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:

أهمية التوعية والتدريب في تقليل من قابلية الأفراد والمجتمع للتعرض لهجمات الهندسة الاجتماعية

من إعداد الباحثين :

- سايح عبد الله، أستاذ محاضر أ، جامعة غرداية، sayah.abdallah@univ-ghardaia.edu.dz
- دحو سليمان، أستاذ ، جامعة غرداية، dahou.slimane@univ-ghardaia.edu.dz

من خلال المحور رقم: 05

الملخص:

تهدف هده المداخلة الى تسليط الضوء على أهمية التدريب ونشر الوعي لأهمية مواجهة تداعيات ومخاطر الهندسة الاجتماعية من خلال جوانب وطرق تقليدية وأخرى حديثة مبنية على الواقع الافتراضي والنمادج الحديثة وتبيان ايجيابات وسلبيات مل من الطريقيتين.

أيضا تسليط الضوء على جانب الامن المجتمعي المبني على الوعي بمخاطر الهندسة الاجتماعية بكل أنواعها واشكالها، خاصة بعد تعميم استعمال المنصات سواء الترفيهية او الانتاجية والخدمية

الكلمات المفتاحية: هندسة اجتماعية، تدريب، وعي رقمي، احتيال، امن مجتمعي

Abstract:

This intervention aims to highlight the importance of training and raising awareness of the importance of confronting the repercussions and risks of social engineering through traditional and modern approaches based on virtual reality and modern models, and to highlight the pros and cons of each approach. It also highlights the aspect of community security based on awareness of the risks of social engineering in all its forms and types, especially with the widespread use of platforms, whether for entertainment, production, or services.

Keywords: Social engineering, training, digital awareness, fraud, community security

مقدمة

تُعد المخاطر الناجمة عن الهندسة الاجتماعية واحدة من أبرز التهديدات للأمن السيبراني، حيث أن العامل البشري يُمثل الحلقة الأضعف في منظومة الحماية الأمنية، تتناول هذه الدراسة أثر التوعية والتدريب في مواجهة هذه المخاطر وتقديم استراتيجيات فعّالة لتعزيز الأمن المجتمعي، يُستند البحث في ذلك إلى مجموعة من الدراسات والأبحاث التي تناولت موضوعات متنوعة منها آليات التلاعب الاجتماعي، وتطوير برامج تعليمية مستندة إلى أساليب مبتكرة مثل الألعاب التعليمية، بالإضافة إلى تطبيقات عملية في مؤسسات حيوية مثل البنى التحتية الحرجة والقطاعات الصحية.

حيث تهدف هذه المداخلة إلى استعراض الأدلة البحثية والأمثلة العملية التي تؤكد أهمية التوعية والتدريب المستمر في تقليل قابلية الأفراد والمجتمعات للتعرض لهجمات الهندسة الاجتماعية، كما توضح كيف يمكن للإعلام والوسائل التقنية أن يكونا جسورًا لتعزيز الوعي الأمني وتوفير بيئة عمل ومجتمع أكثر أماناً.

وتطرح هنا الإشكالية الرئيسية وهي هل يهم الوعي والتدريب المستمر في التقليل من مخاطر الهندسة الاجتماعية؟

1.تعريف الهندسة الاجتماعية:

الهندسة الاجتماعية (Social Engineering) هي مجموعة من التقنيات والأساليب التي يستخدمها المهاجمون للتأثير على الأشخاص وحملهم على اتخاذ إجراءات معينة أو الكشف عن معلومات حساسة أو منحهم حق الوصول إلى أنظمة أو مواقع أو بيانات محمية. بدلاً من استغلال نقاط ضعف تقنية في الأنظمة، تركز الهندسة الاجتماعية على استغلال نقاط الضعف البشرية مثل الثقة، والخوف، والفضول، والرغبة في المساعدة.

