مداخلة ضمن المحور الخامس

بعنوان: الهندسة الاجتماعية بين أساليب الاختراق وآليات التصدي

Title: Social engineering: hacking methods and countermeasures

كريم هندي *

جامعة غرداية، الجزائر

hendi.karim@univ-ghardaia.edu.dz

****

ملخص:

تهدف الدراسة إلى إبراز مخاطر اختراقات الهندسة الاجتماعية على الأفراد والمؤسسات حيث أصبحت الهندسة الاجتماعية أساس العديد من التهديدات الإلكترونية، بدءًا من رسائل التصيد الاحتيالي عبر البريد الإلكتروني ووصولًا إلى هجمات التصيد الاحتيالي عبر الرسائل النصية القصيرة والتصيد الصوتي. قمنا من خلال هذه الدراسة بعرض جملة من تقنيات اختراقات الهندسة الاجتماعية الشائعة مع تقديم بعض الأمثلة الواقعية، كما تم التطرق إلى آليات التصدي لهجمات الهندسة الاجتماعية للحد من تأثيرها السلبي على الأفراد والمؤسسات، وخلصنا إلى أن هذه الاختراقات تعتمد أساسا على عنصر الثقة من خلال دراسة سلوكيات الأفراد ورغباتهم، وتنتهج أسلوب التصيد والتحايل بالدرجة الأولى، كما يتوسع تأثيرها حتى على المؤسسات من خلال استغلال الضعف البشري أو المعرفي للمستخدمين لغياب الوعي أو عدم القيام باختبارات الاختراق داخل المؤسسة.

الكلمات المفتاحية: هندسة اجتماعية، اختراق، أمن سيبراني، التصيد الاحتيالي.

Abstract:

The study aims to highlight the risks of social engineering breaches to individuals and organizations, as social engineering has become the basis of many cyber threats, ranging from email phishing messages to sms phishing and voice phishing attacks. Through this study, we presented a set of common social engineering breach techniques with some real-world examples. We also discussed mechanisms to counter social engineering attacks to limit their negative impact on individuals and organizations. We concluded that

*المؤلف المرسل.

these breaches primarily rely on the element of trust by studying individuals' behaviors and desires, and they primarily employ phishing and deception. Their impact also extends to organizations by exploiting the human or cognitive weakness of users due to a lack of awareness or the absence of penetration testing within the organization.
Key words: Social engineering, hacking, cybersecurity, phishing.

1. مقدّمة:

مع ظهور ما يعرف بالثورات الرقمية في جميع مجالات الحياة وانتشار شبكات التواصل الاجتماعي باختلاف أنماطها من محادثات كتابية إلى صوتية ومرئية، فرضتها وسائل تكنولوجيا الاتصالات في شكل شبكة معلوماتية دولية سهلت واختصرت مسافات التواصل وتبادل المعلومات، حيث أضحت هذه الوسائل الحديثة في متناول أغلبية سكان العالم من حيث الاستخدامات والولوج إليها.

بالرغم من كل الإيجابيات التي تقدمها وسائل التواصل الحديثة إلا أنها تواجه مشكلة اقتحام خصوصية الأفراد والاستخدام السلبي لها، حيث أصبحت إمكانية الولوج واختراق البيانات والمعلومات المتعلقة بالآخرين سهلة وبسيطة جدا تمكن من استغلالها لأغراض شخصية كالابتزاز والمساومة للحصول على مقابل مادي أو لغرض تخريب البيانات أو بهدف التجسس وسحب أكبر قدر من معلومات قد توصف بالسرية والخطيرة، ويستعمل المخترقون أو ما يسمى بالمهاجمين تقنيات متطورة للاختراق تنطلق بداية من معرفة ودراسة توجهات الأفراد ورغباتهم ما أصبح يعرف حاليا بعلم الهندسة الاجتماعية، والتي تعنى أيضا بدراسة أساسيات برمجية وأكاديمية لمفاهيم الاختراق الإلكتروني واكتساب مهارة وفن وتقنيات لاختراق عقول البشر وجمع أكبر قدر من المعلومات عن الضحايا من أجل أغراض لا أخلاقية كالسرقة أو التشهير أو نشر الرذائل، والركيزة التي انطلقت منها هي اختراق الحلقة الأضعف في سلسلة أمن المعلومات وهي العنصر البشري، ولإتمام عملية البرمجة الذهنية اعتمدت الهندسة الاجتماعية على التعامل مع الغرائز البشرية التي تعتبر ثغرات موجودة في الطبيعة الإنسانية مثل الخوف والثقة والطمع والفضول والرغبة في المساعدة والانجذاب للأشخاص من خلال استعمال عدة أدوات أهمها شبكة الأنترنت، والرسائل الإلكترونية والمواقع المزيفة والشبكات الاجتماعية.

