سيف سبيس
Safe Space

منهج التربية الرقمية

خطة ورشة عمل للطلاب

الهندسة الاجتماعية

دولة قطر
وزارة التعليم و التعليم العالي

دولة قطر
State Of Qatar
Ministry of Transport & Communications
وزارة المواصلات والاتصالات

سيف سبيس
Safe Space

مكونات ورشة العمل

ملاحظة:
تشتمل هذه الوثيقة على خطة ورشة العمل فقط. جميع المكونات الأخرى لورشة العمل مذكورة في القائمة أدناه لعلم المدرب، ويمكنه الاطلاع عليها في ملف ورشة عمل الهندسة الاجتماعية.

- خطة ورشة العمل
- قراءة مرجعية للمدرب
- قراءة مرجعية للطالب
- عرض تقديمي عن الهندسة الاجتماعية
- أنشطة ورشة العمل
- مذكرات تدريبية للتوزيع
- استبيان تقييم ورشة العمل

سيف سبيس
Safe Space

مقدمة عن ورشة عمل الهندسة الاجتماعية

الجمهور المستهدف:
الطلاب

مدة ورشة العمل:
٢,٥ ساعة

مكونات ورشة العمل:

- خطة ورشة العمل
- قراءة مرجعية للمدرب
- قراءة مرجعية للطالب
- عرض تقديمي عن الهندسة الاجتماعية
- أنشطة ورشة العمل
- مذكرات تدريبية للتوزيع
- استبيان تقييم ورشة العمل

نظرة عامة على ورشة العمل:
تهدف ورشة عمل الهندسة الاجتماعية إلى تدريس الهندسة الاجتماعية ورفع الوعي بها. وتستهدف ورشة العمل الطلاب الذين تتراوح أعمارهم بين ١٣ و ١٨. ومدة ورشة العمل ساعتان ونصف تقريباً بحد أقصى ٢٥ طالب. وسوف تلقي ورشة العمل الضوء على فئتين رئيسيتين يمكن تصنيف كافة محاولات الهندسة الاجتماعية وفقاً لهما وهما الخداع القائم على التكنولوجيا والخداع القائم على العنصر البشري. وسوف يتم توضيح كل فئة ومناقشتها باستخدام أمثلة من الحياة الواقعية. كما ستلقي ورشة العمل الضوء على السلوكيات الشائعة المعرضة لهجوم الهندسة الاجتماعية بالإضافة إلى ذكر تأثيرها. وللتأكد من استيعاب الطلاب لمفاهيم الهندسة الاجتماعية فإنهم سوف يشاركون في نشاطين مختلفين بالإضافة إلى الكثير من المناقشات خلال ورشة العمل التي سوف تتيح لهم الفرصة لتبادل أفكارهم وممارسة ما يتعلمونه في ورشة العمل.

سيف سبيس
Safe Space

خطة ورشة عمل
الهندسة الاجتماعية

المدة:
حوالي ١٥٠ دقيقة

المتطلبات:
- لوحات الشرح
- أقلام تظليل
- مواد تدريبية وخطة
- رشة العمل
- عرض تقديمي

عدد المشاركين:
٢٥ طالب بحد أقصى

الغرض:
تدريس الهندسة الاجتماعية ورفع الوعي بها.

الأهداف:
١. تعريف الهندسة الاجتماعية.
٢. إلقاء الضوء على الخداع القائم على العنصر البشري.
٣. إلقاء الضوء على الخداع القائم على استخدام الكمبيوتر أو التكنولوجيا.
٤. إلقاء الضوء على السلوكيات الشائعة المعرضة لهجمات الهندسة الاجتماعية.
٥. إلقاء الضوء على تأثيرها.
٦. جعل الطلاب قادرين على تقييم السيناريوهات.
٧. مساعدة الطلاب من خلال تقديم بعض الآليات الوقائية للتصدي لهجمات الهندسة الاجتماعية.
٨. طرح نصيحة نهائية.

المواد المستخدمة:
- لوحات أوراق الشرح
- وأقلام تظليل
- مواد تدريبية
- وخطة ورشة العمل
- وعرض تقديمي