ببساطة، هي **فن اختراق العقول بدلاً من اختراق الأجهزة.**

2. أنواع الهندسة الاجتماعية:

تتنوع أساليب الهندسة الاجتماعية بشكل كبير وتتطور باستمرار، ولكن يمكن تصنيفها إلى عدة أنواع رئيسية بناءً على الطريقة المستخدمة للتأثير على الضحية:

1. التصيد الاحتيالي:(Phishing) (العتيبي et al., 2020)

- **الوصف :**إرسال رسائل بريد إلكتروني أو رسائل نصية قصيرة (SMS/Smishing) أو رسائل عبر تطبيقات التواصل الاجتماعي تبدو وكأنها واردة من جهات موثوقة (مثل البنوك، الشركات، المؤسسات الحكومية). تهدف هذه الرسائل إلى خداع الضحايا وحملهم على النقر على روابط ضارة، أو إدخال معلومات شخصية حساسة (مثل كلمات المرور، أرقام بطاقات الائتمان)، أو تنزيل برامج ضارة.
- **الأنواع الفرعية:**

- ✓ **التصيد بالرمح :(Spear Phishing)** هجمات تصيد تستهدف أفرادًا أو مجموعات محددة داخل مؤسسة أو منظمة، وغالبًا ما تتضمن معلومات شخصية تجعل الرسالة تبدو أكثر مصداقية.
- ✓ **التصيد بالجرافين :(Whaling)** نوع من التصيد بالرمح يستهدف كبار المسؤولين التنفيذيين في الشركات.
- ✓ **التصيد الصوتي :(Vishing)** استخدام المكالمات الهاتفية لخداع الضحايا وحملهم على الكشف عن معلومات حساسة أو اتخاذ إجراءات معينة.
- ✓ **التصيد عبر الرسائل النصية القصيرة :(Smishing)** استخدام الرسائل النصية القصيرة لنفس أغراض التصيد الاحتيالي عبر البريد الإلكتروني.

2. الذريعة:(Pretexting)

وهو قيام المهاجم بإنشاء سيناريو وهمي أو قصة ملفقة (ذريعة) لكسب ثقة الضحية وحملها على الكشف عن معلومات أو القيام بأفعال معينة. قد ينتحل المهاجم شخصية موظف دعم فني، أو مسؤول في قسم الموارد البشرية، أو حتى زميل عمل.

- **المثال :**يتصل المهاجم بموظف في قسم تكنولوجيا المعلومات مدعيًا أنه فني دعم ويحتاج إلى كلمة المرور الخاصة بحساب معين لإصلاح مشكلة عاجلة.

3. الإغراء:(Baiting)

وهو ترك أجهزة أو وسائط تخزين مصابة مثل أقراصUSB في أماكن يسهل العثور عليها (مثل مواقف السيارات أو بالقرب من مكاتب العمل). عندما يقوم الضحية بتوصيل الجهاز بجهاز الكمبيوتر الخاص به، يتم تثبيت برامج ضارة تلقائيًا.

- **المثال :**العثور على قرص USB بعنوان "رواتب الموظفين" وتركه بالقرب من مكتب الموارد البشرية.

4. التتبع:(Tailgating/Piggybacking)

وهو دخول شخص غير مصرح له إلى منطقة محظورة عن طريق التتبع خلف شخص مصرح له بالدخول. يستغل المهاجم طيبة أو عدم انتباه الشخص المصرح له بالمرور عبر البوابات الأمنية أو الأبواب المقفلة.

المثال :المشي مباشرة خلف موظف يقوم بفتح باب باستخدام بطاقة الدخول دون أن يتم طلب إبراز هوية أو بطاقة دخول.

5. الهندسة الاجتماعية العكسية:(Reverse Social Engineering) (على إبراهيم أحمد et al., 2022)

في هذا النوع، يقوم المهاجم بتهيئة موقف يجعل الضحية تتصل به طلبًا للمساعدة. غالبًا ما يتضمن ذلك زرع مشكلة ظاهرية أو خلق حالة طارئة وهمية.

المثال :تعطيل نظام معين في الشركة بشكل غير ملحوظ، ثم الانتظار حتى يتصل الموظفون بقسم الدعم الفني (الذي ينتحله المهاجم) لطلب المساعدة، مما يمنح المهاجم فرصة لجمع المعلومات أو الوصول إلى الأنظمة.

6. التطفل:(Eavesdropping)

محاولة الحصول على معلومات حساسة عن طريق الاستماع إلى المحادثات أو مراقبة الاتصالات دون علم الأطراف المعنية. يمكن أن يحدث ذلك عبر التنصت على المكالمات الهاتفية أو قراءة رسائل البريد الإلكتروني أو حتى مراقبة ما يكتبه شخص ما على لوحة المفاتيح.

