مجلة الأسرة والمجتمع
مجلة دولية محكمة نصف سنوية
تصدر بثلاث لغات
FAMILY AND SOCIETY JOURNAL
International Biannual Journal
refereed Issued in three languages
الترقيم الدولي: ISSN:2392-5337 الترقيم الإلكتروني: EISSN: 2602-6716
https://www.asjp.cerist.dz/en/PresentationRevue/236

المجلد: 09/ العدد: 02/ 2021	تاريخ إرسال المقال: 2021/05/18	تاريخ القبول: 2021/10/08	تاريخ النشر: 2021/12/31	الصفحة: 172 – 189

الاختراق عن طريق الهندسة الاجتماعية وأساليب الحماية منها

Hacking through social engineering and methods of protection from it

سعيـــد زيـــوش	المركز الجامعي بريكة، (الجزائـــر)	saidziouche@cu-barika.dz

ملخص:

الاختراق عن طريق الهندسة الاجتماعية هو استراتيجية يستخدمها المهاجمون السيبرانيون، ويعتمد بشكل كبير على التفاعل البشري، وغالبًا ما يتضمن خداع الأشخاص لخرق ممارسات الأمان القياسية، يعتمد نجاح تقنيات الهندسة الاجتماعية على قدرة المهاجمين على التلاعب بالضحايا لتنفيذ إجراءات معينة أو تقديم معلومات سرية، في هذا المقال سنحاول إلقاء الضوء على الاختراق عن طريق الهندسة الاجتماعية باعتباره واحد من أكبر التهديدات الأمنية التي تواجه كل من يتصل بشبكة الانترنت، معتمدين في ذلك على أسلوب التحليل والاستقصاء، وصولا إلى نتيجة مفادها أن الحماية من الاختراق عن طريق الهندسة الاجتماعية تتم بالتوعية والتعليم، فإذا كان جميع المستخدمين على دراية بالتهديدات، فسوف تتحسن سلامتهم كمجتمع بصفة عامة.

الكلمات المفتاحية: الاختراق، الهندسة، الأساليب، الحماية، المجتمع.

عنوان المقال: الاختراق عن طريق الهندسة الاجتماعية وأساليب الحماية منها	المؤلف: سعيد زيوش	المجلد: 09/ العدد: 02 /2021	الصفحة: 172 – 189

Abstract:

Social engineering hacking is a strategy used by cyber attackers, that relies heavily on human interaction, and often involves tricking people into breaching standard security practices. The success of social engineering techniques depends on the attackers' ability to manipulate victims to perform certain actions or provide confidential information. We will try to shed light on penetration through social engineering as one of the biggest security threats facing everyone who connects to the Internet, relying on the method of analysis and investigation, leading to the conclusion that protection from penetration through social engineering is done through awareness and education. Users are aware of the threats, their safety as a society in general will improve

Keywords: Penetration, Engineering, Methods, Protection, Society.

مقدمة:

لقد أصبحت الأنترنت فعلاً متوفرة لدى غالبية أفراد المجتمع الجزائري، حيث "نشير هنا إلى آخر تقرير للموقع الإلكتروني "داتاريبورتال" (**DATAREPORTAL**) المختص في الإحصائيات المتعلقة بأنترنت الهاتف الثابت والنقال في العالم إلى أن عدد مستخدمي الأنترنت في الجزائر ارتفع بـ 3.6 مليون في ظرف سنة منتقلا بذلك إلى 26.35 مليون مستخدما يمثل زيادة تقدر بـ 3.6 مليون مستخدم (16 %) منذ جانفي 2020". (**Kemp, Simon(2021), P70**)

وتضمن التقرير ذاته إحصائيات متعلقة بوسائل التواصل الاجتماعي والتجارة الإلكترونية؛ إضافة إلى توجهات ومعلومات تخص وضع الرقمنة في العالم، وحسب آخر تقرير لسلطة ضبط البريد والاتصالات الإلكترونية فإن هذا الرقم يمثل العدد الحقيقي لمستخدمي الأنترنت في الجزائر، وليس مشتركيها والذي كان يبلغ 41.8 مليون خلال الثلاثي الثالث من سنة 2020، ويوضح موقع "داتاريبورتال" أن نسبة ولوج الأنترنت في الجزائر بلغت 59.6 % خلال جانفي 2021 من مجموع سكان يبلغ عددهم 44.23 مليون، حسب الأمم المتحدة.

كما عرف عدد مستخدمي مواقع التواصل الاجتماعي (فايسبوك، تويتر، يوتيوب، انستغرام ...) ارتفاعا في الجزائر إلى غاية 31 جانفي 2021، وأكد ذات الموقع أنه "تم تسجيل حوالي ثلاثة ملايين مستخدم جديد لمواقع التواصل الاجتماعي أي بزيادة 13.6 % خلال سنة واحدة، وهو ما جعل العدد الإجمالي لمستخدمي هذه

التطبيقات يقفز إلى 25 مليون أي بنسبة 56.5 %من عدد السكان الإجمالي، وتستعمل أغلبية مستخدمي مواقع التواصل الاجتماعي (24.8 مليون أي 97.9 %) الهاتف الذكي واللوحات الإلكترونية للاتصال بهذه الشبكات"(**Kemp, Simon(2021), P80**)، كل هذه الإحصائيات تؤكد على أن مفتاح الحفاظ على سرية وسلامة وتوافر معلومات وأنظمة المعلومات الخاصة بالأفراد أو المؤسسات؛ هو التحكم في من يصل إلى أي معلومات أو بيانات مهمة، حيث "يتم تحقيق ذلك من خلال القدرة على تحديد هوية مقدم الطلب، والتحقق من أن مقدم الطلب ليس محتالاً، والتأكد من أن لديه المستوى المناسب من التصريح للوصول إلى مورد معلوماتي معين، لكن لطالما كان هناك من يحاول تجاوز هذه الآلية الأمنية من خلال قوة غير شرعية (المخترق) أو باستخدام المكر والحيلة".(**Thornburgh, Tom(2004), P30**)

في الماضي كان يُطلق على أولئك الذين يستخدمون المكر من رجال الثقة بالمحتالين، اليوم يُطلق على هؤلاء الأشخاص اسم المهندسين الاجتماعيين، لكن التقنيات المستعملة تظل كما هي حتى لو تغيرت الأهداف.

