الشرق الأوسط، 1992, ص،ص 28-29 .

[10] تيري ديبيل، **استراتيجية الشؤون الخارجية...منطق الحكم الأمريكي**، ترجمة :وليد شحادة ، دار الكتاب – العربية ومؤسسة محمد بن آل راشد آل مكتوم، بيروت، 2009 ، ص258

[11] معجم اكسفورد على الرابط: http:// en.oxforddictionaires.com/ definition/cyber

[12] ادريس عطية ،**مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، مجلة مصداقية، جامعة العربي تبسي، تبسة، المجلد 01، العدد 01،2019 ،ص 108.

التهديد السيبراني هو عملية تخويف وترهيب الضحية باستخدام الفضاء الإلكتروني، ووسائل الإعلام، وأجهزة الاتصال، واستخدام الإنترنت، وتدفق المعلومات والبيانات، حيث يشكل ذلك تهديدًا للضحية من عدة جوانب، ويمكن القول تؤثر هذه التهديدات على الأفراد والجماعات وحتى الدول

2) انماط التهديدات السيبرانية

تتميز التهديدات السيبرانية ان لها اشكال وانماط عديدة باستطاعتها مهاجمة الحسابات والاجهزة، وعمومًا نجدها في ثلاث فئات متمثلة في الهجمات على النزاهة والسرية والتوافر.

- **التعدي على الخصوصية:**

يتم فيها سرقة معلومات الحساب المصرفي وبطاقات الائتمان ومعلومات التعريف الشخصية حيث يسرق العديد من المتسللين المعلومات، ويبيعونها للآخرين على شبكة الإنترنت المظلمة، ويشترونها ويستخدمونها بشكل غير قانوني.

- **الهجوم على النزاهة**

تتكون هذه الهجمات من أعمال تخريبية (تسمى غالبًا تسريبات) من قبل أفراد أو منظمات، وفي هذا العمل التخريبي، يقوم مجرمو الإنترنت بالوصول إلى المعلومات الحساسة وكشفها بهدف كشف البيانات والتسبب في فقدان ثقة الجمهور في تلك المعلومات، منظمة أو شخص.

- **هجمات التوافر**

تتجسد في منع المستخدمين من الحصول إلى بياناتهم الشخصية حتى يقدموا رسومًا أو فدية معينة.

3) مجالات التهديدات السيبرانية:

- **التهديدات المستمرة المتقدمة:**

يُعرف باسم APTS، وهو نوع من هجمات التكامل حيث يدخل مستخدم ضار إلى شبكة دون أن يتم اكتشافه ويبقى هناك لفترة طويلة من الوقت والغرض من APTS هو غملية سرقة البيانات من غير افساد الشبكة وتحدث غالبا APTS في القطاعات التي تحتوي على معلومات عالية القيمة، مثل الدفاع وشركات التصنيع والمنصات المالية.

- **البرمجيات الخبيثة وبرامج التجسس:**

هذا نوع من هجوم الإتاحة ويشير هذا إلى البرامج المخصصة للوصول إلى الأجهزة والحواسيب أو افساده بدون اخبار وعلم المالك وتشمل أنواع البرامج الضارة المعروفة.

- **الهندسة الاجتماعية:**

هذا شكل من أشكال انتهاك الخصوصية الذي ينطوي على التلاعب النفسي في تنفيذ إجراء ما أو إكراه الضحية على التخلي عن معلومات مهمة، وسيتم شرح ذلك لاحقًا.