7. الاستمالة:(Preying/Elicitation)

بناء علاقة ثقة مع الضحية ببطء بهدف الحصول على معلومات حساسة أو استغلالها لاحقًا، قد يتظاهر المهاجم بأنه صديق أو زميل أو شخص لديه اهتمامات مشتركة.

8. التهديد المباشر:(Quid Pro Quo)

تقديم خدمة أو هدية أو منفعة مقابل الحصول على معلومات أو القيام بفعل معين.

المثال :الاتصال بموظفين وتقديم "دعم فني مجاني" مقابل الحصول على بيانات تسجيل الدخول الخاصة بهم.

9.أهمية فهم الهندسة الاجتماعية:(سليمان, 2022)

فهم أساليب الهندسة الاجتماعية أمر بالغ الأهمية للأفراد والمؤسسات على حد سواء. يمكن أن تؤدي الهجمات الناجحة للهندسة الاجتماعية إلى:

- سرقة معلومات شخصية ومالية.
- اختراق الحسابات والأنظمة.
- نشر البرامج الضارة.
- فقدان البيانات الهامة.
- الإضرار بالسمعة.
- خسائر مالية كبيرة.

من خلال الوعي بهذه الأساليب واتخاذ الاحتياطات اللازمة، يمكن تقليل خطر الوقوع ضحية لهجمات الهندسة الاجتماعية بشكل كبير. تتضمن هذه الاحتياطات التحقق من هوية المرسل، عدم

مشاركة معلومات حساسة عبر البريد الإلكتروني أو الهاتف، توخي الحذر عند النقر على الروابط أو تنزيل الملفات من مصادر غير موثوقة، وتدريب الموظفين على التعرف على هذه الهجمات وكيفية التعامل معها(Akçayır & Akçayır, 2017).

10. أهمية التوعية والتدريب في مواجهة مخاطر الهندسة الاجتماعية

لقد أثبتت الدراسات أن عوامل الخطر المرتبطة بسوء السلوك البشري يمكن الحد منها بشكل كبير عبر برامج توعية فعالةفي مجال الهندسة الاجتماعية ومن أبرز الحقائق المدعومة بالبيانات أن نسبة نجاح هجمات الهندسة الاجتماعية ترتبط ارتباطًا وثيقًا بمدى تدريب ووعي الأفراد على كيفية التعرف على هذه المحاولات ومن ثم اتخاذ الإجراءات الوقائية اللازمة للتصدي لهذه الهجمات.

تشير الدراسات والأدلة المادية إلى أن التكلفة المالية والأمنية الناجمة عن الهجمات الناجحة يمكن أن تقل بشكل ملحوظ إذا ما تم استثمار موارد كافية في تعليم وتطوير قدرات الموظفين في المؤسسات والشركات عبر برامج التوعية المستمرة، يُعتبر هذا أمراً محفزاً لصانعي السياسات في المؤسسات الحكومية والخاصة لاعتماد أساليب تعليمية مدمجة بين الوسائل التقنية والتدخّل البشري المباشر.

ومن ثم يطرح التساؤل الأساسي وهو كيف نقوم وماهي الأساليب التي يمكن استعمالها لزيادة الوعي بالهندسة الاجتماعية

11. أساليب التوعية والتدريب:

هنا يطرح أساليب وطرق متعددة ونستطيع تصنيفها لصنفين رئيسيين وهما الأساليب التقليدية والأساليب و النماذج المبتكرة

1.11 البرامج التدريبية التقليدية وأهميتها

لطالما اعتمدت المؤسسات على أساليب التدريب التقليدية مثل الدورات المعتمدة والمحاضرات التفاعلية لضمان إعداد الموظفين لمواجهة هجمات الهندسة الاجتماعية، تعتمد هذه الأساليب على منح المعرفة النظرية والعملية، وتعتمد في كثير من الأحيان على مديرين ذوي خبرة لضمان فهم الموظفين لأساسيات الأمن السيبراني ومخاطر الهندسة الاجتماعية، ومع ذلك فقد تبين أن هذه الأساليب تواجه بعض القيود مثل محدودية التفاعل ونقص التحديث المستمر للمحتوى التعليمي وربما حتى الملل والتذمر من كثرة الدورات لأن التحديثات العملية دورية ومتقاربة.