إشكالية البحث:

على ضوء ما سبق ذكره، فإن إشكالية دراستنا ترتكز حول التساؤل التالي:

ما هي أساليب اختراقات الهندسة الاجتماعية وآليات التصدي لها للحد من سلبياتها على الأفراد والمؤسسات؟

للإجابة على الإشكالية الرئيسية ارتأينا أن نضع جملة من التساؤلات الفرعية حتى نتمكن من الإلمام بجميع محاور الموضوع وتأتي صياغتها كما يلي:

- ما المقصود بالهندسة الاجتماعية واختراقاتها؟
- ما هي أساليب اختراقات الهندسة الاجتماعية؟
- ما هي آليات التصدي لاختراقات الهندسة الاجتماعية؟

فرضيات البحث:

بناء على الاشكالية الرئيسية للبحث وللإجابة على التساؤلات الفرعية، كان لزاما علينا ابتداء عرض جملة من الفرضيات التي ستمكننا من الوصول إلى نتائج الدراسة، وهي كالتالي:

- يعتمد مهاجمو الهندسة الاجتماعية على طرق وأساليب مشتركة في اختراقاتهم لبيانات الأفراد والمؤسسات.
- يحاول مهاجمو الهندسة الاجتماعية بشكل مستمر ودوري من استحداث أساليب متطورة للاختراق تتماشى مع التطورات الحاصلة في آليات وتقنيات حماية بيانات الأفراد والمؤسسات.
- تطورت آليات التصدي ومحاربة اختراقات الهندسة الاجتماعية مع تطور الأساليب التي يعتمدها المهاجمين والمخترقين لبلوغ أهدافهم اللاأخلاقية.

أهداف البحث:

يهدف هذا البحث إلى دراسة خطورة اختراقات الهندسة الاجتماعية التي تعتمد على دراسة سلوكيات الأفراد ورغباتهم لاستمالتهم واختراق خصوصياتهم عبر وسائل الكترونية للتواصل، كما تهدف إلى دراسة خطورة ذلك أيضا على المؤسسات عن طريق استغلال معلومات يقدمها المستخدمين بقصد أو بغير قصد، ونبحث من خلال هذه الورقة البحثية أيضا تسليط الضوء على أهم الآليات والتقنيات التي تمكن من التصدي لاختراقات الهندسة الاجتماعية والحد من سلبياتها على الأفراد والمؤسسات.

. **منهج البحث:**

للإجابة على إشكالية الدراسة، قمنا باستخدام المناهج المعتمدة في الدراسات الاقتصادية عموما، وعليه نعتمد على المنهج الوصفي في كل محاور الدراسة، كما نتخذ من التحليل منهجا لتفسير الظاهرة الاقتصادية للإلمام بجميع جوانب موضوع اختراقات الهندسة الاجتماعية، بعرض جملة من المفاهيم المقدمة من وجهات نظر اقتصادية واجتماعية، ومحاولة الإلمام بالتقنيات والآليات المستعملة في هذا المجال، اعتمادا على المقالات والكتب والدراسات إلى جانب شبكة الإنترنت وبعض البحوث التي تناولت الموضوع.

1. مفاهيم حول الهندسة الاجتماعية، أسبابها ومراحلها

1.2. تعريف الهندسة الاجتماعية :

التعريف الأول: يعرفها الكاتب الأمريكي كرستوفر هادناجي على أنها "مجموعة من الأنماط والسلوكيات البشرية التي نمارسها بقصد أو دون قصد، والتي يستخدمها المختصون عامة في التسويق لإقناع الجمهور بمنتج بعينه والترويج لمؤسسات، كما تستخدم في عالم السياسة من أجل كسب تأييد الجماهير، كما يستخدمها الأطباء في بعض الأحيان لحث مرضاهم على اتباع نظام غذائي معين على سبيل المثال من أجل صحتهم". (It-pillars, 2025)