المطلب الثاني: الهندسة الاجتماعية –التعريف وطريقة العمل –

عندما يفكر معظم الناس في الأمن السيبراني، فإنهم يفكرون في الحماية من المتسللين الذين يستخدمون الثغرات التقنية لمهاجمة شبكات البيانات، ولكن هناك طرقًا أخرى لتهديد المنظمات والشبكات، يتعلق الأمر باستغلال نقاط الضعف البشرية، يُعرف هذا باسم الهندسة الاجتماعية وينطوي على خداع شخص ما للتخلي عن المعلومات أو منح الوصول إلى شبكة البيانات من خلال هذا العنصر سيتم التطرق الى تعريف الهندسة الاجتماعية – امنيا و اجتماعيا –واهم اهداف الهندسة الاجتماعية ، وكيف تؤثر الهندسة الاجتماعية على عقول الناس، وتغير بعض تصوراتهم، وتضليل الناس.

الفرع الأول: تعريف الهندسة الاجتماعية

أ. **التعريف الامني:**

- تشير الهندسة الاجتماعية: امنيا إلى التأثير والتلاعب بالآخرين من أجل الكشف عن المعلومات الشخصية، وهذا الاستخدام للهندسة الاجتماعية يندرج تحت ما يسمى بالخدعة أو خدعة الثقة، مما يعني كسب ثقة شخص ما ثم خداعهم للحصول على بيانات حساسة للاحتيال عليهم أو استخدامها لأغراض شخصية أو مهنية.

- الهندسة الاجتماعية: المعروفة أيضًا باسم القرصنة البشرية، هي فن خداع الموظفين أو المستهلكين للكشف عن بيانات اعتمادهم واستخدامها للوصول إلى الشبكات والحسابات.

- الهندسة الاجتماعية: هي تلاعب نفسي، واستراتيجيات هجوم تعتمد على التفاعل البشري، وخطط احتيال متطورة، وتقنيات لاستخراج معلومات حساسة عن طريق خداع الأفراد لتقديم معلومات مثل كلمات المرور، ويفضل المجرمون استغلال ثقة الناس على التكنولوجيا، لأنه من الأسهل استغلال ميول الناس الطبيعية للثقة، وهذا يؤدي إلى قلة الوعي بهذه الجرائم، ناهيك عن التغاضي عن الهندسة الاجتماعية وعدم التعامل معها على أنها تهديد خطير.

ب. **تُعرّف الهندسة الاجتماعية اجتماعياً**

بأنها تؤثر على السلوك الاجتماعي ونمط الحياة وعقلية المجتمع بأسره. يستخدم المهندسون الاجتماعيون المعرفة المكتسبة لتغيير سلوك الناس وطرق التصرف والتفكير لتحقيق الأهداف والهجمات المرغوبة، باستخدام وسائل التواصل الاجتماعي بخلاف الهجمات مثل تخمين كلمة المرور لتحقيق غرض معين، وفي هذه الحالة، ترتكز جهود الهندسة الاجتماعية على المنهج العلمي المعروف بجمع البيانات وتحليلها واستخلاص النتائج الملموسة وتقديم توصيات واضحة يمكن تطبيقها وتطبيقها علميًا.[13]

ويتحدث الكاتب الأمريكي كريستوفر هادناجي عن الهندسة الاجتماعية للهاكر وفن اختراق العقل البشري، وعرفها بأنها مجموعة من الأنماط والسلوكيات البشرية التي نمارسها عن قصد أو عن غير قصد، والتي يستخدمها بشكل عام متخصصو التسويق لإقناع الإنسان والجمهور لمنتج معين والترويج للمؤسسات، كما هو مستخدم في العالم السياسي لكسب استحسان الجمهور، كما يستخدمه الأطباء أحياناً لتشجيع مرضاهم على اتباع نظام غذائي معين، على سبيل المثال لصالح صحتهم.[14]

من خلال ما سبق يمكن القول ان الهندسة الاجتماعية هي فن وعلم التلاعب بالأشخاص والتأثير عليهم للحصول على معلومات سرية أو للقيام بأعمال غير قانونية أو ضارة، وتستخدم الهندسة الاجتماعية في العديد من المجالات مثل الاحتيال الإلكتروني والتجسس والقرصنة الإلكترونية، ويستخدم المهندسون الاجتماعيون ضعف البشر والثقة الزائدة في الوصول إلى المعلومات الحساسة أو إقناعهم باتخاذ إجراءات غير مرغوب فيها.