11. 2. الأساليب المبتكرة والتدريب عبر الألعاب

انتقلت بعض المؤسسات إلى تبني أساليب مبتكرة للتدريب مثل استخدام ألعاب الحاسوب والأساليب التفاعلية المبنية على المحاكاة والسيناريوهات الواقعية، تُظهر الدراسة تحت عنوان "Game Based Cyber Security Training: are Serious Games suitable for cyber security training?" أن الأساليب المبنية على الألعاب التعليمية أدت إلى تحسين نسب التوعية لدى المشاركين وساعدت في رفع مستوى رد الفعل الصحيح تجاه هجمات الهندسة الاجتماعيةبشكطل ملحوظ مقارنة بنظرائهم الذين تلقوا التدريب التقليدي.

على سبيل المثال، لعبة "Anti Phishing Phil" تعتبر نموذجًا جيدًا لتدريب الأفراد على التمييز بين الرسائل الاحتيالية والرسائل الشرعية، إضافة إلى لعبة "Cyber CIEGE" التي أثبتت جدواها في تجسيد مواقف عملية تتيح للمستخدمين تجربة سيناريوهات الأمن السيبراني بشكل تفاعلي، تُظهر هذه الطرق فعالية كبيرة خاصةً مع دمجها في منهجيات التدريب المستمرة التي تأخذ بعين الاعتبار التغيرات السريعة في تقنيات الهجمات.

11. 3.الدمج بين التدريب المعتمد على الكمبيوتر والتدريب العملي

يُعتبر الدمج بين التدريب المعتمد على الكمبيوتر والتدريب العملي الذي يُقدَّم من خلال جلسات موجهة من قبل خبراء الأمن السيبراني من الأنماط الناجحة في رفع مستوى الوعي الأمني في المؤسسات .يُتيح هذا النموذج للمشاركين الاطلاع على سيناريوهات حقيقية، كما يُوفر لهم فرصة التفاعل والتطبيق العملي للمعرفة المكتسبة في بيئة محاكاة تقترب من الواقع العملي للمؤسسات الحيوية مثل البنوك والمستشفيات.

يُبرز هذا النموذج أيضًا أهمية عناصر الدعم الفني وتحديث المحتوى بانتظام، إذ إن التحديث الدوري للمواد التدريبية يعد ضروريًا لمواكبة تطور تقنيات الهجمات وعددها المتزايد.

جدول مقارنة بين أساليب التدريب التقليدية والحديثة

نوع التدريب	المميزات	العيوب
التدريب التقليدي	محتوى نظري شامل، قابلية للتطبيق العملي المحدودة	نقص التفاعل والتحديث الدوري للمحتوى
التدريب القائم على الألعاب	تحفيز عالي وتفاعل المستخدمين، محاكاة سيناريوهات حية	الحاجة لمزيد من الاستثمار في التكنولوجيا

12. تعزيز ثقافة الأمن السيبراني في المؤسسات والمجتمع

تكتسب ثقافة الأمن السيبراني أهمية قصوى عند الحديث عن تقليل آثار مخاطر الهندسة الاجتماعية. يعتمد هذا الجانب على تبني نهج استراتيجي يشمل وضع سياسات وتشريعات داخلية قوية، إضافة إلى تعزيز المساءلة والمراقبة المستمرة.

12. 1.بناء المؤسسات الآمنة

يعتبر تطوير البنية المؤسسية لمكافحة الفساد وسوء الإدارة أحد الجوانب التي يجب تضمينها لخلق بيئة مؤسسية مقاومة للتلاعب والاستغلال ، تُظهر الدراسات أن بناء نظام قائم على مبدأ الحوكمة الرشيدة والشفافية يساعد في تقليل فرص استغلال العامل البشري وتعزيز الثقة داخل المؤسسة.