التعريف الثاني: الهندسة الاجتماعية هي فن اختراق عقول البشر وخداعهم بهدف الحصول على معلومات أو بيانات أو أموال كانت ستظل خاصة وآمنة ولا يمكن الوصول إليها، كما اعتمدت الهندسة الاجتماعية على التعامل مع الغرائز البشرية التي تعتبر ثغرات موجودة في الطبيعة الإنسانية مثل الخوف والثقة والطمع والفضول والرغبة في المساعدة والانجذاب للأشخاص المشابهين، وغيرها من خلال أساليب مختلفة أهمها الإنترنت، والرسائل الإلكترونية والمواقع المزيفة والشبكات الاجتماعية.(زمان، 2019، ص02)

التعريف الثالث: الهندسة الاجتماعية هي تقنية خطيرة تتطلب فهما عميقا للسلوك البشري وتشير إلى مجموعة من الأساليب التي تهدف إلى خداع الأفراد للحصول على معلومات سرية أو الوصول إلى أنظمة محمية تعتمد هذه الأساليب على استغلال الثقة البشرية. (Kumar & Singh 2019)

التعريف الرابع: الهندسة الاجتماعية هي فن التأثير على الأفراد من أجل الحصول على معلومات سرية مثل كلمات المرور والعناوين والتفاصيل المصرفية، إلخ. من خلال استغلال نقاط الضعف البشرية مثل المشاعر والثقة والعادات لكسب رضا الناس، بدلا من استخدام نقاط الضعف التكنولوجية، ويمكن أن تسبب ضرراً جسيماً للضحية. (عبد الرحمان محمد، 2024، ص 449)

من خلال التعاريف المفاهيم المقدمة يمكننا أن نستخلص مفهوما شاملا حول الهندسة الاجتماعية بأنها طريقة تستغل سلوكيات ورغبات الأفراد والمؤسسات من أجل وضعهم في حالة من الثقة والأريحية ومن ثم دفعهم إلى الكشف عن بياناتهم الشخصية والخاصة ومعلومات حساسة تؤدي إلى استغلالهم وابتزازهم أو استعمال تلك البيانات والمعلومات لأغراض لا أخلاقية.

2.2. أسباب اختراقات الهندسة الاجتماعية:

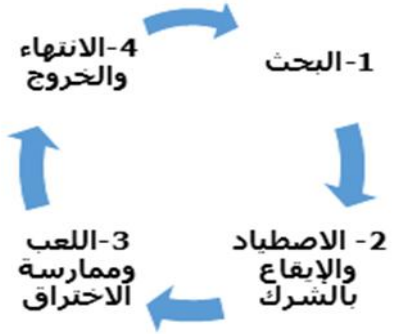
- هناك عدة أسباب تدفع المهاجمين والمخترقين إلى استعمال تقنيات وأساليب الهندسة الاجتماعية ليتمكنوا من ضحاياهم باستغلال ثقتهم وضعفهم البشري، من أهمها الانتشار الواسع للشبكة المعلوماتية وتوسع رقعة استخدامات الأنترنت ومواقع التواصل الاجتماعي بأنواعها، إلا أن الخبراء يحددون جملة من الأسباب الأخرى والمباشرة لاختراقات الهندسة الاجتماعية، من بينها: (زمان، 2019، ص05)

- الافتقار إلى وضع سياسات وقوانين تحمي الأنظمة المعلوماتية ومستخدميها.
- سهولة الوصول إلى المعلومة وخاصة مع انتشار الشبكات الاجتماعية ومحركات البحث.
- قلة أو ضعف التدريب في المجال الأمني للمعلومات .
- عدم توفر المعدات الأمنية والتقنية التي تمنع من وقوع الاختراق.
- سهولة اكتساب المهاجم لمهارات الاختراق، فهي تقنيات غير مكلفة.
- كتمان الضحايا للاختراقات والسرقات التي تعرضوا إليها خوفا من الفضيحة أو اللوم.
- عدم إدراك أهمية الاختراق ومدى خطورته.
- صعوبة الكشف عن اختراقات الهندسة الاجتماعية وتتبع أثرها.