النشاط	المدرب	المشاركون	المواد	الوقت
مقدمة عامة عن البرنامج وموضوع اليوم – الشريحة ١.	هذه الشريحة افتتاحية. يقدّم المدرب نفسه /نفسها والبرنامج وموضوع اليوم (منهج التربية الرقمية). إذا دعت الحاجة – يطلب المدرب من المشاركين تقديم أنفسهم. وإذا رأى أن الأمر يتطلب استخدام أحد تمارين كسر حواجز التواصل– يقوم المدرب بأدائه الآن.	يستمع المشاركون ويقدموا أنفسهم.	عرض تقديمي، وتمارين كسر حواجز التواصل – نشاط ١.	١٥ دقيقة
أهداف الصف – الشرائح ٢ – ٣.	قم بتحديد أهداف الفصل. واستعرضها معهم وقم بإلقاء الضوء على النواحي الرئيسية الهامة التي سوف تتناولها.	يستمع المشاركون.	عرض تقديمي.	٥ دقائق
تعريف الهندسة الاجتماعية – الشريحة ٤.	قم بتعريف الهندسة الاجتماعية كما عرفها معهد سانز SANs بمزيد من التفصيل مع ذكر إيضاحات أكثر من جانبك.	يستمع المشاركون.	عرض تقديمي.	٥ دقائق
تقسيم مفهوم الهندسة الاجتماعية – الشريحة ٥.	يلزم عليك هنا إلقاء الضوء على الفئتين الرئيسيتين للهندسة الاجتماعية وقد تحتاج إلى الاستفاضة ولكن دون إسهاب حيث سيتم تناولها في الشرائح التالية.	يستمع المشاركون.	يستمع المشاركون.	٥ دقائق
الخداع القائم على العنصر البشري – الشرائح ٦–٧.	يلزم عليك أن تقوم هنا بإلقاء الضوء على الأنواع المختلفة لطرق الخداع البشري، وحاول تقديم أمثلة من الحياة الواقعية في مناقشتك للاستفاضة في الموضوع.	يستمع المشاركون.	عرض تقديمي.	١٥ دقيقة
الخداع القائم على التكنولوجيا – الشرائح ٨–٩.	يلزم عليك أن تقوم هنا بإلقاء الضوء على الأنواع المختلفة لطرق الخداع القائم على التكنولوجيا، وحاول تقديم أمثلة من الحياة الواقعية في مناقشتك للاستفاضة في الموضوع.	يستمع المشاركون.	عرض تقديمي.	١٥ دقيقة

النشاط	المدرب	المشاركون	المواد	الوقت
السلوكيات التي تعرض لهجمات الهندسة الاجتماعية – الشريحة ١٠–١١.	قم بإلقاء الضوء على العلاقة بين السلوكيات الشائعة المعرضة لهجمات الهندسة الاجتماعية وهجمات الهندسة الاجتماعية المرتبطة بها.على سبيل المثال، بسبب الثقة الزائدة في أشخاص لا تعرفهم فإنك قد تتعرض لهجمات التصيد بالحربة.	يستمع المشاركون.	عرض تقديمي.	١٠ دقائق
ما مدى تأثير ذلك علينا؟ – الشريحة ١٢.	هنا وبعد أن قمت بتعريف الأنماط المختلفة لهجمات الهندسة الاجتماعية وعلاقتها بسلوكياتنا، فإنك قد تحتاج إلى إلقاء الضوء على تأثيرها على حياتنا.	يستمع المشاركون.	عرض تقديمي.	١٠ دقائق
كيف تقييم الموقف – الشريحتان ١٣ و ١٤.	قم بتعليم المشاركين بعض الأسئلة التي يلزم عليهم ان يسألونها لأنفسهم قبل تقديم معلوماتهم للآخرين أو للغرباء.	يستمع المشاركون.	عرض تقديمي.	١٠ دقائق
فلنلعب دوراً! – الشريحة ١٥.	هنا يلزم أن تقسم المشاركين إلى مجموعات من خمس أفراد وتوزيع سيناريوهين من المذكرة التدريبية على كل مجموعة. ودعهم يقدمون عرض لعب أدوار لهذه السيناريوهات.	يستمع المشاركون ويشاركون في النشاط.	عرض تقديمي، والسيناريوهات الواردة في المادة التدريبية (ص ٨ و٩)، والنشاط ٢.	٣٠ دقيقة
كيف تتقي الهندسة الاجتماعية – الشرائح ١٦– ٢٢.	تحتاج هنا إلى التركيز على كيفية توخي المزيد من الحيطة ودعوتهم إلي ذلك عندما يتعلق الأمر بالتواصل من خلال شبكة الإنترنت أو دون الاتصال بشبكة الإنترنت من خلال منحهم بعض النصائح والمشورة.	يستمع المشاركون.	عرض تقديمي.	١٥ دقيقة

النشاط	المدرب	المشاركون	المواد	الوقت
نصيحة عامة – الشريحة ٢٣–٢٤.	قم بإلقاء الضوء على النقاط الأساسية المتعلقة بكيفية توخي المزيد من الحذر عندما يتعلق الأمر بالهندسة الاجتماعية.	يستمع المشاركون.	عرض تقديمي	٥ دقائق
هل هناك أية أسئلة؟ – الشريحة ٢٥.	قم بتشجيع المشاركين على طرح أسئلة عن الموضوع أو تتعلق بالسلامة بوجه عام. وقم بتمرير استبيانات التقييم بالإضافة إلى مقالات والأسئلة الشائعة ونصائح عليهم ليقوموا بقراءتها عندما يعودون إلى المنزل.	يطرح المشاركون الأسئلة إن وجدت.	عرض تقديمي واستبيان تقييم.	١٠ دقائق