في هذه الورقة البحثية سنحاول تسليط الضوء على هذا المفهوم الجديد نسبيا، حيث تختلف الهندسة الاجتماعية عن القرصنة التقليدية، بمعنى أن هجمات الهندسة الاجتماعية يمكن أن تكون غير تقنية، ولا تنطوي بالضرورة على تسوية أو استغلال البرامج أو الأنظمة عند نجاحها، وتمكّن العديد من هجمات الهندسة الاجتماعية المهاجمين من الحصول على وصول شرعي ومصرح به إلى المعلومات السرية، الأمر الذي يقودنا إلى طرح التساؤل الآتي:

هل نحن في مأمن من الاختراق عن طريق الهندسة الاجتماعية؟

وللإجابة على هذا السؤال وجب علينا في ورقتنا البحثية التعريف بالهندسة الاجتماعية، وتوضيح ماهيتها، وكيف يمكن للفرد العادي أن يتأكد من أنه لم يتعرض إلى هذا النوع من الاختراق، معتمدين في ذلك على اسلوب التحليل والاستقصاء من أجل الوصول إلى تحديد أهم الأساليب التي تمكننا من حماية أنفسنا منه.

أولاً: تعريف الهندسة الاجتماعية:

الهندسة الاجتماعية هي تقنية تلاعب تستغل الخطأ البشري للحصول على معلومات خاصة أو الوصول أو الأشياء الثمينة في الجرائم الإلكترونية، "تميل حيل "القرصنة البشرية" هذه إلى إغراء المستخدمين المطمئنين بكشف البيانات أو نشر إصابات بالبرامج الضارة أو منح الوصول إلى الأنظمة المحظورة، يمكن أن تحدث الهجمات عبر الإنترنت أو شخصيًا أو عبر تفاعلات أخرى" (**Administration, Kaspersky(2008)**).

تتمحور عمليات الاحتيال القائمة على الهندسة الاجتماعية حول كيفية تفكير الناس وتصرفهم على هذا النحو، حيث "تعد هجمات الهندسة الاجتماعية مفيدة بشكل خاص للتلاعب بسلوك المستخدم وهذا بمجرد أن يفهم المهاجم ما الذي يحفز تصرفات المستخدم، كما يمكنه من خداع المستخدم والتلاعب به بشكل فعال"(**Administration, Kaspersky(2008)**)، بالإضافة إلى ذلك يحاول المتسللون استغلال افتقار المستخدم إلى المعرفة بفضل سرعة التكنولوجيا، حيث "لا يدرك العديد من المستهلكين والموظفين بعض التهديدات مثل تنزيل البرامج مجهولة المصدر والفرد بالسيارة، وقد لا يدرك المستخدمون أيضًا القيمة الكاملة للبيانات الشخصية مثل رقم هواتفهم .ونتيجة لذلك فإن العديد من المستخدمين غير متأكدين من أفضل طريقة لحماية أنفسهم ومعلوماتهم"(**محمد النور أحمد، معتصم (2019)، ص 5**).

بشكل عام يمتلك مهاجمو الهندسة الاجتماعية هدفًا من هدفين:

- **التخريب**: تعطيل البيانات أو إتلافها لإحداث ضرر أو إزعاج.
- **السرقة**: الحصول على الأشياء الثمينة مثل المعلومات أو الوصول أو المال.

يمكن توسيع تعريف الهندسة الاجتماعية هذا من خلال معرفة كيفية عملها بالضبط.

1-كيف تعمل الهندسة الاجتماعية؟

تعتمد معظم هجمات الهندسة الاجتماعية على التواصل الفعلي بين المهاجمين والضحايا، حيث يميل المهاجم إلى تحفيز المستخدم على تعريض نفسه للخطر بدلاً من استخدام أساليب الاحتيال والمراوغة لخرق بياناته، تمنح دورة الهجوم هؤلاء المجرمين عملية موثوقة لخداعه، عادة ما تكون خطوات دورة هجوم الهندسة الاجتماعية على النحو التالي:

- **استعد من** خلال جمع معلومات أساسية عنك أو عن مجموعة أكبر أنت جزء منها؛
- **تسلل من** خلال إقامة علاقة أو بدء تفاعل يبدأ ببناء الثقة؛
- **استغل الضحية** بمجرد أن تنشأ الثقة والضعف لتعزيز الهجوم؛
- **فك الارتباط** بمجرد أن يتخذ المستخدم الإجراء المطلوب. (**علي عباس، مراد (2017)، ص 18**)

يمكن "أن تتم هذه العملية في رسالة بريد إلكتروني واحدة أو على مدار أشهر في سلسلة من محادثات الوسائط الاجتماعية، حيث يمكن أن يكون تفاعلًا وجهاً لوجه لكنها تنتهي في النهاية بإجراء تتخذه، مثل مشاركة معلوماتك أو تعريض نفسك لبرامج ضارة". (**شعبان تهامي، عبد الرحمن (2020)، ص 29)**

من المهم الحذر من الهندسة الاجتماعية كوسيلة للارتباك، قد لا يدرك العديد من الموظفين والمستهلكين أن مجرد أجزاء قليلة من المعلومات، يمكن أن تمنح المتسللين إمكانية الوصول إلى شبكات وحسابات متعددة من خلال التنكر كمستخدمين شرعيين لموظفي دعم تكنولوجيا المعلومات مثلا، وبالتالي يحصلون على تفاصيلك الخاصة – مثل الاسم أو تاريخ الميلاد أو العنوان، وهنا من السهل إعادة تعيين كلمات المرور والحصول على وصول غير محدود تقريبًا؛ مما يمكنهم من سرقة الأموال ونشر البرامج الضارة الخاصة بالهندسة الاجتماعية.

2– سمات هجمات الهندسة الاجتماعية:

تتمحور هجمات الهندسة الاجتماعية حول استخدام المهاجم للإقناع والثقة عندما تتعرض لهذه التقنيات فمن المرجح أن تتخذ إجراءات لن تفعلها بخلاف ذلك، من بين معظم الهجمات ستجد نفسك مضللاً في السلوكيات التالية:

2–1– زيادة المشاعر: يمنح التلاعب العاطفي المهاجمين اليد العليا في أي تفاعل، أنت أكثر عرضة لاتخاذ إجراءات غير عقلانية أو محفوفة بالمخاطر عندما تكون في حالة عاطفية محسّنة، يتم استخدام جميع المشاعر التالية بشكل متساوٍ لإقناعك: يخاف، الإثارة، فضول، الغضب، الذنب، حزن.

