جامعة غرداية

كلية العلوم الاقتصادية و التجارية وعلوم التسيير

قسم علوم التسيير

بالتعاون مع مخبر الدراسات التطبيقية في العلوم المالية والمحاسبة

ينظمون ملتقى وطني (حضوري/ عن بعد) بعنوان:

" مخاطر الهندسة الاجتماعية ومتطلبات تحقيق الأمن المجتمعي

للمؤسسات الاقتصادية"، يوم 04 ماي 2025.

مداخلة بعنوان:

دور الوعي المعلوماتي لدى مستخدمي المؤسسة في التصدي لهجمات الهندسة الاجتماعية

من إعداد الباحثين :

- مراد عبد القادر، أستاذ محاضر أ، جامعة زيان عاشور الجلفة ، a.merrad @univ-djelfa.dz
- راقع حسن ، أستاذ محاضر ب، جامعة زيان عاشور الجلفة ، hassen.ragaa@univ-djelfa.dz

من خلال المحور رقم: 01

الملخص:

مع تنامي قوة استراتيجيات الأمن السيبراني وتحدياتها، يُطوّر قراصنة المعلومات هجماتهم لتصبح أكثر مراوغة، معتمدين في ذلك على الهجمات القائمة على الهندسة الاجتماعية لاستغلال العامل البشري (مستخدمي المؤسسة) في اختراق البنية الأمنية للمؤسسات. حيث تستغل هجمات الهندسة الاجتماعية سماتٍ بشريةً ونفسيةً محددةً لتجاوز التدابير الأمنية و التقنية للمؤسسة، وبسبب ان تلك الهجمات لا تتبع أنماطًا أو مناهج محددة لشنّ الهجوم، يجعل منها اداة سهلة، فعالة و في نفس الوقت غامضة لاختراق اي مؤسسة يصعب للغاية مواجهتها. ومن ثمة فقد أصبحت الهندسة الاجتماعية نهجًا واسع الانتشار يُستخدم من طرف القراصنة لاختراق الأفراد والمؤسسات على حد سواء، ولمواجهة مثل تلك الهجمات، يُعدّ فهم طرق الهجوم ومواجهته بشكل أفضل أمرًا بالغ الأهمية. لذا، تُقدّم هذه الورقة البحثية الطرق المستخدمة في شنّ الهجمات القائمة على الهندسة الاجتماعية وسبل مواجهتها.

الكلمات المفتاحية: وعي ملعوماتي، أمن سيبراني، هندسة إجتماعية، عامل بشري.

Abstract:

As cyber security strategies grow in strength and challenge, hackers are developing more sophisticated attacks, relying on social engineering to exploit the human factor (organizational users) to breach the security infrastructure of organizations. Social engineering attacks exploit specific human and psychological traits to bypass an organization's security and technical measures. Because these attacks do not follow specific patterns or methods, they are an easy, effective, and at the same time obscure tool for infiltrating any organization, making them extremely difficult to counter. Social engineering has thus become a widespread approach used by hackers to compromise both individuals and organizations. To combat such attacks, a better understanding of attack methods and how to counter them is crucial. This paper presents the methods used to launch social engineering-based attacks and ways to counter them.

Keywords: : Information literacy, cyber security, social engineering, human factor.

.

1. مقدمة:

أصبح الفضاء السيبراني ضروريا لعمل أغلب مستخدمي المؤسسات، وذلك بسبب التطوّر التكنولوجي الذي شهده العالم مؤخرا، حيث أصبح مستخدمو المؤسسات يلجئون إلى مختلف المواقع للحصول على المعلومات الحديثة في مجال عملهم، وحتّى للقيام بدورات تدريبية لتحسين كفاءتهم وزيادة إنتاجيتهم، ومع تزايد ولوج المستخدمين لفضاءات الانترنت جعلهم عرضة لمختلف الهجمات السيبرانية التي تعتمد على أساليب الهندسة الاجتماعية للحصول على معلومات خاصة بالفرد والمؤسسة على حدّ السواء ممّا يعرّض هذه الاخيرة لأخطار عديدة تؤثر على أدائها وتنافسيّتها.

ومن أجل معرفة الطرق القائمة على الهندسة الاجتماعية وجب علينا أولا تحديد المعنى الدقيق لهذا المصطلح ، وقد ورد في موقع خاص ببرنامج الحماية الشهير "كاسبرسكي" التعريف الاتي : "الهندسة الاجتماعية تقنية تلاعب تستغل الخطأ البشري للحصول على معلومات خاصة أو حق الوصول أو الأشياء الثمينة. وفي الجرائم الإلكترونية، تميل عمليات احتيال "القرصنة البشرية" هذه إلى إغراء المستخدمين المطمئنين لكشف بياناتهم، أو نشر إصابات البرامج الضارة، أو منح الوصول إلى الأنظمة المقيدة. ويمكن أن تحدث الهجمات عبر الإنترنت، وبشكل شخصي، وعبر تفاعلات أخرى.