12. 2.التوعية عبر الحملات الإعلامية

يُعد الإعلام الأمني أداة فعّالة لتوعية الجمهور بمخاطر الهندسة الاجتماعية والتهديدات التي يُمكن أن تتعرض لها الشبكات المعلوماتية في الحياة اليومية، من خلال تنظيم ورش عمل وحملات توعوية مكثفة عبر وسائل الإعلام التقليدية والرقمية، يمكن تحقيق زيادة ملحوظة في وعي الجمهور وتخفيض نسب النجاح للهجمات الاحتيالية.

12. 3.دمج التكنولوجيا في تعزيز الأمن

يُمكن أن تُستخدم الأنظمة التكنولوجية المتطورة، مثل أنظمة تحليل البيانات الكبيرة ونظم الذكاء الاصطناعي، لمراقبة نشاطات المستخدمين بشكل فوري وتنبيههم عند حدوث أي نشاط مشبوه

تعتبر هذه الأدوات حاسمة في تنفيذ نهج متعدد الطبقات يهدف إلى سد الثغرات الأمنية التي قد تستغلها الهجمات القائمة على الهندسة الاجتماعية.

13. التقييم والمراقبة وتحديث البرامج التدريبية

يعتبر التقييم المستمر جانبًا أساسيًا لقياس مدى فاعلية برامج التوعية والتدريب في المؤسسات. يُستخدم هذا التقييم لتحليل الأداء وتحديد نقاط الضعف في المنهجيات الحالية.

13. 1.تقييم الأداء والاختبارات التمهيدية

يجب وضع نظام تقييم دوري يتضمن اختبارات قبل وبعد التدريب لقياس التحسن في معرفة المشاركين واستعدادهم للتصدي للهجمات السيبرانية .3يمكن أن يتم إعداد هذه الاختبارات باستخدام أساليب متعددة تشمل تقييمات قصيرة واختبارات محاكاة السيناريوهات الأمنية، والتي أثبتت فعاليتها في تعزيز قدرات الأفراد على اتخاذ القرارات الأمنية الصحيحة.

13. 2.تحليل البيانات واستخدام التغذية الراجعة

يجب تحليل النتائج المستخلصة من برامج التدريب بدقة باستخدام أدوات تحليل بيانات متقدمة، مما يتيح تحديد المستويات الفعلية للتوعية والتفاعل مع المواد التدريبية .تُعد التغذية الراجعة من المستخدمين أحد أهم المؤشرات التي تساعد في تعديل المحتوى وتحديثه باستمرار لتلبية المتطلبات المتغيرة للتهديدات الأمنية.

13. 3.تحديث البرامج وإعادة تصميم المحتوى

بناءً على نتائج التقييم، ينبغي أن تتخذ المؤسسات قرارات بإعادة تصميم وتحديث المواد التدريبية دورياً بحيث تواكب أحدث تقنيات وأساليب الهجمات السيبرانية، ويُعدّ دمج تقنيات التدريب التفاعلي مع المحتوى الرقمي حلاً مبتكرًا لضمان تحديث مستمر وملائم يلبي احتياجات المتدربين على اختلاف مستوياتهم.

14. التحديات والقيود والحلول المستقبلية

تواجه برامج التدريب على الأمن السيبراني تحديات عدة قد تُعيق تحقيق الأهداف المنشودة، من بينها القيود المالية والتحفظات المؤسسية وعدم كفاية ميكانيزمات القياس والتحديث.

14. 1.القيود المالية ونقص الميزانيات

يُعدّ نقص الميزانيات أحد أكبر التحديات التي تواجهها المؤسسات لتوفير التدريب اللازم ضد الهجمات الاحتيالية، في ظل الضغوط الاقتصادية، تكون ميزانيات التدريب غير كافية في العديد من الحالات، مما يؤدي إلى قصور في تقديم برامج توعية شاملة ومستمرة.

14. 2.المقاومة المؤسسية وثقافة عدم الأولوية

في بعض المؤسسات، قد يكون هناك مقاومة داخلية لتبني أساليب جديدة في التدريب بسبب التمسك بالطرق التقليدية أو عدم تقدير أهمية التوعية الأمنية بقدر كافٍ، يتطلب الأمر جهوداً منهجية لتغيير الثقافة التنظيمية وتشجيع الموظفين على المشاركة الفعالة في برامج التدريب.