3.2. مراحل اختراقات الهندسة الاجتماعية:

تمر اختراقات الهندسة الاجتماعية على أربع مراحل، يمكننا توضيحها في الشكل البياني التالي:

الشكل 01: مراحل هجوم الهندسة الاجتماعية



المصدر: ياسر قلعه جي، اختراقات الهندسة الاجتماعية واختباراتها، مجلة المعلوماتية، الجمعية العلمية السورية للمعلوماتية، العدد 155، أكتوبر 2020، ص 02.

1.3.2. مرحلة البحث: وهي المرحلة التمهيدية لتنفيذ الهجمة وتنطلق بداية من خلال:

- **تحديد الضحية:** يشرع المخترق في البداية في جمع المعلومات الكافية حول الضحية من مختلف المصادر، أهمها المواقع الالكترونية ومواقع التواصل الاجتماعي أو من البيانات والتقارير الموجودة على مستوى المؤسسة التي تنتمي إليها الضحية أو تربطها بها علاقة، أو حتى من سلة المهملات بالمؤسسة.
- **اختيار وسيلة الهجوم:** بعد تحديد هوية الضحية وجمع المعلومات الكافية، يتم اختيار وسيلة للهجوم تتناسب مع طبيعة وشخصية واحتياجات الضحية.

2.3.2. مرحلة الإيقاع بالشرك: من مميزات المخترق الاجتماعي والمهاجم القدرة على الاقناع والتلاعب والمناورة والثبات في الشخصية، ويشرع للإيقاع بالضحية من خلال منهجية تعتمد على جملة من الخطوات وهي:

- البدء بالتواصل لخداع الضحية وإيجاد منفذ للاختراق.
- مشاركة الضحية.
- اختلاق قصة.
- السيطرة على أحداث التفاعل مع الضحية.

3.3.2. مرحلة اللعب: تعتمد هذه المرحلة على الخطوات التالية:

- توسيع الفجوة ومنفذ الاختراق قدر الإمكان.
- تنفيذ الهجوم.
- تعطيل الأعمال وسحب البيانات.

4.3.2. مرحلة الانتهاء والخروج:

بعد الانتهاء من الاختراق ينهي المهاجم الاتصال بالضحية بشكل مباشر، وينسحب من مكان الهجوم خروجًا آمنا يضع الضحية في أريحية دون شكوك؛ وذلك بعد بمحو كل آثار البرامج المستعملة التي شكلت ضرارا للضحية ليقوم المهاجم بإعادة الوضع كما كان في البداية. (ياسر،2025، ص02)

3. أساليب اختراقات الهندسة الاجتماعية:

تعتمد الاختراقات والهجمات المتعلقة بالهندسة الاجتماعية على جملة من التقنيات والأساليب يتشارك فيها أغلبهم، فهناك من يقوم بالاختراق من منطلق التفاعل المباشر مع الضحية، وهناك من

يستعمل تقنيات الحاسوب لاختراق البيانات، نحاول فيما يلي ذكر أهم أساليب اختراقات الهندسة الاجتماعية:

1.3. اختراقات الهندسة الاجتماعية القائمة على العنصر البشري: هنا يتم التفاعل مع الضحية مباشرة، وفيما يلي بعض أنواع تقنيات الاختراق:

- **انتحال الهوية:** في هذا النوع من الهجوم، يتظاهر المهندس الاجتماعي (المهاجم) بأنه موظف في الشركة، فيرتدي بدلة ويحمل بطاقة هوية مزوَّرة للشركة. وبمجرد دخوله المبنى يمكنه الحصول على معلومات مهمة.
- **التنصت:** هو الاستماع غير المصرح به للتواصل بين شخصين أو قراءة الرسائل الخاصة. يمكن تنفيذه باستعمال قنوات الاتصال مثل خطوط الهاتف والبريد الإلكتروني.
- **الهندسة الاجتماعية العكسية:** يختلق المهاجم شخصية ذات سلطة، مدير تنفيذي مثلًا، ويطلب المعلومات التي يريدها. تحدث الهجمات الهندسية العكسية عادة في مجالات التسويق والدعم الفني. وهذه الهجمات صعبة التنفيذ لأنها تحتاج إلى تحضير مسبق وجمع معلومات كثيرة.
- **البحث في القمامة:** الغرض من البحث في سلال المهملات هو الحصول على معلومات مكتوبة على قطع من الورق أو مطبوعات الحاسوب. غالبًا ما يجد المتسلل كلمات مرور أو أسماء ملفات أو أجزاء أخرى من التقارير الفنية والمالية والمعلومات السرية في القمامة.
- **التظاهر بأنه مستعمل شرعي:** يتقمص المهاجم هوية مستعمل شرعي ويحاول الحصول على المعلومات، كأن يتصل بمكتب المساعدة ويقول: "مرحبا، أنا عمر من قسم التصميم ولا أتذكر كلمة مرور حسابي، فهل يمكنكم مساعدتي؟" ويمكن تنفيذ هذا النوع من الاختراق بالهاتف عن طريق التصيد الاحتيالي (vishing) الصوتي أو برسائل نصية.
- **الضغط والحل:** يقوم المهاجم بممارسة الضغط على الضحية وخلق حالة عاطفية سلبية كالترهيب أو الغضب أو السخط والصدم، ثم يقدّم المهاجم حلًّا للضحية من شأنه أن يخفف أو يزيل وطأة هذا الضغط. بالطبع يساعد هذا الحل المهاجم على تحقيق هدفه. يوضح المثالان التاليان كيف يمكن استعمال هذه التقنية.