2–2– الاستعجال: ونقصد بها "اقتناص الفرص أو الطلبات الحساسة للوقت هي أداة أخرى يمكن الاعتماد عليها في ترسانة المهاجم، حيث قد يكون لديك الدافع للتنازل عن خصوصياتك تحت ستار مشكلة خطيرة تحتاج إلى اهتمام فوري، بدلاً من ذلك قد تتعرض لجائزة أو مكافأة قد تختفي إذا لم تتصرف بسرعة، كلا النهجين يتجاوز قدرتك على التفكير النقدي".(**شعبان تهامي، عبد الرحمن (2020)**، ص43)

2–3–الثقة: "المصداقية لا تقدر بثمن وضرورية لهجوم الهندسة الاجتماعية، ونظرًا لأن المهاجم يكذب عليك في النهاية، فإن الثقة تلعب دورًا مهمًا هنا، لقد أجروا بحثًا كافيًا عنك لصياغة قصة يسهل تصديقها ومن غير المرجح أن تثير الشكوك".(**علي عباس، مراد (2017)، ص 18)**

هناك بعض الاستثناءات لهذه السمات، حيث في بعض الحالات يستخدم المهاجمون أساليب أكثر بساطة في الهندسة الاجتماعية للوصول إلى الشبكة أو الكمبيوتر، على سبيل المثال قد يتردد أحد المخترقين على قاعة الطعام العامة في مبنى إداري كبير ومستخدمي "الولوج الجماعي للأنترنت (ونشير هنا إلى وجود واي فاي مجاني) الذين يعملون على أجهزة الكمبيوتر اللوحية أو أجهزة الكمبيوتر المحمولة الخاصة بهم، يمكن أن يؤدي القيام بذلك إلى تراكم عدد كبير من كلمات المرور وأسماء المستخدمين، كل ذلك دون إرسال بريد إلكتروني أو كتابة سطر من رمز الفيروس.

الآن بعد أن تناولنا المفهوم الأساسي ربما قد نتساءل "ما هو هجوم الهندسة الاجتماعية وكيف يمكنني اكتشافه؟

3– أنواع هجمات الهندسة الاجتماعية:

يحتوي كل نوع من أنواع هجمات الأمن السيبراني تقريبًا على نوع من الهندسة الاجتماعية، على سبيل المثال الرسائل المخادعة عبر البريد الإلكتروني والفيروسات التقليدية مليئة بالإيحاءات الاجتماعية.

"يمكن أن تؤثر الهندسة الاجتماعية على الفرد رقميًا من خلال هجمات الأجهزة المحمولة، بالإضافة إلى أجهزة الكمبيوتر العادية، يمكن الفرد بسهولة أن يواجه تهديدًا شخصيًا، حيث يمكن أن تتداخل هذه الهجمات وتتراكم فوق بعضها البعض لإنشاء عملية احتيال".(**زيوش، سعيد(2017)، ص 74**).

وفيما يلي بعض الأساليب الشائعة التي يستخدمها مهاجمو الهندسة الاجتماعية:

3–1– هجمات التصيد الاحتيالي:

يتظاهر مهاجمو **التصيد الاحتيالي** بأنهم مؤسسة أو فرد موثوق به؛ في محاولة لإقناعك بالكشف عن البيانات الشخصية والأشياء الثمينة الأخرى.

يتم استهداف الهجمات باستخدام التصيد بإحدى طريقتين:

– **التصيد غير المرغوب فيه، أو التصيد الجماعي** وهو هجوم واسع النطاق يستهدف العديد من المستخدمين، هذه الهجمات غير شخصية وتحاول القبض على أي شخص يعتقد أنه في مأمن.

– **التصيد بالرمح وبالتبعية، صيد الحيتان** وهو استخدم المعلومات الشخصية لاستهداف مستخدمين معينين، حيث تستهدف هجمات صيد الحيتان تحديدًا أهدافًا عالية القيمة مثل المشاهير ومسؤولي الإدارات الكبرى وكبار المسؤولين الحكوميين، سواء كان ذلك اتصالًا مباشرًا أو عبر نموذج موقع ويب مزيف، فإن أي شيء تشاركه ينتقل

مباشرة إلى جيب المحتال، قد يتم خداع الفرد في تنزيل برامج ضارة تحتوي على المرحلة التالية من هجوم التصيد الاحتيالي، لكل من الأساليب المستخدمة في التصيد الاحتيالي أوضاعًا فريدة للتسليم، بما في ذلك على سبيل المثال لا الحصر:

- قد تكون المكالمات الهاتفية **للتصيد الصوتي (التصيد الصوتي)** عبارة عن أنظمة رسائل آلية تسجل جميع **مدخلات** الفرد، في بعض الأحيان قد يتحدث معه شخص ما وهذا لزيادة الثقة والإلحاح.
- **قد تتضمن رسائل التصيد الاحتيالي عبر الرسائل النصية القصيرة (SMS)** أو رسائل تطبيقات الجوال، رابط ويب أو مطالبة بالمتابعة عبر بريد إلكتروني أو رقم هاتف احتيالي.

"يعد **التصيد الاحتيالي عبر البريد الإلكتروني** أكثر الوسائل التقليدية للتصيد الاحتيالي، وذلك باستخدام بريد إلكتروني يحثك على الرد أو المتابعة بوسائل أخرى .يمكن استخدام روابط الويب أو أرقام الهواتف أو مرفقات البرامج الضارة".**(زيوش، سعيد (2017)، ص 78)**

- يحدث **تصيد Angler** على وسائل التواصل الاجتماعي المختلفة، حيث يقلد المهاجم فريق خدمة عملاء شركة موثوق بهيعترضون اتصالات الفرد مع علامة تجارية لاختطافها وتحويل محادثتك إلى رسائل خاصة، حيث يقومون بعد ذلك بتقدم الهجوم.
- محاولة **تصيد محرك البحث** لوضع روابط لمواقع ويب مزيفة أعلى نتائج البحث، قد تكون هذه إعلانات مدفوعة أو تستخدم طرق تحسين مشروعة للتلاعب بترتيب البحث.
- قد تغري الفرد روابط **التصيد الاحتيالي لعناوين URL** لزيارة مواقع التصيد الاحتيالي،حيث يتم تسليم هذه الروابط عادةً في رسائل البريد الإلكتروني والنصوص ورسائل الوسائط الاجتماعية والإعلانات عبر الإنترنت، كما قد تخفي الهجمات الروابط في نص أو أزرار مرتبطة تشعبيًا، أو باستخدام أدوات تقصير الارتباط، أو عناوين URL مكتوبة بطريقة مضللة.
- يظهر **التصيد أثناء الجلسة على** أنه مقاطعة لتصفح الويب العادي، على سبيل المثال قد يرى مثل النوافذ المنبثقة الزائفة لتسجيل الدخول للصفحات التي يزورها حاليًا. **(سلمان الجبوري، سامر (2018)، ص 55)**

3-2- هجمات الاصطياد:

يشير **الطُعم** إلى فضول الفرد الطبيعي لإقناعه بتعريض نفسه لمهاجم ما، عادةً ما تكون إمكانية الحصول على شيء مجاني أو حصري هي التلاعب بالمستخدم لاستغلاله، كما يتضمن الهجوم عادةً إصابته ببرامج ضارة.