---

[13] **فارس محمد العمارات، الهندسة الاجتماعية واختراق عقول البشر تم الاطلاع على الموقع في 12/04/2023على الرابط–https://www.new-educ.com/%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9-%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D8%B9%D9%82%D9%88%D9%84-%D8%A7%D9%84%D8%A8%D8%B4%D8%B1**

[14] **ما هي الهندسة الاجتماعية ؟طرقها وكيف تتجنبها** متوفر على الرابط، تمت زيارته في 10 06 2023 https://www.it-pillars.com/ar/blog/%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9/

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

الفرع الثاني: اهداف الهندسة الاجتماعية

الغرض الرئيسي من الهندسة الاجتماعية مشابه للقرصنة، وهذا يعني الوصول إلى أنظمة غير مصرح بها أو الحصول على معلومات من خلال الخداع أو التجسس على الشبكة أو التجسس على خطوط الإنتاج أو انتحال الهوية أو تعطيل النظام أو الشبكة، وعادة ما يتم استهداف شركات الاتصالات والشركات المعروفة والمؤسسات المالية والجيش والوكالات الحكومية والمستشفيات لهذا النوع من الهجمات، ويتمتع الإنترنت أيضًا بنصيب عادل من هذه الأنواع من الهجمات، لكن المهاجمين يركزون عادةً على أهداف كبيرة ومن الصعب جدًا العثور على أمثلة من العالم الحقيقي لهجمات الهندسة الاجتماعية، لا تفصح المؤسسات المستهدفة علناً عن تعرضها لهذا النوع من الهجمات لأنها تجعلها تبدو سيئة أمام عملائها وتؤثر على سمعة المنظمة نفسها، يظهر هذا الهجوم أن موظفي المنظمة ليسوا على علم بذلك. مستوى الذكاء والاجتهاد المطلوب[15]

المبحث الثاني: مضامين الهندسة الاجتماعية في التهديدات السيبرانية

الهندسة الاجتماعية هي واحدة من أحدث التقنيات التي يستخدمها المهاجمون السيبرانيون للحصول على معلومات حساسة والوصول بشكل غير قانوني إلى أنظمة الكمبيوتر، وتعتمد هذه التقنية على استغلال الجانب الإنساني من عملية الهجوم، باستخدام الخداع والتلاعب النفسي لإقناع الأفراد بالكشف عن معلومات حساسة أو القيام بأعمال غير مرغوب فيها ، من خلال هذا المحور سوف نتطرق الى الأساليب المتبعة في الهندسة الاجتماعية ثم نتطرق بعدها الى اهم مراحل تنفيذ الهندسة الاجتماعية وفي الأخير نتكلم عن اهم طرق الوقاية من اخطار الهندسة الاجتماعية

المطلب الأول: الأساليب المتبعة في الهندسة الاجتماعية

الهندسة الاجتماعية هي أداة قوية للمهاجمين السيبرانيين لأنها يمكن أن تستغل الثقة المفرطة الشخصية، وتستغل الجهل، ويمكن أن تتخذ الهندسة الاجتماعية عدة أشكال، بما في ذلك رسائل البريد الإلكتروني المزيفة والمكالمات الهاتفية المزيفة والرسائل النصية المزيفة والتلاعب بوسائل التواصل الاجتماعي، ومن أهم تقنيات الهندسة الاجتماعية نجد:

[15] https://mafhome.com/%D9%85%D8%A7-%D9%87%D9%8A-%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%D8%A7%D9%84%D8%A5%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9 متوفر على الموقع-

- **سرقة الهوية**

من السهل إنشاء حساب أو بريد إلكتروني على منصة وسائط اجتماعية باسم مزيف أو بنفس اسم شخص تعرفه، نحن نطلق على هذا الانتحال لأن منتحل الشخصية يسيء إلى ثقتك للحصول على معلومات معينة أو الانضمام إلى شبكات معينة، ومنظمة سرية لغرض جمع المعلومات.