تتمحور عمليات الاحتيال القائمة على الهندسة الاجتماعية حول كيفية تفكير الأشخاص وتصرفاتهم. وعلى هذا النحو، تكون هجمات الهندسة الاجتماعية مفيدة بشكل خاص للتلاعب بسلوك المستخدم. وبمجرد أن يفهم المهاجم ما يحفز تصرفات المستخدم، يمكنه خداع المستخدم والتلاعب به بشكل فعال.

بالإضافة إلى ذلك، يحاول المتسللون استغلال نقص المعرفة لدى المستخدم .وبفضل سرعة التكنولوجيا، لا يدرك العديد من المستهلكين والموظفين بعض التهديدات مثل التنزيلات العرضية .وقد لا يدرك المستخدمون أيضًا القيمة الكاملة للبيانات الشخصية، مثل أرقام هواتفهم. ونتيجة لذلك، لا يتأكد العديد من المستخدمين من كيفية حماية أنفسهم ومعلوماتهم بأفضل طريقة".[1]

وعليه يمكن طرح الاشكالية التالية : **كيف يمكننا التصدي لهجمات الهندسة الاجتماعية من خلال الوعي المعلوماتي؟**

2. مفهوم هجمات الهندسة الاجتماعية

تعرف الهندسة الاجتماعية بأنها فن استغلال علم النفس البشري، بدلاً من أساليب الاختراق التقنية، للوصول إلى المباني أو الأنظمة أو البيانات. وهي إحدى الطرق الفعالة لاستغلال الأخطاء البشرية[2]. وتعرف بأنها مجموعة من التقنيات والمهارات التي تستهدف الجانب البشري في الامن السيبراني، وتهدف الى التأثير على الناس وإقناعهم بالقيام بأشياء تخدم مصالح المهاجمين او المخترقين، مثل الكشف عن المعلومات السرية او السماح بالوصول الى الانظمة او الشبكات او التعرض للبرمجيات الخبيثة. الهندسة الاجتماعية تعتمد على استغلال الثغرات النفسية والسلوكية والاجتماعية للضحايا، مثل الثقة والفضول والخوف والجشع والرغبة في المساعدة[3].

1.2 طريقة عمل الهندسة الاجتماعية:

تعتمد معظم هجمات الهندسة الاجتماعية على التواصل الفعلي بين المهاجمين والضحايا، حيث يميل المهاجم الى تحفيز المستخدم على تعريض نفسه للخطر بدلا من استخدام اساليب الاحتيال والمراوغة لخرق بياناته، تمنح دورة الهجوم هؤلاء المجرمين عملية موثوقة لخداعه، عادة ماتكون خطوات دورة هجوم الهندسة الاجتماعية على النحو التالي[4]:

- استعد من خلال جمع معلومات اساسية عنك او عن مجموعة اكبر انت جزء منها؛
- تسلل من خلال اقامة علاقة او بدء تفاعل يبدأ ببناء الثقة؛
- استغل الضحية بمجرد ان تنشا الثقة والضعف لتعزيز الهجوم؛
- فك الارتباط بمجرد ان يتخذ المستخدم الاجراء المطلوب.

3. انواع الهجمات القائمة على الهندسة الاجتماعية

1.3 هجمات التصيد الاحتيالي (Phishing Attack) :

عرف التصيد الاحتيالي على أنه استخدام رسائل البريد الإلكتروني، المصممة لتبدو وكأنها رسائل من جهة موثوقة، مثل البنك أو موقع المزادات أو موقع التجارة الإلكترونية. عادةً ما تطلب هذه الرسائل من المستخدم اتخاذ شكل من أشكال الإجراءات، مثل التحقق من صحة معلومات حسابه، غالبًا ما يستخدمون الشعور بالإلحاح (مثل التهديد بتعليق الحساب) لتحفيز المستخدم على اتخاذ إجراء. في الآونة الأخيرة، كانت هناك العديد من أساليب الهندسة الاجتماعية الجديدة لخداع المستخدمين الغافلين. تتضمن هذه الطرق عرض ملء استبيان لموقع مصرفي عبر الإنترنت بمكافأة مالية إذا أدرج المستخدم معلومات الحساب، ورسائل البريد الإلكتروني التي تدعي أنها من نوادي مكافآت تابعة للفنادق، وتطلب

من المستخدمين التحقق من معلومات بطاقة الائتمان التي قد يخزنها العميل على الموقع الرسمي لأغراض الحجز. تتضمن الرسالة رابط لموقع وهمي ليستخدمه الضحية، والذي يوجه المستخدم بعد ذلك إلى موقع لإدخال معلوماته الشخصية. تم تصميم هذا الموقع لتقليد شكل ومظهر الموقع الرسمي. ثم يتم جمع المعلومات واستخدامها من قبل المجرمين[5].