يمكن أن تشمل طرق الاصطياد الشائعة ما يلي:

- تُركت محركات أقراص(**USB (flash disk** في الأماكن العامة، مثل المكتبات والأماكن العامة.
- مرفقات البريد الإلكتروني بما في ذلك تفاصيل حول عرض مجاني أو برنامج مجاني احتيالي.

3-3- هجمات الخرق الجسدي:

تتضمن **الانتهاكات الجسدية** ظهور المهاجمين شخصيًا والتظاهر كشخص شرعي للوصول إلى مناطق أو معلومات غير مصرح بها، حيث تعتبر الهجمات من هذا النوع أكثر شيوعًا في بيئات المؤسسات، مثل الحكومات أو الشركات أو المنظمات الأخرى.

قد "يتظاهر المهاجمون بأنهم ممثلون لشركة معروفة وبأنهم ذو ثقة حتى أن بعض المهاجمين قد يُطردون مؤخرًا موظفين بالثأر من صاحب العمل السابق، إنهم يجعلون هويتهم غامضة ولكنها قابلة للتصديق بما يكفي لتجنب الأسئلة، تطلب هذا القليل من البحث من جانب المهاجم وينطوي على مخاطر عالية، لذلك إذا حاول شخص ما هذه الطريقة فقد حدد إمكانية واضحة للحصول على مكافأة قيّمة للغاية – إذا نجحت طبعا –" (**محمد عبد الرؤوف المنيفي، أحمد (2021)، ص 43**)

3-4- هجمات نصوص مسبقة:

يستخدم **المحتوى المسبق** هوية مخادعة "كذريعة" لتأسيس الثقة، مثل انتحال شخصية بائع أو موظف منشأة مباشرةً، يتطلب هذا الأسلوب من المهاجم أن يتفاعل مع الفرد بشكل أكثر استباقية، إذ يتبع طريقة الاستغلال المباشر بمجرد إقناعهم بأنهم شرعيون.

3-5- الوصول إلى هجمات Tailgating:

و"يطلق عليه التحميل على الظهر، هو فعل تأخير موظف مرخص إلى منطقة (في الجهاز) محظورة الوصول، قد يلعب المهاجمون على سبيل المجاملة الاجتماعية لحمل الفرد على إمساك الباب من أجلهم أو إقناعه بأنه مسموح لهم أيضًا بالتواجد في المنطقة، مما يمكن المخترق من الاطلاع على مختلف أنواع الملفات أو الأنظمة التي تعمل ضمن نطاق أهدافه" (**Administration, Kaspersky (2008)**).

3-6- هجمات Quid Pro Quo :

هو مصطلح يعني تقريبًا "خدمة مقابل خدمة"، والتي تعني في سياق التصيد الاحتيالي تبادل معلومات الفرد الشخصية مقابل مكافأة أو تعويض آخر، الهبات أو العروض للمشاركة في الدراسات البحثية قد تعرض الفرد لهذا النوع من الهجوم.

"يأتي الاستغلال من إثارة حماس الفرد لشيء ذي قيمة يأتي باستثمار منخفض من جانبه، ومع ذلك فإن المهاجم ببساطة يأخذ بياناته دون أي مكافأة له"(**Kuston, Clarc (2018)**).

3-7- هجمات انتحال DNS وتسمم ذاكرة التخزين المؤقت:

يتلاعب **انتحال DNS** بالمتصفح وخوادم الويب لدى الفرد للانتقال إلى مواقع الويب الضارة عند إدخال عنوان **URL** شرعي، بمجرد الإصابة بهذا الاستغلال ستستمر إعادة التوجيه ما لم يتم مسح بيانات التوجيه غير الدقيقة من الأنظمة المعنية.

تصيب **هجمات التسمم بذاكرة التخزين المؤقت لنظام أسماء النطاقات** جهاز الضحية، بإرشادات توجيه لعنوان **URL** الشرعي أو عناوين **URL** متعددة للاتصال بمواقع الويب الاحتيالية.

3-8- هجمات Scare ware :

هو أحد أشكال البرامج الضارة المستخدمة لإخافةالفرد لاتخاذ إجراء ما، حيث تستخدم هذه البرامج الضارة المخادعة تحذيرات تنذر بالخطر والتي تبلغ عن إصابات مزيفة بالبرامج الضارة أو تدعي اختراق أحد حسابات الفرد، ونتيجة لذلك تدفعه البرامج الضارة إلى شراء برنامج أمان إلكتروني احتيالي، أو الكشف عن تفاصيل خاصة مثل بيانات اعتماد حسابه.

3-9- هجمات ثقب الري:

تصيب **هجمات الثقب** المائي صفحات الويب الشهيرة ببرامج ضارة للتأثير على العديد من المستخدمين في وقت واحد، حيث يتطلب الأمر تخطيطًا دقيقًا من جانب المهاجم للعثور على نقاط الضعف في مواقع محددة، كما أنهم يبحثون عن الثغرات الموجودة غير المعروفة والمصححة – مثل هذه الثغرات تعتبر ثغرات يوم الصفر.