14. 3.التحديات التقنية والتحديث المستمر للمواد

نظرًا للتغيرات السريعة في أساليب الهجمات السيبرانية واختراع تقنيات جديدة، فإن البرامج التدريبية تواجه تحديًا كبيرًا في مواكبة هذا التطور، يتطلب الأمر حلولاً تقنية تتضمن تحديث المحتوى بشكل دوري باستخدام تقنيات الذكاء الاصطناعي والتحليل الذكي للبيانات.

14. 4.الحلول المقترحة لمواجهة التحديات

لمواجهة التحديات والأساليب المبتكرة والمحدثة تقريبا بشكل يومي نقتح مجموعة من الحلول والإجراءات المتناسبة مع المخاطر المرتقبة ومن الحلول المقترحة:

- زيادة الحصص الميزانية المخصصة للتدريب عبر تحفيز الجهات الحكومية والمؤسسات الخاصة لدمج التوعية الأمنية ضمن الأولويات الاستراتيجية.
- اعتماد نماذج تدريبية هجينة تجمع بين التدريب التقليدي والتفاعلي باستخدام التقنيات الحديثة مثل الألعاب التعليمية والتدريب العملي المباشر.
- تطوير آليات تقييم مستمرة تعتمد على أحدث تقنيات التحليل والذكاء الاصطناعي لاستقبال التغذية الراجعة وتحديث المحتوى بشكل سريع وفعّال.
- تنظيم حملات توعوية شاملة بالتعاون مع وسائل الإعلام لتغطية شريحة واسعة من المجتمع وتعزيز الثقافة الأمنية لدى الأفراد.

15. دور الإعلام والوسائل التقنية في رفع مستوى الوعي

لا يقتصر جتنب التوعية على الجهات الرسمية والمؤسسات الحكومية وانما يتوسع ذلك ليصل الى المؤسسات الإعلامية والاشهارية على حد سواء حيث يلعب الإعلام دورًا محوريًا في نشر الوعي حول مخاطر الهندسة الاجتماعية، حيث تساهم الحملات الإعلامية في توعية الجمهور بخطورة هذه الهجمات وأهمية اتباع إجراءات السلامة، أو التقليل من الاخطار المترتبة على تلكم الهجمات.

1.15 الحملات الإعلامية والمنصات الرقمية

تُعتبر الحملات الإعلامية المشتركة بين الهيئات الحكومية والمؤسسات الخاصة من الركائز الأساسية لنشر الوعي الأمني، كما يُستخدم الإنترنت ووسائل التواصل الاجتماعي لنشر مقاطع فيديو تعليمية ونشرات توعوية توضح كيفية التصرف عند مواجهة هجمات الهندسة الاجتماعية، وتوضح أيضا كيفية تلافي الوقوع في فخاخ الاحتيال والهندسة المجتمعية خاصة في منصات التواصل ومنصات التوظيف والبيع والشراء الالكتروني

2.15 الوسائل التقنية والتطبيقات الذكية

توفر التطبيقات الذكية والأنظمة المدمجة حلولاً تقنية مبتكرة لمراقبة وتحليل سلوك المستخدمين وتنبيههم عند حدوث نشاط مشبوه، يمكن لهذه الأنظمة أن تعمل بالاشتراك مع برامج التدريب، حيث تُعرض للمستخدمين رسائل توعوية فورية لتذكيرهم بالإجراءات الوقائية عند استخدامهم للأجهزة.

15. 3.الشراكات بين القطاعين العام والخاص

يمكن تعزيز جهود التوعية من خلال شراكات استراتيجية بين القطاع الحكومي والشركات الخاصة المتخصصة في الأمن السيبراني، مما يتيح تبادل الخبرات وتطوير برامج تعليمية متكاملة تُغطي مختلف جوانب المخاطر الأمنية،

16. دراسات الحالة والأمثلة العملية

تعكس دراسات الحالة والأمثلة العملية فعالية أساليب التوعية والتدريب في مواجهة هجمات الهندسة الاجتماعية، حيث يُمكن استخلاص الدروس المستفادة من تجارب حقيقية، جرت وتم التعامل معها سواء في إحصاء حجم الاخطار او أساليب الوقاية والاحتراز

1.16 دراسة حالة: الهجمات على NHS وتأثير التدريب على الوقاية

أوضحت إحدى الدراسات أن هجومًا على خدمات الطوارئ في المملكة المتحدة كان بالإمكان تفاديه لو كانت هناك برامج تدريبية فعالة ومستدامة، يشير هذا المثال إلى أن تقديم التدريب العملي والمحاكاة الواقعية للمواقف الأمنية يمكن أن يحد من نسبة النجاح لهذه الهجمات.