- **سمعة وهمية لتطبيق معين**

هنا، يدعي المهاجم أن الرابط أو الملف هو نفس إصدار محدث من تطبيق معين، ولكنه يحتوي بالفعل على ملفات ضارة، أشهر مثال في حالة سوريا هو اعتماد تطبيقات وهمية ومعدلة لتطبيق المراسلة WhatsApp.

- **التقاط كلمة المرور**

كيفية الحصول على كلمة مرور لمستخدم خدمة أو موقع ويب، وتستند هذه الحيلة إلى وهم أن الضحية على موقع عادي وشرعي، بينما في الواقع هو موقع "مزيف" يديره لص كلمة مرور، لذلك إذا تم خداع المستخدم لإدخال كلمة مرور على هذا الموقع، فسيتم منح كلمة المرور ببساطة للسارق.

- **الضحية يفتقر إلى الخبرة الفنية**

يستغل المهاجمون الرقميون الخبرة التقنية الضعيفة للأفراد أو المجموعات المستهدفة للتمييز بين الملفات المشروعة والخبيثة. على سبيل المثال، يدعي المهاجم أن هذا الرابط أو الملف يساعد في حماية جهاز الضحية من الفيروسات، على الرغم من أنه ضار بالفعل، وملف أو ارتباط.

- **إساءة استخدام الشائعات**

يستفيد المهاجمون من قابلية انتشار الشائعات على الشبكات الاجتماعية، وخاصة WhatsApp و Facebook، لتمرير المحتوى الضار عبر البرامج والروابط الوهمية، وخداع الضحايا للنقر على الروابط، والحصول على كلمة مرور، الهواتف، وما إلى ذلك.

- **استغلال عواطف الضحية**

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 681- 701

يشير الاستغلال العاطفي إلى استخدام نصوص أو صور تخاطب الضحية ومشاعرها، مثل الحب والخوف والحزن والكراهية والرغبة في الانتقام والكراهية، ويستخدم المهاجمون فضول أهدافهم لخداعهم لفتح ملفات أو روابط ضارة.

- **استغلال التواجد المادي للمهاجم في المنطقة المجاورة مباشرة للضحية**

على سبيل المثال، الجاني والضحية في نفس المكان، في هذه الحالة، يمكن للمهاجم استخدام المعلومات الاستخباراتية للوصول إلى جهاز الكمبيوتر المحمول الخاص بالضحية، والهاتف المحمول، وما إلى ذلك. ان من الحكمة ضمان خصوصية المعلومات الشخصية المنشورة على "الويب" لتجنب الوقوع ضحية للهندسة الاجتماعية، وهذا لأنه يمكن أن يكون هدفًا سهلاً للمهاجمين، ولا يجب أبدًا مشاركة كلمات المرور مع الآخرين أو تخزين كلمات المرور، والاحتفاظ به في مكان يسهل الوصول إليه، وفحص جميع الملفات والروابط إلى الحسابات، ولا يتم فتح الملفات أبدًا مباشرة قبل التحقق من أنها لا تحتوي على برامج ضارة.

- **الاستفادة من الموضوعات الشائعة**

على غرار استغلال الشائعات، يُنظر إلى الموضوعات الساخنة على أنها طعم مناسب لتضليل الضحايا للاعتقاد بأن الروابط المرفقة بالرسائل آمنة من البرامج الضارة، ويستخدمها المهاجمون لتمرير عمليات الاحتيال الرقمية.[16]