"في أوقات أخرى قد يجدون أن أحد المواقع لم يقم بتحديث بنيته التحتية لتصحيح المشكلات المعروفة، قد يختار مالكو مواقع الويب تأخير تحديثات البرامج للحفاظ على إصدارات البرامج التي يعرفون أنها مستقرة وبالتالي سيتم تبديلهم بمجرد أن يتمتع الإصدار الأحدث بسجل حافل من استقرار النظام، يسيء المتسللون استخدام هذا السلوك لاستهداف نقاط الضعف التي تم تصحيحها مؤخرًا". ((**Jem, Dantis (2019)).**

ثانياً: طرق الهندسة الاجتماعية غير العادية:

في بعض الحالات استخدم مجرمو الإنترنت أساليب معقدة لإكمال هجماتهم الإلكترونية بما في ذلك:

- **التصيد الاحتيالي عبر الفاكس:** عندما يتلقى عملاء أو زبائن أحد البنوك بريدًا إلكترونيًا مزيفًا يزعم أنه من البنك – يطلب من العميل تأكيد رموز الوصول الخاصة به –، لم تكن طريقة التأكيد عبر طرق البريد الإلكتروني / الإنترنت المعتادة بدلاً من ذلك، طُلب من العميل طباعة النموذج في البريد الإلكتروني، ثم ملء بياناته وإرسال النموذج بالفاكس إلى رقم هاتف المجرم الإلكتروني.
- **التوزيع التقليدي للبرامج الضارة عبر البريد"** :في اليابان استخدم مجرمو الإنترنت خدمة التوصيل للمنازل لتوزيع الأقراص المضغوطة المصابة ببرامج تجسس طروادة، حيث تم تسليم الأقراص لعملاء بنك ياباني سبق أن تمت سرقة عناوين العملاء من قاعدة بيانات البنك". ((**Vander, C (2019**)).

1– أمثلة على هجمات الهندسة الاجتماعية:

تستحق هجمات البرامج الضارة تركيزًا خاصًا لأنها شائعة ولها تأثيرات طويلة الأمد، عندما يستخدم منشئو البرامج الضارة تقنيات الهندسة الاجتماعية، يمكنهم جذب مستخدم غير حذر (ونشير هنا إلى الأفراد المبتدئين في استخدام الكمبيوتر ولواحقه) إلى تشغيل ملف مصاب أو فتح رابط إلى موقع ويب مصاب، تستخدم العديد من الفيروسات المتنقلة وأنواع أخرى من البرامج الضارة، هذه الأساليب بدون مجموعة برامج أمان شاملة لأجهزة الجوّال وأجهزة سطح المكتب، فمن المحتمل أن الفرد يعرض نفسه للإصابة.

2– هجمات الدودة:

يهدف المجرم الإلكتروني إلى جذب انتباه المستخدم إلى الرابط أو الملف المصاب – ثم حث المستخدم على النقر عليه. تتضمن أمثلة هذا النوع من الهجوم ما يلي:

- **دودة Love Letter** التي أثقلت كاهل العديد من خوادم البريد الإلكتروني للشركات في عام 2000، تلقى الضحايا رسالة بريد إلكتروني تدعوهم لفتح رسالة الحب المرفقة، عندما فتحوا الملف المرفق نسخت الدودة نفسها إلى جميع جهات الاتصال في دفتر عناوين الضحية، لا تزال هذه الدودة تعتبر من أكثر الدودة تدميراً من حيث الأضرار المالية التي ألحقتها.
- **استخدمت دودة البريد الإلكتروني – My doom** التي ظهرت على الإنترنت في يناير 2004 – نصوصًا تحاكي الرسائل الفنية الصادرة عن خادم البريد.

- **لقد** نقلت **دودة Swen** نفسها كرسالة تم إرسالها من .**Micro soft** ادعت أن الملف المرفق كان عبارة عن تصحيح من شأنه إزالة نقاط الضعف في **Windows**، ليس من المستغرب أن يأخذ الكثير من الناس هذا الادعاء على محمل الجد وحاولوا تثبيت التصحيح الأمني المزيف – على الرغم من أنه كان في الواقع دودة.

3– قنوات توصيل ارتباط البرامج الضارة:

يمكن إرسال الروابط إلى المواقع المصابة عبر البريد الإلكتروني و**ICQ وأنظمة** المراسلة الفورية الأخرى – أو حتى عبر غرف الدردشة عبر الإنترنت**IRC** - غالبًا ما يتم تسليم فيروسات الجوال عن طريق رسائل**SMS .**

"أيًا كانت طريقة التوصيل المستخدمة، ستحتوي الرسالة عادةً على كلمات لافتة للنظر أو مثيرة للفضول تشجع المستخدم المطمئن على النقر فوق الرابط كما يمكن أن تسمح طريقة اختراق النظام هذه للبرامج الضارة بتجاوز عوامل تصفية مكافحة الفيروسات في خادم البريد."(**حسن، شفيق (2017)، ص 102**).

4– هجمات شبكة نظير إلى نظير(P2P) :

تُستخدم شبكات P2P أيضًا لتوزيع البرامج الضارة، سيظهر فيروس متنقل أو فيروس حصان طروادة على شبكة P2P ولكن سيتم تسميته بطريقة من المحتمل أن تجذب الانتباه، وتحمل المستخدمين على تنزيل الملف وتشغيله. على سبيل المثال:

- **AIM & AOL Password Hacker.exe**
- **Microsoft CD Key Generator.exe**
- **PornStar3D.exe**
- بلاي ستيشن المحاكي**crack.exe**

5- عدم إبلاغ المستخدم عن الهجوم:

في بعض الحالات يتخذ منشئو وموزعو البرامج الضارة خطوات تقلل من احتمالية إبلاغ الضحايا عن الإصابة. قد يستجيب الضحايا لعرض وهمي لأداة مجانية أو دليل يعد بمزايا غير قانونية مثل:

- الوصول المجاني إلى الإنترنت أو اتصالات الهاتف المحمول؛
- فرصة تنزيل مولد رقم بطاقة الائتمان؛
- طريقة لزيادة رصيد حساب الضحية عبر الانترنت.

في هذه الحالات عندما يتضح أن التنزيل من فيروس حصان طروادة، ستحرص الضحية على تجنب الكشف عن نواياها غير القانونية، وبالتالي من المحتمل ألا تبلغ الضحية عن العدوى لأي من السلطات المعنية (مكافحة الجرائم الالكترونية الموجودة على مستوى كل من الشرطة والدرك الوطني) .

"كمثال على هذه التقنية تم إرسال فيروس حصان طروادة مرة واحدة إلى عناوين البريد الإلكتروني التي تم أخذها من موقع التوظيف، تلقى الأشخاص الذين سجلوا على الموقع عروض عمل مزيفة، لكن العروض تضمنت فيروس حصان طروادة . استهدف الهجوم بشكل أساسي عناوين البريد الإلكتروني للشركات، عرف مجرمو الإنترنت أن الموظفين الذين استقبلوا حصان طروادة لن يرغبوا في إخبار أصحاب العمل بأنهم أصيبوا أثناء بحثهم عن عمل بديل."(**درة، خضر (2013)، ص 120**)

ثالثا: كيفية اكتشاف هجمات الهندسة الاجتماعية:

يتطلب من الفرد الدفاع ضد الهندسة الاجتماعية بأن يمارس الوعي الذاتي، وعليه أن يتمهل دائمًا، وأن يفكر قبل القيام بأي شيء أو الاستجابة.