2.16 دراسات حالة في القطاع المصرفي والقطاع الصحي

أظهرت بعض التقارير ارتفاع نسب الهجمات الاحتيالية بنسبة تزيد عن 667% خلال فترة جائحة كوفيد-19، مما يؤكد ضرورة تحديث وتكثيف برامج التوعية والتدريب لجميع العاملين في

القطاعين المصرفي والصحي، في هذا السياق، تعمل بعض المؤسسات على تطبيق نظم متقدمة تجمع بين التقييم الذاتي والدورات التدريبية المباشرة لتحقيق نمط متكامل للأمن السيبراني.

3.16 أمثلة تطبيقية في التدريب القائم على الألعاب

على غرار لعبة"Anti Phishing Phil" ، تُظهر نتائج التدريب القائم على المحاكاة التفاعلية أن المشاركين يصبحون أكثر قدرة على التعامل مع الانتهاكات الأمنية وتصنيفها بالشكل الصحيح ، يُظهر هذا المثال كيف يمكن ربط التفاعلات الرقمية بأساليب تعليمية مبتكرة تقلل من مخاطر التعرض للهجمات الاحتيالية.

17. إطار شامل لتعزيز الأمن المجتمعي

في سياق الحديث عن الامن المجتمعي والوقاية من الهندسة الاجتماعية يتطلب تحقيق الأمن المجتمعي في ظل التهديدات السيبرانية تبني إطار شامل يتكون من العناصر التالية:

1.17 السياسات والتشريعات

- وضع سياسات داخلية واضحة للدفاع عن البيانات وحماية الأصول الحيوية.
- تشجيع تبادل المعلومات بين الجهات الحكومية والخاصة لوضع معايير موحدة للتصدي للهجمات الاحتيالية.

2.17 البرامج التدريبية المتكاملة

- اعتماد برامج تدريبية هجينة تجمع بين المدخلات النظرية والعملية، بالإضافة إلى التدريب القائم على المحاكاة والألعاب التفاعلية.
- تحديث المحتوى التدريبي بشكل دوري اعتماداً على أحدث التقنيات وأساليب الهجمات.

3.17 الدعم التقني والمراقبة المستمرة

- استخدام أنظمة الذكاء الاصطناعي وأدوات تحليل البيانات لمراقبة سلوك المستخدمين والتعرف المبكر على أي نشاط مشبوه.
- توفير دعم فني متواصل وتحديث آليات الأمان لمواكبة التهديدات المتجددة.

4.17 التوعية العامة والإعلام

- تنظيم حملات إعلامية توعوية تشمل المؤتمرات والندوات والورش التدريبية التي تستهدف جميع فئات المجتمع، لا سيما الفئات الأكثر عرضة للهجمات الاحتيالية .
- استخدام وسائل الإعلام الرقمية والتطبيقات الذكية لنشر الرسائل التوعوية التي تساعد في تغيير سلوكيات المستخدمين.

جدول يوضح إطار عمل شامل لتعزيز الأمن المجتمعي

العنصر الرئيسي	الوصف
السياسات والتشريعات	وضع معايير وقوانين داخلية للتصدي للهجمات
البرامج التدريبية	برامج هجينة تجمع بين التدريب النظري والعملي
الدعم الفني والمراقبة	استخدام الذكاء الاصطناعي لتحليل سلوك المستخدم
التوعية العامة	حملات إعلامية وتوعوية تستهدف جميع فئات المجتمع

5.17 الشراكات والتعاون المؤسسي

- تعزيز التعاون بين القطاع الحكومي والمؤسسات الخاصة لتوحيد الجهود وتبادل الخبرات وتطوير برامج أمن سيبراني متكاملة.
- تنظيم ورش عمل مشتركة ودورات تدريبية تركز على تحقيق التكامل بين مختلف القطاعات الحيوية.