2.3 هجمات التصيد بالرمح (Spear-Phishing Attack) :

التصيد بالرمح هو شكلٌ من اشكال التصيد الاحتيالي، يستهدف تحديدًا الأفراد أو المؤسسات لسرقة معلومات حساسة، مثل بيانات تسجيل الدخول أو البيانات المالية، أو لنشر برامج ضارة داخل الشبكة. على عكس هجمات التصيد الاحتيالي العامة، التي تُغطي نطاقًا واسعًا للإيقاع بأي ضحية غافلة، فإن التصيد الاحتيالي الموجه مُصممٌ بدقة للاستهداف الفردي، مما يجعله أكثر خطورةً وفعاليةً بشكل ملحوظ[6]. حيث يستخدم المهاجمون الأكثر تطورًا التصيد بالرمح لتضييق نطاق الفئة المستهدفة التي قد تكون من نفس المؤسسة او من نفس مجال العمل وزيادة دقة رسائلهم مما يعزز مصداقيتهم عند تلك الفئة[7].

3.3 هجمات الغوص في حاويات النفايات (Dumpster Diving Attack):

هجوم الغوص في حاويات النفايات هو أسلوب بسيط يُستخدم للحصول على معلومات عن الهدف. تتضمن العملية البحث في النفايات عن مستندات ممزقة وإيصالات وأوراق أخرى قد تحتوي على معلومات عن الهدف، حيث يمكن لهذه المعلومات أن تساعد المتسللين بطرق متعددة لشن هجوم إلكتروني على شخص ما. يُعد الغوص في حاويات النفايات أيضًا من أكثر أساليب سرقة الهوية شيوعًا.

4.3 هجمات الهندسة الاجتماعية العكسية (Reverse Social Engineering Attack) :

تُعد هجمات الهندسة العكسية من أبسط أساليب الهجوم وأكثرها فعالية في هجمات هندسة النظم. تُنفذ هجمات الهندسة العكسية على خطوتين. أولاً، يُنشئ المُهاجم الخبيث مشكلةً للهدف. الفكرة الأساسية وراء خلق المشكلة هي بدء تفاعل مع الهدف. ثانياً، يُقدم المُهاجم الخبيث حلاً لتلك المشكلة للضحية. على سبيل المثال، يُحدد المُهاجم هدفاً مُحتملاً في مؤسسة، ويُنشئ عمداً مشكلةً تتعلق بقسم تكنولوجيا المعلومات. لاحقاً، يُقدم المُهاجم صفة شخص من قسم تكنولوجيا المعلومات، ويُقدم المساعدة. تُستخدم هذه الأفعال لكسب ثقة الهدف المُستهدف. مع مرور الوقت، يكتسب المُهاجم الخبيث ثقةً أكبر، ويستغل عامل الثقة للحصول على معلومات حساسة أو التلاعب بالضحية. تُعتبر هجمات الهندسة العكسية هجمات شائعة جداً على مستوى المؤسسات[8].

5.3 هجمات ثقب الماء (Water Hole Attack) :

تعمل هجمات "ثقب الماء" على استهداف مواقع الويب الرسمية التي يزورها المستخدمون بشكل متكرر. تتمثل الخطوة الأولى للمهاجم في إنشاء ملف تعريف للمستخدمين المستهدفين لمعرفة المواقع التي يميلون إلى زيارتها. عادةً ما يكون هؤلاء مستخدمين في شركات كبيرة أو وكالات أو حتى منظمات حقوق الإنسان، وقد تكون المواقع التي يزورونها منتديات نقاش أو مؤتمرات متخصصة في مجالهم. بعد تحديد المواقع الأكثر زيارة، تاتي الخطوة الثانية حيث يبحث المهاجم عن ثغرة أمنية فيها، ويستغلها ويحقنها ببرمجيات خبيثة، في الخطوة الثالثة يمكن من خلال البرمجيات المخقونة بعد ذلك إعادة توجيه الضحية إلى موقع ويب مزيف. كل ما على المهاجم فعله بعد إصابة الموقع هو انتظار وصول الضحايا إليه. بعض هذه الهجمات ستُدخل وتُثبت برامج ضارة على النظام دون أن يدرك المستخدم ذلك. يُعرف هذا باسم الهجوم المُتطفل. ولا يقتصر تأثيره على سيطرة المهاجم الكاملة على جهاز الضحية فحسب، بل يمتد إلى الوصول إلى شبكته أيضًا، و تكمن المشكلة الحقيقية هنا عندما يربط الضحية الجهاز المُصاب بشبكة عمله، دون علمه بالوضع. وهكذا، كخطوة اخيرة يكتمل الهجوم "المُتطفل" ويتمكن المهاجم من الوصول إلى شبكة الشركة او المؤسسة دون إصابة بنيتها التحتية إطلاقًا[9].