يتوقع المهاجمون منه اتخاذ إجراء قبل التفكير في المخاطر، مما يعني أنه يجب عليه فعل العكس، للمساعدة نوجه للفرد بعض الأسئلة التي يجب أن يطرحها على نفسه؛ إذا كان يتشك في حدوث هجوم:

- **هل اشتدت مشاعري؟** عندما تكون فضوليًا أو خائفًا أو متحمسًا بشكل خاص فمن غير المرجح أن تقيم عواقب أفعالك، في الواقع ربما لن تفكر في شرعية الموقف المعروض عليك، اعتبر هذا علمًا أحمر إذا كانت حالتك العاطفية مرتفعة.
- **هل جاءت هذه الرسالة من مرسل شرعي؟** افحص عناوين البريد الإلكتروني وملفات تعريف الوسائط الاجتماعية بعناية عند تلقي رسالة مريبة، قد تكون هناك أحرف تحاكي الآخرين، مثل "**torn@example.com**" بدلاً من ."**tom@example.com**" ملفات تعريف الوسائط الاجتماعية المزيفة التي تكرر صورة صديقك، وتفاصيل أخرى شائعة أيضًا.
- **هل قام صديقي بالفعل بإرسال هذه الرسالة إلي؟** من الجيد دائمًا سؤال المرسل عما إذا كان هو المرسل الحقيقي للرسالة المعنية، سواء كان زميل عمل أو شخصًا آخر في حياتك، اسأله شخصيًا أو عبر مكالمة هاتفية إن أمكن، قد تم اختراقهم وهم لا يعرفون أو ربما ينتحل شخص ما حساباتهم.

- **هل يحتوي موقع الويب الذي أستخدمه على تفاصيل غريبة؟** يمكن أن تكون المخالفات في **عنوان URL** وجودة الصورة الرديئة، وشعارات الشركة القديمة أو غير الصحيحة، والأخطاء المطبعية لصفحات الويب بمثابة علامات حمراء لموقع ويب احتيالي، إذا قمت بإدخال موقع ويب مخادع، فتأكد من المغادرة على الفور.
- **هل هذا العرض يبدو جيدا لدرجة يصعب تصديقها؟** في حالة الهبات أو طرق الاستهداف الأخرى، تعتبر العروض حافزًا قويًا لدفع هجوم الهندسة الاجتماعية إلى الأمام، يجب أن تفكر في سبب تقديم شخص ما لك شيئًا ذا قيمة مقابل القليل من الربح من نهايته، كن حذرًا في جميع الأوقات لأنه حتى البيانات الأساسية مثل عنوان بريدك الإلكتروني يمكن حصادها وبيعها للمعلنين البغيضين.
- **المرفقات أو الروابط المشبوهة؟** إذا ظهر ارتباط أو اسم ملف غامضًا أو غريبًا في الرسالة، فأعد النظر في مصداقية الاتصال بالكامل، أيضًا ضع في اعتبارك ما إذا كانت الرسالة نفسها قد تم إرسالها في سياق غريب أو وقت أو ترفع أي علامات حمراء أخرى.
- **هل يستطيع هذا الشخص إثبات هويته؟** "إذا لم تتمكن من جعل هذا الشخص يتحقق من هويته مع المنظمة، يدعي أنه جزء منها فلا تسمح له بالوصول الذي يطلبه، حيث تتطلب الانتهاكات الجسدية التغاضي عن هوية المهاجم.(**لطف جاد الله، عبد العزيز (2017)، ص 235**)

رابعاً: كيفية منع هجمات الهندسة الاجتماعية:

بالإضافة إلى اكتشاف أي هجوم يمكن الفرد أيضًا أن يكون استباقيًا بشأن خصوصيته وأمانه، حيث تُعد معرفة كيفية منع هجمات الهندسة الاجتماعية أمرًا مهمًا للغاية لجميع مستخدمي الأجهزة المحمولة وأجهزة الكمبيوتر، فيما يلي بعض الطرق المهمة للحماية من جميع أنواع الهجمات الإلكترونية:

1- عادات الاتصال الآمن وإدارة الحساب:

الاتصال عبر الإنترنت هو المكان الذي تكون فيه عرضة للخطر بشكل خاص، حيث تُعد الوسائط الاجتماعية والبريد الإلكتروني والرسائل النصية أهدافًا شائعة، ولكنه سيحتاج أيضًا إلى حساب التفاعلات الشخصية أيضًا.

2- لا يجب النقر أبدًا على الروابط الموجودة في أي رسائل بريد إلكتروني:

سيحتاج الفرد دائمًا إلى كتابة عنوان **URL** يدويًا في شريط العناوين الخاص به، بغض النظر عن المرسل، ومع ذلك عليه أن يتخذ الخطوة الإضافية للتحقيق للعثور على نسخة رسمية من عنوان **URL** المعني، لا يتعامل مطلقًا مع أي

عنوان **URL** لم يتحقق منه على أنه رسمي أو شرعي"(**زيوش، سعيد وبومدفع، الطاهر(2020)، ص4**).

3– استخدم المصادقة متعددة العوامل:

تعد الحسابات عبر الإنترنت أكثر أمانًا عند استخدام أكثر من مجرد كلمة مرور لحمايتها، تضيف المصادقة متعددة العوامل طبقات إضافية للتحقق من هوية الفرد عند تسجيل الدخول إلى الحساب، يمكن أن تشمل هذه "العوامل "القياسات الحيوية مثل بصمات الأصابع أو التعرف على الوجه، أو رموز المرور المؤقتة المرسلة عبر رسالة نصية.

4– استخدم كلمات مرور قوية (ومدير كلمات مرور):

يجب أن تكون كل كلمة مرور فريدة ومعقدة، على الفرد أ يستهدف استخدام أنواع أحرف متنوعة، بما في ذلك الأحرف الكبيرة والأرقام والرموز، أيضًاقد يفضلالفرد في اختيار كلمات مرور أطول عندما يكون ذلك ممكنًا .لمساعدته في إدارة جميع كلمات المرور المخصصة، وقد يفضلأيضا في استخدام مدير كلمات المرور لتخزينها وتذكرها بأمان.