2.3. اختراقات الهندسة الاجتماعية القائمة على الحاسوب: وهي الهجمات التي تنفَّذ بمساعدة برامج الحاسوب للحصول على المعلومات. نذكر فيما يلي بعض أنواع الهجمات:

- **النوافذ المنبثقة:** تخدع النوافذ المنبثقة المستعملين للنقر فوق ارتباط تشعبي يعيد توجيههم لزيارة صفحة الويب الخاصة بالمهاجم، ويطلب منهم معلوماتهم الشخصية أو تنزيل برنامج لها مرفقات فيروسات تعمل في الخلفية.
- **الهجوم من الداخل:** ينفذ هذا الهجوم من داخل الشبكة المستهدفة، ومعظمها ينفِّذها موظفون ساخطون غير راضين عن مناصبهم أو بسبب ضغينة على موظف آخر أو على الإدارة، وهي هجمات خطرة لأن لدى المهاجم معلومات كثيرة عن الضحية.
- **التصيد الاحتيالي:** غالبا ما يقوم مرسلو البريد العشوائي بإرسال كمية كبيرة من الرسائل إلى حسابات البريد الإلكتروني، على سبيل المثال:

✓ رسائل يدعي فيها المهاجمون أنهم من قسم شركة معينة ويبلغون الضحية أنه ربح جائزة، ويطلبون منه النقر على ارتباط في البريد الإلكتروني لتقديم تفاصيل بطاقة الائتمان الخاصة به أو إدخال معلومات شخصية.

✓ رسائل تزعم أنها من بنك يريد من زبائنه تأكيد معلومات الأمان الخاصة بهم، ومن ثم توجيههم إلى موقع مزيف يتم فيه تسجيل بيانات اعتماد تسجيل دخولهم.

- **التصيد الاحتيالي الموجَّه:** يستهدف "التصيّد الاحتيالي الموجه" شخصا واحدا داخل الشركة ويرسل بريدا إلكترونيا يزعم أنه يأتي من مسؤول تنفيذي رفيع المستوى في الشركة يطلب معلومات سرية.
- قد يرسل "صديق" مقطع فيديو "لا تفوّت مشاهدته"، يرتبط ببرنامج ضار أو بفيروس حصان طروادة يسجل ضغطات لوحة المفاتيح.
- **هجوم الهندسة الاجتماعية برسالة نصية مزيفة:** يرسل المهاجم رسالة نصية قصيرة إلى الهدف مدّعيا أنه من إدارة الأمن في البنك الذي يتعامل معه، ويدّعي أيضا أنه من الضروري أن يتصل الهدف برقم محدد. وعند اتصال الضحية بهذا الرقم يحصل المهاجم على المعلومات المطلوبة.
- **قرص التخزين المصيدة:** من الممكن مثلا وضع قرص تخزين محمول يحوي أدوات وبرمجيات خبيثة (صور، برمجيات، أفلام فيديو، روابط لمواقع يديرها المهاجم) على الأرض أمام منزل الضحية أو أمام مكتبه أو سيارته، وعندما يجدها الضحية سيفتحها بدافع الفضول، وقد يشغل بعض محتوياتها وهنا تقع الكارثة. (ياسر،2025، ص04)

4.آليات التصدي لاختراقات الهندسة الاجتماعية:

التصدي لاختراقات الهندسة الاجتماعية يتطلب معرفة مسبقة بخصوصيات وأنواع الاختراقات التي يمارسها المهاجمين، وتوجد العديد من الآليات والتقنيات المساعدة على ذلك بالرغم

من صعوبة الكشف عن هذه الهجمات، بسبب القدرات الكبيرة والاحترافية في التحايل التي يتميز بها مخترقو الهندسة الاجتماعية.