6.3 هجمات برنامج الرعب (Scareware Attack):

ويمكن تعريفه على انه نوع من هجمات الهندسة الاجتماعية التي تعتمد على المشاعر الانسانية(مثل القلق والصدمة والتلاعب).يستخدم هذا الهجوم المشاعر الانسانية للتلاعب بالمستخدمين لتثبيت برمجيات خبيثة. يمكن رؤية اجراء هجمات البرمجيات الخبيثة من خلال حقيقة ان القراصنة يجذبون الاهداف باستخدام تنبيهات منبثقة على مواقع الويب المختلفة.عندما ينقر الهدف على النافذة المنبثقة، يتم اعطاء معلومات مضللة له، حيث تهدف هذه المعلومات المضللة الى التاثير عليه لدفعه الى الذعر واتخاذ اجراء ما. قد يطلب الاجراء المقصود من الهدف تقديم معلومات سرية او شراء منتج لحل مشكلة وهمية. في هجوم التخويف يحتاج المخترق فقط الى اقناع الضحية بالنقر على رابط ما. ولتحقيق هذا الاقناع، يمكن للمهاجمين استخدام العديد من التقنيات لحمل الضحايا على تثبيت البرمجيات الخبيثة. تعتبر الواجهة الرسومية لبرمجيات التخويف عنصر اساسيا لخداع الضحايا من عدة نواح. فالتمثيلات المرئية للبرمجيات (مثل النوافذ المنبثقة او تقارير الفحص) تعطي مظهرا وكانه تطبيق جدير بالثقة[10].

7.3. هجمات المقايضة(Quid Pro Quo):

تُشبه هذه التقنية الهجومية القائمة على الهندسة الاجتماعية تقريبًا أساليب الإغراء والتصيد الاحتيالي. إلا أن ما يميز هذا النوع من التهديدات هو أن المهاجم يقدم الهجوم على أنه خدمة دعم فني مقابل معلومات،

يهدف من خلال تلك الخدمة إلى نشر برمجيات خبيثة على نظام المستخدم. على سبيل المثال، يتظاهر المهاجم بأنه خبير تكنولوجيا معلومات لمساعدة مستخدم يحتاج إلى دعم فني، ومن خلال الوصول إلى النظام الذي يستخدمه المستخدم (الضحية) ، يُمكن للمهاجم زرع أي جهاز أو برنامج في ذلك النظام[11].

4.نقاط الضعف البشرية في الهندسة الاجتماعية

تستغل هجمات الهندسة الاجتماعية مجموعة واسعة من نقاط الضعف البشرية يذكر منها[12]:

1.4 نقاط الضعف البشرية في الإدراك والمعرفة:

ان الإدراك القائم على الاستدلالات أو الاختصارات الذهنية، مثل الأحكام الحدسية والاندفاعية، يكون أكثر عرضة للاستغلال في محاولات الهندسة الاجتماعية الإقناعية. وسيكون من الصعب جدًا ضمان أمن المعلومات بالنسبة للموظفين غير المبالين بعملهم، ، خاصةً عند عدم اتباع قواعد الأمن. كما يمكن للمهاجمين استغلال الجهل (على سبيل المثال، انخفاض الوعي بقيمة المعلومات والأمان) بسهولة، من خلال "النهج المباشر". فالجهل وقلة الخبرة يؤديان إلى مخاطر أمنية. لذى يجب توعية المستخدمين بما يشكل معلومات حساسة وكيف يمكن إساءة استخدامها في الهجمات عبر الإنترنت.

2.4 نقاط الضعف البشرية في السلوك والعادة:

عندما لا يولي الشخص اهتمامًا كافيًا لسياق الأمان، أو لا يفكر في المخاطر الأمنية المحتملة، أو لا يرغب في بذل العمل أو الجهد اللازم لمنع التهديد الأمني، فسيكون هذا الشخص هدفًا يمكن من خلاله بسهولة التعرض لهجوم الهندسة الاجتماعية.

يوجد نمط أفعال ثابت في سلوكيات كل من الحيوانات والبشر، ويتألف من سلسلة من السلوكيات الغريزية الثابتة نسبيًا، والتي يُحفزها مُحفز رئيسي. هذه المجموعة من الأفعال تلقائية ولا إرادية، وتكتمل حتى مع إزالة المُحفز.