الخاتمة

تلخص هذه الدراسة الدور الحيوي للتوعية والتدريب في مواجهة مخاطر الهندسة الاجتماعية وتعزيز الأمن المجتمعي، من خلال استعراض عدة جوانب مهمة. وتشمل هذه الجوانب التأكيد على الأهمية القصوى لتطوير قدرات الأفراد والمؤسسات لمواجهة الهجمات السيبرانية من خلال برامج تدريبية محدثة ومتكاملة، بالإضافة إلى التمييز بين الأساليب التقليدية والحديثة في التدريب، مع الإشارة إلى فعالية الأساليب القائمة على الألعاب والمحاكاة العملية في تحسين مستوى الوعي. كما تُشدد على أهمية دمج الوسائل التقنية مع الفعاليات التوعوية والإعلامية لتعزيز ثقافة الأمن داخل المؤسسات والمجتمعات، وضرورة تقييم أداء برامج التدريب بشكل مستمر وتحديثها وفقًا لأحدث التهديدات والتقنيات لضمان جاهزية العاملين للاستجابة لأي محاولات احتيالية، كما تتناول الدراسة معالجة التحديات القائمة، مثل القيود المالية وثقافة عدم الأولوية، من خلال تبني استراتيجيات شاملة وإطار عمل مرن يوفر تدريبًا وتوعية متكاملة.

من بين التوصيات المهمة، تأتي ضرورة دمج الوسائل التقنية مع الفعاليات التوعوية والإعلامية لتعزيز ثقافة الأمن داخل المؤسسات والمجتمعات. بالإضافة إلى ذلك، يجب تقييم أداء برامج التدريب بشكل مستمر وتحديثها وفقًا لأحدث التهديدات والتقنيات، ضمان جاهزية العاملين لمواجهة أي محاولات احتيالية. كما شددت الدراسة على أهمية مواجهة التحديات مثل القيود المالية وثقافة عدم الأولوية، من خلال تبني استراتيجيات شاملة وإطار عمل مرن يوفر تدريبًا وتوعية متكاملة.

فيما يتعلق بالآفاق المستقبلية، توصي الدراسة بضرورة استثمار المزيد في تكنولوجيا التدريب الحديثة وتعزيز التعاون بين القطاعات المختلفة لتبادل الخبرات والأفضل ، كما تشير إلى أن تحديث برامج التدريب بشكل مستمر سيكون مفيدًا لمواكبة التهديدات الناشئة من الهندسة الاجتماعية، التي تتطور بسرعة في عالم رقمي متغير. أخيرًا، تُشدد على أهمية بناء ثقافة أمن شاملة في جميع المستويات، سواء في المنظمات أو المجتمعات، لتأسيس مجتمع أكثر متانة وقدرة على التعامل مع التحديات السيبرانية الحالية والمستقبلية.

5. قائمة المراجع:

Anderson, R., Smith, J., & Brown, K. (2020). Understanding and mitigating social engineering attacks. Journal of Cybersecurity Studies, 5(2), 123-145.

Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. Wiley.

Hafez, A., & Alqahtani, A. (2024). The role of knowledge management in confronting social engineering in the Saudi banking sector: A proposed model. Cybrarians Journal, (74), 105-157. https://doi.org/10.70000/cj.2024.74.616

Akçayır, M., & Akçayır, G. (2017). Advantages and challenges associated with augmented reality for education: A systematic review of the literature. Educational Research Review, 20, 1–11. https://doi.org/10.1016/J.EDUREV.2016.11.002

علي, إ. م. م. . م. (2020). دور العتيبي, ع. ا. ب. ب. ش. ا., Al-Otaibi, A. R. B., & الأمن السيبراني في تحقيق رؤية 2030. http://repository.nauss.edu.sa//handle/123456789/66694

سليمان, م. (2022). نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية. المجلة المصرية للعلوم الاجتماعية والسلوكية, 6(6), 114–130. https://doi.org/10.21608/EJSBS.2022.129409.1005

على إبراهيم أحمد, ف., يوسف, أ. د. ر., & عيد, د. و. (2022). الأمن السيبراني والنظافة الرقمية. المجلة المصرية لعلوم المعلومات, 9(2), 390–422. https://doi.org/10.21608/JESI.2022.166729.1066