1.4. طرق الحد من الاختراقات بالنسبة للمؤسسات: تتعرض الكثير من المؤسسات لمحاولات الاختراق لبياناتها أو استغلال مستخدميها لجمع المعلومات لاستعمالها في عمليات الابتزاز عن طريق التصيد الاحتيالي أو باستخدام أساليب أخرى للهندسة الاجتماعية، لهذا نحاول عرض جملة من الإجراءات والآليات التي تعتمدها المؤسسات لمجابهة خطر الهندسة الاجتماعية والحماية من هجمات التصيد الاحتيالي عبر البريد الإلكتروني وتعزيز الوعي بالأمن السيبراني، نحصرها فيما يلي:

- **التثقيف:** يتم من خلال استخدام التدريب على التوعية الأمنية للتثقيف وكسب المعارف وتغيير السلوك داخل المؤسسات، ويجب وضع سياسة أمن معلومات للشركة وإلزام الموظفين التقيد بها.
- **المراقبة:** تتم المراقبة عن طريق استخدم أدوات محاكاة التصيد الاحتيالي لمراقبة معارف الموظفين وتحديد الأشخاص الأكثر عرضة لخطر تلقي أو الاستجابة لهجوم تصيد احتيالي في المؤسسة.
- **التواصل:** لإحداث التواصل داخل المؤسسة فإنه من الضروري الحفاظ على الاتصالات المستمرة وإطلاق حملات توعية حول رسائل التصيد الاحتيالي عبر البريد الإلكتروني، والهندسة الاجتماعية، والأمن السيبراني.
- **الدمج:** من الضروري أن تدرج المؤسسات ضمن سياساتها الداخلية وثقافتها كجزء لا يتجزأ منها حملات توعوية وتحسيسية لفائدة مستخدميها في إطار تعزيز المعارف والمكتسبات حول الأمن السيبراني، والتدريب على طرق محاربة الهجمات السيبرانية، مع المرافقة والدعم والتثقيف في ذلك.
- **التطبيق:** يجب حث المستخدمين بشكل دوري وإلزامهم بتطبيق معارفهم على أرض الواقع حول هجمات التصيد السيبراني عبر البريد الإلكتروني على أنشطتهم اليومية. ليتمكنوا من حصر كل المخاطر والتعامل معها وإعطاء وقت كافي لتقييم رسائلهم عبر البريد الإلكتروني، والرسائل النصية، والمواقع الإلكترونية.

1.4. طرق الحد من الاختراقات بالنسبة للأفراد:

نحاول فيما يلي عرض بعض الطرق الناجعة للتصدي لاختراقات الهندسة الاجتماعية التي تهدد الأفراد وتكسر حاجز السرية على بياناتهم:

- ✓ عدم فتح مرفقات البريد الوارد من مصادر مجهولة.
- ✓ يجب استعمال مصادقة متعددة التحقق.
- ✓ الحذر من العروض المغرية.
- ✓ التحقق من المصدر بعدم الثقة بالاتصالات الواردة، وأخذ الوقت الكافي للتقصي عنها في حال الشك. أما في حال تتبع الروابط أو المواقع الانتحالية فيكفي تمرير الفأرة فوق الرابط ليعطيك الرابط الفعلي في شريط معلومات المستعرض.
- ✓ ضرورة طلب الهوية وعدم السماح بالدخول للبيانات لأي شخص دون هوية أو إذن.
- ✓ مناقشة واقعية الطرح، وعدم تصديق محتوى الرسائل والقصص غير العقلانية بسبب الطمع الزائد، فليس معقولا أن يطلب شخص فائق الثراء في بلد ما المساعدة بمبلغ بسيط من شخص في دولة أخرى، بدعوى رد الجميل بمبالغ مضاعفة فور حله لمشكلته أو استرداد سلطته المزعومة.
- ✓ الحرص على عدم استعمال كلمة المرور نفسها لحسابات أخرى مختلفة.
- ✓ يجب وضع كلمة مرور محمية لتشغيل شاشة التوقف للمكتب.
- ✓ يجب تحديث برنامج مكافحة البرامج الضارة.
- ✓ ضرورة تأمين البيانات بصفة دورية.
- ✓ ضرورة البقاء على اطلاع حول المخاطر والأساليب الجديدة في اختراقات الهندسة الاجتماعية.
- ✓ ضرورة بالمشاركة في دورات للتدريب والتأهيل وحضور ندوات والاستفادة من المنشورات الإعلامية تعرف بمخاطر الهندسة الاجتماعية وآليات الوقاية منها والحفاظ على البيانات الشخصية. (Hadnagy C, 2018)