على ضوء ما سبق، تعد الهندسة الاجتماعية واحدة من أحدث التقنيات التي يستخدمها المهاجمون السيبرانيون للحصول على معلومات حساسة والحصول على وصول غير مصرح به إلى أنظمة الكمبيوتر. إنها أيضًا أداة قوية للمهاجمين السيبرانيين لأنها إجراء غير مرغوب فيه ويمكن أن تستفيد من ثقة الناس المفرطة، وتستغل جهلهم وتقوض أمن المعلومات، ويمكن أن تتخذ الهندسة الاجتماعية أشكالًا عديدة، بما في ذلك التلاعب بوسائل التواصل الاجتماعي، ويعد البريد الإلكتروني المزيف أحد أكثر أشكال الهندسة الاجتماعية شيوعًا، حيث يتم إرسال بريد إلكتروني يتظاهر بأنه شخص تثق به ويطلب من المستلم تقديم معلومات شخصية أو تسجيل الدخول إلى حسابه، وإذا قدم الضحايا هذه المعلومات، فيمكن للمهاجمين استخدامها لأغراض غير قانونية، ويمكن استخدام وسائل التواصل الاجتماعي للتفاعل مع

[16] https://www.enabbaladi.net/archives/610666 موجود على الموقع

الأشخاص، أو تلقي معلومات حساسة، أو تنفيذ إجراءات غير مرغوب فيها، كما تُستخدم أيضًا لتنفيذ الهندسة الاجتماعية من خلال الحسابات التي تمتلكها.

المطلب الثاني: مراحل الهندسة الاجتماعية وطرق الوقاية

في هذا المطلب سوف نتحدث عن المراحل والخطوات المتبعة لتنفيذ الهندسة الاجتماعية ثم نتكلم بعدها عن اهم الإجراءات المتخذة للوقاية من اخطار الهندسة الاجتماعية

الفرع الأول: مراحل الهندسة الاجتماعية

ان تجسيد ما يسمى بالهندسة الاجتماعية يحتاج الى خطوات ينتهجها المهاجمين يمكن اجمالها فيما يلي:

المرحلة الأولى: تحديد الهدف

تعتبر المرحلة الأولى من الهندسة الاجتماعية، وفيها يقوم المهاجم بتحديد الهدف الذي يرغب في مهاجمته والمعلومات التي يود الحصول عليها.

المرحلة الثانية: جمع المعلومات

بمجرد أن يحدد المهاجم هدفًا، يبدأ في جمع المعلومات المختلفة المتعلقة بذلك الهدف، ويستثمر المهاجمون قدرًا كبيرًا من الوقت والموارد المختلفة لجمع معلومات متنوعة حول أهدافهم، كلما كانت المعلومات أفضل، كان الهجوم أسهل، وكذلك فعل المهاجمون، وتتم هذه الخطوة أحيانًا عن طريق التصيد الاحتيالي لمحاولة الحصول على أرضية مشتركة مع الهدف أو للحصول على جزء صغير من المعلومات لتبرير الاتصال بالهدف، و أن نجاح الهجمات المختلفة يستند على نجاح هذه المرحلة، من خلال ربط المهاجم مع الهدف ، ويبدأ المهاجم في تحديد طريقة الهجوم المناسبة لاستخدامها ضد الهدف.

المرحلة الثالثة: مرحلة التحضير

في هذه المرحلة، يقوم المهاجم بعملية تحليل المعلومات التي وصل اليها التي تخص الهدف، ثم رسم خطة وربطها بالهدف.

المرحلة الرابعة: مرحلة توطيد العلاقة

في هذه المرحلة، يبدأ المهاجمون في استخدام البريد الإلكتروني أو المكالمات الهاتفية ووسائل التواصل الاجتماعي أو الرسائل النصية لإنشاء علاقات مع أهدافهم وتحسينها وتقويتها، وكلما كانت

العلاقة بين المهاجم والهدف أقوى، زادت سرعة وصول المهاجم إلى هدفه، وسيستخدم المهاجم أي وسيلة ضرورية لتأسيس العلاقة مع الهدف وتعزيزها.