5– تجنب مشاركة أسماء مدارسك أو حيواناتك الأليفة أو مكان ميلادك أو أي تفاصيل أخرى:

قد يقوم الفرد بكشف إجابات لأسئلة الأمان الخاصة به أو أجزاء من كلمة المرور الخاصة به دون قصد، إذا قام الفرد بإعداد أسئلة الأمان الخاصة به بحيث لا تُنسى ولكنها غير دقيقة، فسيجعل من الصعب على المجرم اختراق حسابه.

مثال: إذا كانت سيارتك الأولى من طراز "تويوتا"، فإن كتابة كذبة مثل "سيارة المهرج" يمكن أن تتخلص تمامًا من أي متسللين متطفلين.(**سلمان الجبوري، سامر (2018)، ص 99**)

6–كن حذرًا جدًا في بناء صداقات عبر الإنترنت فقط:

على الرغم من أن الإنترنت يمكن أن يكون وسيلة رائعة للتواصل مع الأشخاص في جميع أنحاء العالم، إلا أن هذه طريقة شائعة لهجمات الهندسة الاجتماعية، على الفرد أن يراقب التحذيرات الصادرة من برامج الحماية الشرعية والتي تشير إلى التلاعب أو إساءة استخدام الثقة بشكل واضح.

7– عادات استخدام الشبكة الآمنة:

يمكن أن تكون الشبكات المخترقة عبر الإنترنت نقطة ضعف أخرى يتم استغلالها للبحث في الخلفية، لتجنب استخدام بيانات الفرد ضده، عليه اتخاذ تدابير وقائية لأي شبكة يتصل بها.

8– لا تسمح أبدًا للغرباء بالاتصال بشبكة Wi-Fi الأساسية الخاصة بك:

في المنزل أو في مكان العمل يجب أن يكون الوصول إلى اتصال **Wi-Fi** متاحًا، يسمح هذا لاتصالك الرئيسي المشفر والمحمي بكلمة مرور بالبقاء آمنًا وخاليًا من الاعتراضات، إذا قرر شخص ما "التنصت" للحصول على معلومات، فلن يتمكن من الوصول إلى النشاط الذي يرغب الفرد والآخرون في الحفاظ على خصوصيته.

9– استخدم VPN:

ويعني ''شبكة خاصة افتراضية''، هو خدمة تشفر حركة مرورك على الإنترنت وحماية هويتك أونلاين باستخدام **VPN**، يمكنك الوصول بأمان إلى التطبيقات والمواقع الإلكترونية ومنصات الترفيه من أي مكان في العالم.

في حالة عثور شخص ما على شبكة الفرد الرئيسية – سلكية أو لاسلكية أو حتى خلوية – على طريقة لاعتراض حركة المرور، يمكن لشبكة افتراضية خاصة **(VPN)** إبعادهم. الشبكات الافتراضية الخاصة هي خدمات تمنح الفرد "نفقًا" خاصًا ومشفّرًا على أي اتصال إنترنت يستخدمه، لا يتم حماية اتصاله من أعين غير مرغوب فيها فحسب، بل يتم إخفاء هويته، لذا لا يمكن تتبعها عبر ملفات تعريف الارتباط أو غيرها من الوسائل.

10– حافظ على أمان جميع الأجهزة والخدمات المتصلة بالشبكة:

كثير من الناس على دراية بممارسات أمان الإنترنت لأجهزة الكمبيوتر المحمولة والتقليدية، ومع ذلك فإن تأمين شبكة الفرد نفسها، حيث بالإضافة إلى جميع أجهزته الذكية والخدمات السحابية، لا تقل أهمية عن ذلك، عليه أن يتأكد من حماية الأجهزة التي يتم التغاضي عنها بشكل شائع مثل أنظمة المعلومات والترفيه في السيارة وأجهزة توجيه الشبكة المنزلية(**gps**)، "يمكن أن تؤدي انتهاكات البيانات على هذه الأجهزة إلى إضفاء الطابع الشخصي على عملية احتيال الهندسة الاجتماعية".**(علي عباس، مراد (2017)، ص 55)**

11– عادات استخدام الجهاز الآمن:

إن الحفاظ على أجهزة الفرد نفسها لا يقل أهمية عن جميع سلوكياته الرقمية الأخرى، فعليه حماية هاتفه المحمول وجهازه اللوحي وأجهزة الكمبيوتر الأخرى بالنصائح التالية:

– عليه أن يستخدم برنامج أمان الإنترنت الشاملفي حالة نجاح التقنيات الاجتماعية، تُعد الإصابة بالبرامج الضارة نتيجة شائعة، لمكافحة الجذور الخفية وأحصنة طروادة والروبوتات الأخرى من الضروري استخدام حل أمان إنترنت عالي الجودة يمكنه القضاء على العدوى والمساعدة في تتبع مصدرها.

– لا يجب ترك الأجهزة غير آمنة في الأماكن العامة أبدًا فعليه القيام دائمًا بقفل جهاز الكمبيوتر والأجهزة المحمولة، خاصة في العمل عند استخدام جهازك في الأماكن العامة مثل المطارات والمقاهي، احتفظ بها دائمًا في حوزتك.

– حافظ على تحديث جميع برامجك بمجرد توفرها، توفر التحديثات الفورية لجميع برامج المثبتة إصلاحات أمان أساسية، عندما يتخطى الفرد أو يؤخر تحديثات نظام التشغيل أو التطبيقات، فإنهيترك ثغرات أمنية معروفة مكشوفة للمتسللين لاستهدافها، وبما أنهم يعرفون أن هذا سلوك العديد من مستخدمي الكمبيوتر والجوّال، فقد يصبح الفرد هدفًا رئيسيًا لهجمات البرامج الضارة المصممة اجتماعيًا.

– تحقق من وجود خروقات بيانات معروفة لحساباتك على الإنترنت، تراقب خدمات برمجية مشروعة مثل **Kaspersky Security Cloud** بشكل فعّال عمليات اختراق البيانات الجديدة والحالية لعناوين بريدك الإلكتروني .إذا تم تضمين حسابات الفرد في بيانات تم اختراقها، فسيتلقى إشعارًا مع نصائح حول كيفية اتخاذ إجراء (**Administration, Kaspersky(2008)**)..

خاتمـــــة:

يعد الأمن السيبراني جزءًا من مظلة أمن تكنولوجيا المعلومات، إلى جانب نظرائه والأمن المادي وأمن المعلومات، النقطة المهمة هي أنه ليست كل تدابير أمن تكنولوجيا المعلومات مؤهلة له، حيث أن للأمن السيبراني أصوله المميزة التي يجب حمايتها.