ان تشابه العادات السلوكية المتميزة بالطوعية والتلقائية مع نمط الفعل الثابت الموجود في سلوكيات البشر، يجعل منها عرضة لهجمات الهندسة الاجتماعية، ويجعل من الصعب على المستهدفين إدراك تعرضهم للاستغلال. على سبيل المثال، في هجوم "ثقب الماء"، إذا اعتاد المستهدفون زيارة مواقع ويب معينة بشكل دوري، فقد يُصيب المهاجم هذه المواقع ببرمجيات خبيثة مسبقًا وينتظر المستهدفين لزيارتها وتفعيلها[13].

3.4 نقاط الضعف البشرية في العاطفة والشعور

تؤثر العواطف والمشاعر على الإدراك والمواقف واتخاذ القرارات. العواطف (الخوف، التوتر، الفضول، الإثارة، المفاجأة، الغضب، الاندفاع، إلخ) والمشاعر (السعادة، الحزن، الاشمئزاز، الشعور بالذنب، إلخ) كلها عوامل بشرية يمكن استغلالها كثغرات أمنية في هجمات الهندسة الاجتماعية. وكثيرًا

ما يُستخدم الخوف من الوقوع في مشاكل مع الرؤساء في أسلوب التشهير للحصول على معلومات حساسة، كما يُعدّ إثارة الخوف مثالًا واضحًا على ذلك. فعندما تُثار مشاعر قوية، مثل الغضب، أو الإثارة، أو الخوف، أو القلق، قد تُعيق القدرة الإدراكية للفرد بشكل خطير. غالبًا ما يصاحب الشعور بالذنب العار والندم، وهي مشاعر يحاول الناس التهرب منها، تتحول هذه المشاعر إلى نقاط ضعف في الهندسة الاجتماعية، على سبيل المثال، عندما ينجح المهاجمون في إقناع الهدف بأنه سيعاني بشدة (مثل توبيخ رئيسه وطرده) إذا لم يُلبَّ الطلب. هنا، يُحفِّز شعورٌ متوقع بالذنب الهدف على اتخاذ قرارٍ متساهل و لكنه مُخترق أمنيًا.

4.4 نقاط الضعف البشرية في سمات الشخصية

تساهم سمات شخصية الأفراد بشكل كبير في قابليتهم لاستغلالات الهندسة الاجتماعية، كالتأثير والتلاعب والخداع. يتعامل المهندسون الاجتماعيون مع سمات الشخصية البشرية على أنها نقاط ضعف، ويستخدمون اللغة سلاحًا لخداع الضحايا وإقناعهم، وفي النهاية التلاعب بهم. وتتجلى السمات الشخصية في بُعد الانبساط بشكل رئيسي في النشاط، والدفء، والمشاعر الإيجابية، والحزم، والسعي وراء الإثارة، والروح الاجتماعية. فالأفراد ذوو الانبساط العالي يكونون أكثر نشاطًا، وحماسًا، وحزمًا، وحيوية، وانفتاحًا، وثرثارين. وبالتالي، فإنهم عرضة للهندسة الاجتماعية من خلال آليات التأثير مثل التشابه والإعجاب والمساعدة، والإفصاح عن الذات وبناء العلاقات الودية، وإدارة الانطباعات، والالتزام والاتساق، والمخاطرة من أجل الثقة، والتوافق.

5. امثلة عن الهجمات القائمة على الهندسة الاجتماعية

1.5 هجوم التصيد الاحتيالي على اللجنة الوطنية في الولايات المتحدة الامريكية

من أبرز أمثلة هجمات التصيد الاحتيالي ما حدث خلال الانتخابات الرئاسية الأمريكية عام 2016. إذ أرسل قراصنة يُعتقد أنهم جزء من مجموعة استخبارات روسية رسائل بريد إلكتروني موجهة إلى أعضاء اللجنة الوطنية الديمقراطية (DNC)، متظاهرين بأنهم خبراء أمن من جوجل. وطلبت الرسائل من المستلمين تغيير كلمات مرورهم، مما أدى إلى اختراق حساباتهم ونشر رسائل بريد إلكتروني سرية. مما أثر بشكل كبير على المشهد السياسي، ولفت الانتباه إلى مخاطر الهندسة الاجتماعية في الانتخابات[14].

2.5 هجوم انتحال الشخصية والتظاهر على التويتر

في يوليو 2020، تعرضت العديد من حسابات تويتر البارزة، بما في ذلك حسابات باراك أوباما وإيلون ماسك وبيل غيتس، لهجوم هندسة اجتماعية. خدع المهاجمون موظفي تويتر ليتمكنوا من الوصول إلى أدوات داخلية عبر انتحال صفة فريق دعم تكنولوجيا المعلومات. سمح لهم ذلك بالتغريد

من الحسابات المخترقة، والترويج لعملية احتيال متعلقة بالعملات المشفرة. وقد سلّط هذا الهجوم الضوء على مخاطر التلاعب الداخلي والهندسة الاجتماعية داخل المؤسسات.