المرحلة الخامسة: مرحلة استغلال العلاقة

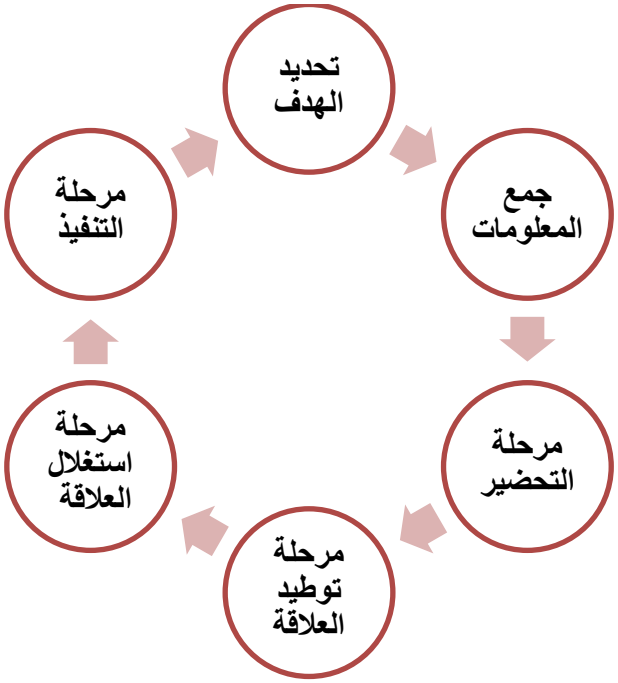
وهي مرحلة بدء الهجوم، حيث يستغل المهاجم العلاقة بينه والهدف لتأسيس ثقة الهدف، ثم يستغل هذه الثقة لتحديد الأساليب التي يستخدمها، مسلحًا بالمعلومات التي يبحثون عنها، يرسل المهاجم إلى الهدف رابطًا يحتوي على برنامج الهجوم، ويخدع الهدف ليطلب بريدًا إلكترونيًا أو كلمة مرور، ويحاول استغلال المعلومات الشخصية أو كليهما، وإنشاء علاقات راسخة مع الأهداف لتحقيق أهداف القرصنة بفعالية دون إثارة الشكوك حتى يتمكن المهاجمون في النهاية من الحصول على المعلومات الأمنية التي يبحثون عنها منهم.

المرحلة الاخيرة: مرحلة التنفيذ

تحدث بعد انتهاء الهجوم ويكون لدى المهاجم المعلومات اللازمة، وفي هذه المرحلة، يحتفظ المهاجم بعلاقة مع الهدف لتجنب الإبلاغ عنه، وقد يحصل المهاجم أو لا يحصل على المعلومات التي يريدها، ولكن على أي حال، فإن مرحلة التنفيذ هي المرحلة الأخيرة، ويستمر المهاجم بطريقة تتجنب الشك، والغاية هي أن يواصل المهاجم العلاقة مع الهدف او أن يستغلها مرة أخرى بهجوم آخر، أو الصمود لفترة حتى يستشعر الهدف شيئًا ما، وبعد ذلك يبدأ المهاجم في الانسحاب ببطء.[17]

الشكل الموالي يوضح مراحل الهندسة الاجتماعية

[17] زينا الشبول، مراحل الهندسة الاجتماعية، تمت زيارة الموقع 12/07/2023 ، على الرابط
: https://mawdoo3.com/%D9%85%D8%B1%D8%A7%D8%AD%D9%84_%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9_%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9



من تصميم الباحث

الفرع الثاني: طرق الحماية من الهندسة الاجتماعية

من بين الإجراءات الوقائية من اخطار الهندسة الاجتماعية للأفراد والمؤسسات نجد:

- **تطوير قوانين الأمان التنظيمي:**

تقوم المنظمة بإبلاغ الموظفين بقوانين الأمان المعمول بها والتي يجب عليهم اتباعها.