وتبدأ الحماية من الهندسة الاجتماعية بالوعي والتعليم، إذا كان جميع المستخدمين على دراية بالتهديدات، فسوف تتحسن سلامتنا كمجتمع افتراضي جماعي، علينا المساهمة جميعا من زيادة الوعي بهذه المخاطر من خلال مشاركة ما تعلمناه مع الزملاءأو الأصدقاء أو المعلمين.

بطبيعة الحال فإن التهديد الذي تتعرض له هذه الأصول الإلكترونية يتمثل في قراصنة لديهم نية خبيثة لسرقة بيانات ومعلومات الملكية عبر عمليات اختراق للبيانات.

وبالتالي يبدو أن التعريف الذي تم إدراكه بالكامل يجب أن يتضمن مجموعة متطورة من أدوات الأمن السيبراني المصممة لحماية البيانات السرية من الوصول غير المصرح به .للقيام بذلك، من الضروري النظر في كيفية قيام الأشخاص والعمليات والتكنولوجيا بأدوار متساوية الأهمية في الحفاظ على أمان المعلومات.

– اقتراحات عملية:

هناك مجموعة من الاقتراحات التي نرى أنها قد تفيد مستخدم الشبكة حيث نوجزها كما يلي:

1- على المستخدم أن يحاول وبجدية أن يتلقى (أن يكون مستعداً لتلقي) معلومات مهمة حول كيفية التعامل مع شبكة الانترنت (الصفحات المختلفة، البريد الالكتروني، وسائل التواصل الاجتماعي، ...)، إذا اقتضت الضرورة يجب عليه الاتصال بمن هو أهل لذلك، كما يجب إنشاء كلمات مرور قوية باستخدام أحرف كبيرة وصغيرة مع أرقام ورموز وأن تحفظ هذه كلمات السر في سجل أو كتاب يكون في مكان آمن.

2- أن يراقب النشاط المشبوه الذي يطلب منه القيام بشيء ما على الفور، أو يقدم شيئا يبدو جيدا جدا بحيث لا يمكن أن يكون صحيحا أو يحتاج إلى معلوماته الشخصية، هنا عليه التفكير جيدا قبل النقر (عندما تكون في شك أو شيء مبهم لا تنقر وأغلق الصفحة).

3- حماية منزل المستخدم أو مكان العمل باستخدام اتصال إنترنت آمن وشبكة واي فاي، وتغيير كلمات المرور بانتظام.

4- لا يشارك عبر الانترنت أرقام التعريف الشخصية أو كلمات المرور أو أرقام البطاقة الذهبية أو أي بطاقة بنكية أخرى أو أي رقم حساب بنكي أو بريدي.

5- لا ينقر على الروابط في النصوص أو رسائل البريد الإلكتروني من أشخاص لا يعرفهم، حيث يمكن للمحتالين إنشاء روابط وهمية لمواقع الويب.

6- يضع في اعتباره أن المحتالين قد يحاولون الاستفادة من الاحتياجات المالية من خلال الاتصال بفرص العمل من المنزل وغيرها من العروض الأخرى، حيث يمكنه الاتصال بالشرطة وتقديم كافة المعلومات لهم حتى يتسنى للفرقة المكلفة بالحماية من الجرائم عبر شبكة الانترنت من مساعدته.

المراجـــع:

1. درة، خضر (2013). **الجرائم المالية في الفضاء الإلكتروني**، بيروت لبنان: شركة المطبوعات للتوزيع والنشر.
2. زيوش، سعيد (2017) "**ظاهرة الابتزاز الالكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية**"، مجلة العلوم الاجتماعية، المجلد 11، العدد 1، جامعة عمار ثليجي الأغواط، الجزائر.
3. زيوش، سعيد، بومدفع، الطاهر (2020)"**الحرية الالكترونية وآليات الرقابة المجتمعية في الجزائر**"، مجلة الخلدونية، المجلد 12، العدد1، جامعة ابن خلدون تيارت، الجزائر.
4. حسن، شفيق (2017). **الإعلام الجديد والجرائم الإلكترونية**، القاهرة مصر: دار فكر وفن.

5. لطف جاد الله، عبد العزيز (2017). **أمن المجتمع الالكتروني**، الاسكندرية مصر: مكتبة الوفاء القانونية.

6. محمد عبد الرؤوف المنيفي، أحمد (2021). **الاحتيال الإلكتروني وحكمه في الاسلام والقوانين المعاصرة**، لبنان: شبكة الألوية. www.alukah.net

7. محمد النور أحمد، معتصم (17 12، 2019) "**الهندسة الاجتماعية**"، https://www.noor-book.com تاريخ الاطلاع: 2021/05/05.

8. سلمان الجبوري، سامر (2018). **جريمة الإحتيال الإلكتروني – دراسة مقارنة**، لبنان: منشورات زين الحقوقية.

9. علي عباس، مراد (2017). **الهندسة الاجتماعية؛ صناعة الإنسان والمواطن**، بيروت لبنان: دار الروافد الثقافية.

10. شعبان تهامي، عبدالرحمن (2020) "**الهندسة الاجتماعية**"، https://www.noor-book.com، تاريخ تصفح الموقع: 2021/05/17، الساعة 23:11.

11. Administration, K. (2008, 4 1). **"What is Social Engineering**? " **https://usa.kaspersky.com/ resource-center/definitions/what-is-social-engineering** , the date the resea rcher browsed the site: 05/ 03/ 2021.

12. Jem, Dantis (2019) "**What is social engineering**?", **https://www.itgovernance.co.uk/social-engineering-attacks**, the date the researcher browsed the site: 05/05/2021.

13. Kemp, S. (2021, 02 11). **'DIGITAL 2021: ALGERIA'**, **https://datareportal.com/reports/digital-2021-algeria**, the date the researcher browsed the site: 05/05/2021.

14. Kuston, Clarc (2018) "**What Is Cybersecurity?**", **https://www.comptia.org/content/articles/what-is-cybersecurity**, the date the researcher browsed the site: 02/05/2021.

15. Nate, Lord (2018) "**Defining and Avoiding Common Social Engineering Threats**", **https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats**, the date the researcher browsed the site: 06/05/2021

16. Thornburgh, T. (2004, 10). "*Social engineering: the "Dark Art"*, the date the researcher browsed the site ;05/ 04/2021

17. Vander, C (2019) " How does social engineering work? "https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html," the date the researcher browsed the site: 06/05/2021.