6. الوعي المعلوماتي:

إنّ الوعي المعلوماتي من المُصطلحات الحديثة التي بدأ الحديث عنها في عالم المعلومات، ويُعبَّر عنه أيضاً بالثقافة المعلوماتيّة، ومحو الأميّة المعلوماتية، ومهارات المعلومات. هذه الثقافة تُمكِّن أجيال الحاضر والمستقبل من المهارات التي تجعلهم مُستخدمين جُدُداً لتقنيّات الاتصالات والمعلومات، ومُحلِّلين واعين لفاعليّة وكفاءة المعلومات التي يحصلون عليها أو يواجهونها، وتُعرَّف الثقافة المعلوماتيّة أنّها المهارات التي يحتاجها الفرد ليستطيعَ العيش في عصرٍ بات يُطلَق عليه إسم عصر المعلومات. لذلك، ستساعده ثقافته المعلوماتية في البحث عن المعلومات وتنقيحها، وتقييمها، والوصول إلى النتائج الصحيحة[15].

1.6 مفهوم الوعي المعلوماتي:

يستخدم مصطلح الوعي المعلوماتي بالتبادل مع مصطلحات أخرى مثل : : محو المعلوماتية ومحو الأمية المعرفية والتوعية المعلوماتية والثقافة المعلوماتية .

ويمكن تعريفه على أنه : التعرف على الحاجة إلى المعلومات ، والقدرة على البحث عنها والوصول إليها من خلال المهارات المكتبية والتقنية ، وتقييمها ونقدها ، واستخدامها بكفاءة وإبداعية في اتخاذ القرارات وحل المشكلات[16] .

أما الأمية المعلوماتية فقد عرفته جمعية المكتبات الأمريكية عن طريق ما يفعله الشخص الذي تمحو أميته المعلوماتية بأنه الشخص الذي (يجب أن تكون له القدرة على إدراك متى يحتاج إلى المعلومات ، والقدرة على تحديد مكانها وتقييمها واستخدامها بفاعلية. وبإختصار فهو الشخص الذي تعلم كيفية التعلم Learned How to Learn وهو يعرف كيف يتعلم لأنه يعرف تنظيم المعرفة، ويعرف كيفية الوصول إلى المعلومات ويعرف كيفية استخدام تلك المعلومات بطريقة يستطيع معها الآخرون أن يتعلموا منه بعد ذلك[17] .

ولذلك أي فرد في حاجة إلى محو أميته المعلوماتية لكي يصبح واعي معلوماتياً ، فلم يعد التعليم يعني مجرد تعلم القراءة والكتابة، بل تطور وأصبح مرتبطاً بالمعلومات وتكنولوجياتها ومن ثمّ ظهر التعليم المعلوماتي.

2.6 مستويات الوعي المعلوماتي:

يمكن تحديد مستويات الوعي المعلومات من خلال عدة جوانب منها:

1.2.6. الوعي المكتبي: يتضمن الوعي المكتبي مجموعة من المهارات التي تشتمل على القدرة على استخدام المكتبة بإعتبارها مصدراً أساسياً للحصول على المعلومات : كاستخدام الفهارس وفهم نظم التصنيف واستخدام قواعد البيانات ، ثم توثيق المعلومات

2.2.6. الوعي التقني (الوعي بالحاسبات) : ويقصد به القدرة على استخدام الحاسبات الآلية وبرامجها لتنفيذ مهام عملية مثل برامج معالجة النصوص.

3.2.6. الوعي البصري : تعد الوسائل المرئية ذات دور كبير في حفظ ونقل المعلومات وذلك بتفوق الصورة المرئية في التعبير والتحكم فيها أكثر من الوسائل المطبوعة.

4.2.6. الوعي الرقمي: هو معرفة فهم الثورة الرقمية وتطبيقاتها في مجالات المعلومات ،وكذلك في البحث وتوثيق المعلومات واسترجاعها ومعالجتها وتوزيعها

5.2.6. الوعي البحثي: يعني القدرة على تحديد مفاهيم البحث وإعداد استراتيجية جيدة للبحث وتحديد مصادر المعلومات والوعي بقوانين حقوق النشر[18] .