- **إنشاء أمن المبنى التنظيمي:**

لا يُسمح للأشخاص الذين لا يعملون داخل المنظمة بالدخول ويتم تحديد الزيارات ضمن نطاق العمل بمعرفة مسبقة بالأوراق المالية، داخل المنظمة وتحت إشرافها.

- **التعليم والتدريب:**

تثقيف الموظفين داخل مؤسستك حول أمن المعلومات والانتهاكات المحتملة. يجب تدريب وتعليم موظفي مكتب المساعدة إلى مستوى كافٍ من حيث الأمن، وتوضيح وتوجيه أساليب المهاجمين، وتدريبهم

على عدم تسريب معلومات سرية للغاية ضمن النطاق المسموح به بخلاف التحقق من الهوية. إنهم يفكرون في كيفية حجب المعلومات عندما لا يكون من الممكن حجبها بطريقة حيلة.

- **استراتيجيات العمل في حالات الأزمات:**

هناك استراتيجيات محددة طورتها المنظمة لتمكين الموظفين من التصرف عند طلب معلومات حساسة تحت الضغط.

- **فحص المكالمات الهاتفية:**

ما لم يكن مطلوبًا ويسمح به مدير المكالمات، اتصل بأنظمة الأمان مع القدرة على التحكم فيمن يمكنه إجراء المكالمات، ومنع المكالمات الخاصة، ومراقبة المكالمات الدولية والمكالمات بعيدة المدى ولن يظهر تسجيل الدخول الخاص على خطوط الهاتف الخاصة بالمؤسسة حتى لا يتمكن الأشخاص من خارج المؤسسة من استخدام الهاتف الخاص

- **التخلص من المستندات والأجهزة غير المستخدمة:**

ترتيب أجهزة التخلص من الورق داخل المؤسسة لجعل المعلومات الواردة في الورقة والمعلومات السرية وكلمات المرور التي تدخل النظام وما إلى ذلك غير قابلة للاستخدام على أجهزة الكمبيوتر القديمة واستخراج المعلومات الحساسة لجعلها غير قابلة للاستخدام. معلومات منهم.[18]

من المهم للأفراد والمؤسسات أن يكونوا على دراية بهذه التهديدات السيبرانية وتقنيات الهندسة الاجتماعية المستخدمة يجب على الأفراد توخي الحذر والتحقق من صحة المصادر قبل تقديم معلومات شخصية أو تقديم طلبات غير معروفة، ونحن بحاجة إلى الاعتراف بأن الهندسة الاجتماعية تشكل تهديدًا خطيرًا في عالم التكنولوجيا الحديثة، ويجب أن نحرص بشدة على الحفاظ على أمن المعلومات الشخصية

الخاتمة:

[18] file:///C:/Users/FC/Desktop/Noor -تجدون الموضوععلى الموقع
Book.com%20%20%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9%20%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9.pdf

مع التطور الكبير للمجتمع الحديث، ومجتمع المعلومات، والابتكار التكنولوجي الواسع النطاق، تم تشكيل "فضاء إلكتروني" جديد للمعلومات يستخدمه الأفراد والدول، كما أن تطوير الاتصالات يتقدم، وساهم في تزايد خطر الهجمات الإلكترونية في العصر الحديث حيث يتم استخدام التكنولوجيا أكثر فأكثر، وعلى نطاق كبير في جميع مجالات الحياة اليومية، و تشمل الهجمات الإلكترونية الشائعة القرصنة والبرامج الضارة والتصيد الاحتيالي وهجمات الهندسة الاجتماعية والتي تعد اخطر الهجمات السيبرانية ،ولتحقيق حماية الأنظمة والشبكات الإلكترونية الخاصة عن طريق تحديث البرامج والأجهزة بانتظام، واستخدام كلمات مرور قوية، وتشفير البيانات الحساسة، وتنفيذ جدران الحماية، واستخدام برامج مكافحة الفيروسات والبرامج الضارة، وتثقيف المستخدمين حول تدابير الأمن السيبراني المناسبة، بما في ذلك نشر الوعي.