خاتمة:

نستنتج مما سبق أن هجمات الهندسة الاجتماعية خطرة جدًّا، ولها عواقب وخيمة ومدمرة على الأفراد والمؤسسات، فبالنسبة للمؤسسات فهي ملزمة بإجراء اختبارات اختراق الهندسة الاجتماعية لتقييم الوضع الأمني واكتشاف الحلقات الضعيفة داخليا، يمكن أن يُجري هذه الاختبارات فريقٌ داخلي أو مؤسسة خارجية متخصصة في اختبار الاختراق. يوفر فريق الاختبار

الداخلي المال، ولكنه قد يقدم رأيًا متحيزًا، أما الشركات الخارجية فتقدِّم رأيًا غير متحيز ولكنها أكثر تكلفة.

يمكننا القول ختاما أن الهندسة الاجتماعية تعد تهديدًا خطيرًا يستهدف الناس والمؤسسات على حد سواء. يجب أن يكون لدى الجميع وعي شامل وتدابير أمنية قوية للتصدي لهذا النوع من الهجمات. فهم مفهوم الهندسة الاجتماعية وتعلم تقنيات الوقاية والتصدي لها يمكن أن يلعب دورا حاسما في حمايتنا وحماية معلوماتنا الشخصية والحساسة، كما يعد تثبيت مجموعة الأمن المعلوماتي الكاملة أمرا إلزاميا وإجباريا وذلك بمجرد القيام بأي نوع من النشاطات على شبكة الإنترنت، وبالإضافة إلى ذلك، من المهم أن يقوم الأفراد بتحيين معلوماتهم حول آخر المستجدات عن التهديدات وحيل وخدع الهندسة الاجتماعية ومعرفة ما يمكن للمخترقين الوصول إليه في الوقت الحالي، لأن هذا ما يعطي الأسبقية والافضلية لتجنب الوقوع كضحية لهذا النوع من الهجمات على الإنترنت، مع ضرورة الحرص على الخصوصية وعدم نشر معلومات خاصة تجنبا لانتحال الشخصية.

قائمة المراجع:

1. الموقع الالكتروني لمؤسسة دعائم التقنية للحاسب الآلي www.lt-pillars.com -ماهي الهندسة الاجتماعية طرقها وكيفية تجنبها، تاريخ التصفح 2025/04/23 على الساعة 22:30.
2. صفاء زمان، الهندسة الاجتماعية social engineering، مجلة إضاءات، معهد الدراسات المصرفية الكويت، السلسلة 11 العدد 04، مارس 2019.
3. Kumar R., & Singh P, Phishing: A Survey of Techniques and Countermeasures. International Journal of Computer Applications Kali Linux Social Engineering, Rahul Singh Patel, 2019.
4. عبد الرحمان محمد عبد الظاهر محمد، فعالية برنامج في طريق العمل مع الجماعات وتوعية الشباب الجامعي بمخاطر الهندسة الاجتماعية في ضوء رؤية مصر 2030، مجلة دراسات في الخدمة الاجتماعية، العدد 65 الجزء الثاني، جمهورية مصر العربية، يناير 2024.
5. ياسر قلعه جي، اختراقات الهندسة الاجتماعية واختباراتها، مجلة المعلوماتية، الجمعية العلمية السورية للمعلوماتية، العدد 155، أكتوبر 2020.
6. Hadnagy, C, Social Engineering: The Science of Human Hacking. Wiley, 2018.
7. https://www.kaspersky.com : طرق تجنب هجمات الهندسة الاجتماعية
8. https://en.wikipedia.org/wiki/Social_engineering_(security