3.6 معايير الوعي المعلوماتي بالمكتبات الجامعية العربية:

تتمثل معايير الوعي المعلوماتي لدى طلاب التعليم العالي في الوطن العربي في خمسة معاييرأساس نوجزها فيما يلي :

المعيار الأول: تحديد المعلومات:

العامل الذي لديه وعي معلومات تكون لديه القدرة على الآتي:

- تحديد طبيعة المعلومات التي يحتاج إليها.
- تحديد مصادر المعلومات المحتملة للحصول على المعلومات.
- ادراك التكاليف والقواعد المتعلقة بالحصول على المعلومات.
- إعادة تقييم طبيعة المعلومات.

المعيار الثاني : الوصول إلى المعلومات **:**

العامل الذي لديه وعي معلومات تكون لديه القدرة تحديد واختيار أنسب نظم وأدوات استرجاع المعلومات للوصول للمعلومات التي يحتاجها واختيار أكثرها كفاءة وفاعلية وذلك من خلال مجموعة من القدرات هي :

- تقييم وتنفيذ استراتيجية بحث فعالة.
- الحصول على المعلومات من خلال الإنترنت بأسوب فعال.
- مراجعة وتعديل استراتيجية البحث إذا لزم الأمر.

- استخراج وتسجيل وإدارة المعلومات والمصادر الخاصة بها

المعيار الثالث : تقييم المعلومات **:**

العامل الذي لديه وعي معلومات تكون لديه القدرة التقييم النقدي للمعلومات والمصادر الخاصة بها ويكون قادر على تضمين المعلومات الجديدة ودمجها مع قادة المعرفة الخاصة به وذلك من خلال مجموعة من القدرات:

- تلخيص الأفكار الرئيسة التي تتضمنها المعلومات التي تم جمعها
- تطبيق المعايير الأساسية الخاصة بتقييم المعلومات وكذلك المصادر الخاصة بها.
- المقارنة بين المعلومات الجديدة والمعارف السابقة لتحديد القيمة المضافة أو التناقضات الموجودة.
- التحقق من فهم وتفسير المعلومات من خلال التواصل مع الآخرين والخبراء.

المعيار الرابع: استخدام المعلومات :

العامل الذي لديه وعي معلوماتي تكون لديه القدرة على استخدام المعلومات بشكل فعال لتحقيق غرض محدد سواء بشكل فردي أو من خلال التعاون مع مجموعة من الأفراد وذلك من خلال مجموعة من القدرات هي :

- تطبيق المعلومات الجديدة والسابقة لتخطيط وتصميم منتج جديد أوإنجاز عمل ما.
- تعديل وتنقيح عمليات تطوير المنتج المعلوماتي خلال مراحل إنجازه .
- توصيل المنتج المعلوماتي بفاعلية للآخرين من خلال اختيار أنسب الوسائل والأشكال للجمهور المستهدف.

المعيار الخامس: الجوانب القانونية والأخلاقية للمعلومات :

العامل الذي لديه وعي معلومات تكون لديه القدرة فهم القضايا القانونية والاجتماعية والاقتصادية والأخلاقية المتعلقة باستخدام المعلومات بأشكالها المختلفة وذلك من خلال القدرات التالية:

- فهم القضايا القانونية والاجتماعية والاقتصادية والأخلاقية المتعلقة باستخدام المعلومات وتقنية المعلومات.
- اتباع القوانين واللوائح والسياسات المؤسسية والآداب المتعلقة باستخدام مصادر المعلومات[19].

7. الخاتمة:

مع التقدم التكنولوجي والثورة المعلوماتية الكبيرة التي شهدها العالم مؤخرا أصبحت كل المؤسسات عرضة للهجمات السيبرانية لاسيما التي تستخدم طرق الهندسة الاجتماعية وذلك لاستدراج العاملين والحصول على معلومات مهمة يمكن أن تؤثر على موقع المؤسسة، ومن هذا المنطلق توصلنا من خلال هذه الورقة البحثية إلى ضرورة إستعمال الوعي المعلوماتي بمختلف مستوياته التقنية ،الرقمية والبصرية كأداة فعالة للوقوف ضد هذه الهجمات، و من خلال ما سبق يمكننا تقديم التوصيات التالية:

- ضرورة تنظيم دورات تدريبية متخصصة للعاملين حول برامج الوعي المعلوماتي، بهدف الارتقاء بمستوى مهارات استخدام المعلومات والإفادة منها، ومهارات تقييم المعلومات ومصادرها،والمهارات التكنولوجية ، وحماية أنفسهم من الهجمات التي تعتمد أساليب الهندسة الاجتماعية.
- إعداد برنامج للوعي المعلوماتي يشمل طلبة وخريجي الجامعة في مختلف التخصصات يشتمل على مهارات كتابة البحوث والتقارير الدراسية مهارات توثيق مصادر المعلومات، مهارات البحث عن مصادر المعلومات للتكاليف والتقارير والوصول إليها واسترجاعها، مهارات اختيار مصادر المعلومات المطلوبة الموثوقة وتقييمها، مهارات استخدام المعلومات والإستفادة منها في كتابة التقارير والواجبات، المهارات التكنولوجية).
- يجب تطوير أداء العاملين عن طريق تدريبهم على برامج الوعي المعلوماتي، وذلك المواكبة التحديات والصعوبات في بيئة العمل.
- إجراء المزيد من الدراسات للوقوف على النتائج العلمية والموضوعية لواقع الوعي المعلوماتي وأساليب الحماية من الهندسة الاجتماعية والاختراق السيبراني .