ولأن الفضاء الإلكتروني متاح للجميع دون استثناء، يجب تعديل التشريعات المتعلقة بجرائم الإنترنت وانتهاك حقوق الغير وفقًا للتشريع والتدابير المتخذة، ودرجة الضرر الناجم عن هذه الإجراءات وتأثيرها على الضحايا، ويجب السعي على الصعيدين الإقليمي والدولي لتطوير الأطر القانونية والاتفاقيات الدولية لإدارة الفضاء السيبراني وجعله أكثر أمانًا، وتشجيع المبادرات والحملات التي تركز على استخدام التكنولوجيا بجميع أنواعها لمنع أي فرد أو منظمة من الوقوع في فخ الهجمات السيبرانية بكل أنواعها، والتركيز على عمليات التنشئة الاجتماعية المتعلقة بالتعليم والنهوض بالجيل الرقمي وتوجيه استخدام التكنولوجيا والأدوات الرقمية ، وعقد ورش عمل في المدارس والجامعات ودور الشباب لتقديم نصائح حول التقنيات المختلفة التي يستخدمها المهندسون الاجتماعيون، للتعرف على عمل للمهندسين الاجتماعيين وكيفية الوقاية من اخطار الهندسة الاجتماعية.

قائمة المصادر والمراجع:

الكتب

1) تيري ديبيل، استراتيجية الشؤون الخارجية...منطق الحكم الأمريكي، ترجمة: وليد شحادة ، دار الكتاب – العربية ومؤسسة محمد بن آل راشد آل مكتوم، بيروت، 2009

2) عادل عبد الصادق ، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني ، مكتبة الإسكندرية وحدة الدراسات المستقبلية ، الاسكندرية، 2016,

الرسائل العلمية

انديرا عراجي، القوة في الفضاء السيبراني: فصل عصري من التحدي والاستجابة، رسالة لنيل شهادة دراسات عليا في العلوم السياسية والإدارية، كلية الحقوق والعلوم السياسيه، لبنان،2016

المقالات

1) أحمد عبد الحليم، أمن الخليج: إلى أين؟، اوراق الشرق الأوسط، 1992,.

2) ادريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، جامعة العربي تبسي، تبسة، المجلد 01، العدد 01،2019 .

3) لامية طالة, التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها،مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد04, العدد 02، 2020

4) محمد مختار،الأمن السيبراني مفاهيم المستقبل، مجلة اتجاهات الأحداث ،العدد 02، 6،2015.

المواقع الإلكترونية

- معجم اكسفورد على الرابط : http:// en.oxforddictionaires.com/ definition/cyber

- فارس محمد العمارات، الهندسة الاجتماعية واختراق عقول البشر تم الاطلاع على الموقع في 2023/04/12 على الرابط https://www.new-educ.com/%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9-%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D8%B9%D9%82%D9%88%D9%84-%D8%A7%D9%84%D8%A8%D8%B4%D8%B1

- ما هى الهندسة الاجتماعية ؟طرقها وكيف تتجنبها متوفر على الرابط، تمت زيارته في 10 06 2023

https://www.it-pillars.com/ar/blog/%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9/

- https://mafhome.com/%D9%85%D8%A7-%D9%87%D9%8A

D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%
%D8%A7%D9%84%D8%A5%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8
%A9

- https://www.enabbaladi.net/archives/610666
- زينا الشبول، مراحل الهندسة الاجتماعية ، تمت زيارة الموقع 2023/07/12 ، على الرابط

https://mawdoo3.com/%D9%85%D8%B1%D8%A7%D8%AD%D9%84_%D8%A7%D9%84%
D9%87%D9%86%D8%AF%D8%B3%D8%A9_%D8%A7%D9%84%D8%A7%D8%AC%D8
%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9

- file:///C:/Users/FC/Desktop/Noo - Book.com%20%20%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9%20%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9.pdf