8. قائمة المراجع:

[1] kaspersky. (2025, 05 01). *https://me.kaspersky.com*. Récupéré sur me.kaspersky.com: https://me.kaspersky.com/resource-center/definitions/what-is-social-engineering

[2] Govindankutty, **Is human error paving way to Cyber Security?**, International Research Journal of Engineering and Technology (IRJET), Volume: 08 Issue: 04 , Apr 2021, P 4174.

[3] عبدالله سعيد ال المحيا، اروا احمد مكين، **اثر الهندسة الاجتماعية على مخاطر الامن السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية**، مجلة الاقتصاد، الادارة والعلوم القانونية (JEALS)، المجلد 9، العدد1، 2025، ص 4.

[4] سعيد زيوش، **الاختراق عن طريق الهندسة الاجتماعية واساليب الحماية منها**، مجلة الاسرة والمجتمع، المجلد 09، العدد02، 2021، ص 175.

[5] Michael Erbschloe, **Social Engineering Hacking Systems, Nations, and Societies**,(USA,Taylor & Francis, 2020), P4.

[6] Victoria Bukky Ayoola, **Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective,** Global Journal of Engineering and Technology Advances, V20,N:3, 2024,P100.

[7] Nezir AKYEŞİLMEN & Amal ALHOSBAN, **Non-Technical Cyber-Attacks and International Cybersecurity: The Case of Social Engineering** , GAZİANTEP UNIVERSITY JOURNAL OF SOCIAL SCIENCES, V23,N:1,2024, P348**.**

[8] Siddiqi, M.A et al, **A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures**, Appl. Sci. 12, 6042. **2022**, PP 5-6, https://doi.org/10.3390/app12126042

[9] Mihai APOSTOL et al**, Malicious Strategy: Watering Hole Attacks**, Romanian Cyber Security Journal, V4, N:1, 2022,P30.

[10] Hussein Falah Aboalhab & Mohamed Farhat. 2024 **; Social Engineering and Its Role in Maintaining Information Security And Privacy,** IAR Journal Medical Case Reports, V5 I2; P5.

[11] Kofi Sarpong Adu-Manu et al **, Phishing Attacks in Social Engineering: A Review,** Journal of Cyber security**,** V4, N:4, 2023,P 244.

[12] Wang, Z.; Zhu, H.; Sun, L. **Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods**, IEEE Access, 9,2021, pp 11903-11904.

[13] Wang, Zuoguang & Zhu, Hongsong & Sun, Limin. (2021). **Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods**. IEEE Access. 9. 11895-11910. 10.1109/ACCESS.2021.3051633.

[14] Siddiqi, Murtaza & Pak, Wooguil & Siddiqi, Moquddam. (2022). **A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures**. Applied Sciences. 12. 10.3390/app12126042.

[15] https://www.almayadeen.net/investigation/%D8%A7%D9%84%D9%88%D8%B9%D9%8A-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A-%D9%81%D9%8A-%D8%B2%D9%85%D9%86-%D8%AB%D9%88%D8%B1%D8%A9-

%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA

12:30 2025/05/03

[16] عبد الهادي، محمد فتحي، **مجتمع المعلومات بين النظرية والتطبيق**، الدار المصرية اللبنانية، القاهرة ، 2006، ص 21

[17] أحمد نور ، بدر ، **محو الأمية المعلوماتية والدخول إلى القرن الواحد والعشرين** ،مجلة الاتجاهات الحديثة في المكتبات المعلومات، مج03 ، 1996، 5م،ص 36

[18] محمد ،مها أحمد إبراهيم ، **الوعي المعلوماتي ضرورة ملحة في القرن الحادي والعشرين: دراسة نظرية واطلالة على الإنتاج الفكري العربي والاجنبي**، بحوث ودراسات في علم المكتبات والمعلومات: دورة محكمة نص سنوية، ع04، 2010 ، ص19-20

[19] العربي ، أحمد عبادة ،بدرية محمد بسيوني، مراجعة: حسن عواد السريحي**: المعايير الموحدة للوعي المعلوماتي: مبادئ توجيهية للمكتبات العامة والمدرسية والجامعية العربية**، مكتبة الملك فهد الوطنية، جدة، 2013، ص40-48