سيف سبيس
Safe Space

منهج التربية الرقمية

ورشة عمل للطلاب: النشاط (١)
تمارين لكسر الحاجز
الهندسة الاجتماعية

دولة قطر
وزارة التعليم و التعليم العالي

دولة قطر
State Of Qatar
Ministry of Transport & Communications
وزارة المواصلات والاتصالات

سيف سبيس
Safe Space

النشاط ١
تمارين لكسر الحاجز

ملاحظات للمدرب:
يمكنك أن تختار أحد تمارين كسر الحاجز المقترحة من القائمة، أو أن تختار واحداً من بين تلك التمارين تكون قد أديته قبل ذلك أثناء ممارستك التدريبية. إن القيام بتمارين كسر الحاجز ليس إلزامياً، وعندما تقوم بتدريب معلمين فإن العادة جرت بأن تختار تلك التمارين التي لا تتطلب الكثير من الطاقة والحركة؛ فمحادثة قصيرة أو حكاية من واقع الحياة أفضل من لعبة "الغميضة" أو أية أنشطة أخرى من هذا النوع. فقط راقب المجموعة وفكر فيما يحتاجونه؛ هل يحتاجون إلى المزيد من الطاقة أو طاقة أقل، أو هل يحتاجون منك إلى أن تستمر في الأنشطة فحسب.

تم وصف تمارين كسر الحاجز بشكل منفصل.

استخدم تمارين كسر الحاجز فقط إذا شعرت أنها ستساعدك في ورشة العمل. فهذه التمارين ليست هي جوهر المحتوى الذي تقدمه – فلا تجعل ورشة العمل عبارة عن مجموعة من تمارين كسر الحاجز فحسب.

سوف تجد وصفاً موجزاً لتمارين كسر الحاجز في المواد الخاصة بالمعلم.

طرق متنوعة لأداء النشاط:
اتخذ من قائمة تمارين كسر الحاجز مصدراً للإلهام. فهذا النوع من الأنشطة البسيطة هو أنشطة يجمعها كل مدرب بنفسه ويدخل عليها ما يشاء من التعديلات بشكل مستمر، ويستخدمها في الوقت الملائم. فإذا كان لديك مجموعة من المعلمين من نفس المدرسة فلا تستخدم تمارين كسر الحاجز التي يفترض أن تساعد المشاركين على تذكر أسماء بعضهم البعض لأنها لن تكون مناسبة، أما إذا كانت مجموعة المشاركين تتكون من معلمين أكبر سناً وأكثر خبرة، فلا تحاول أن تطلب منهم أن يركضوا في المكان ويغنوا لأنهم على الأرجح سيرفضون ذلك.

إذا شعرت أن لديك نشاط بسيط تفضل أن تستخدمه فاستخدمه إذاً.

١. الأسماء
يجلس المشاركون في دائرة وينطق كل واحد منهم اسمه مع تكرار كافة أسماء المشاركين الذين تحدثوا قبله. ويكون للمشارك الأول جولة إضافية يكرر فيها كافة الأسماء في النهاية.

٢. الأسماء
يجلس المشاركون في دائرة وينطق كل واحد منهم اسمه بأن يقول مثلاً: (محمد، مدرس) بحيث يختار كلمات تصفه بدقة وتبدأ بنفس الحرف الذي يبدأ به اسمه.

٣. الأسماء
ينطق المشاركون أسماءهم فحسب واحداً تلو الآخر.

٤. الهوايات
يقف المشاركون على كراسي في شكل دائرة وتنظيم محدد، ثم يمشون على الكراسي ليضعوا أنفسهم في ترتيب معين (تبعاً لمقاس الحذاء مثلاً).

٥. الهوايات
يرسم جميع المشاركين هواياتهم المفضلة. بعد ذلك، يتم اختيار أربعة مشاركين ليقفوا في جوانب الحجرة ودون أن يتحدثوا، وإنما فقط من خلال مشاهدة رسومات المشاركين الآخرين، يحاولون تخمين الأشخاص الذين يشتركون معهم في الهوايات. ثم عليهم بعد ذلك أن يجدوا مكاناً بالقرب من الرسم الذي يرون أنه يصف هواية مماثلة لهوايتهم. كل ذلك دون أن يتحدثوا! وبعد الانتهاء من المهمة، يجلس أفراد المجموعة مع بعضهم البعض ويناقشون النتائج – كيف يمكن أن تكون المظاهر مضللة. ☺

٦. للمتعة فحسب
يقسم المشاركون إلى مجموعات من ثلاثة أفراد على الأقل ويطلب منهم بناء "ماكينة لـ ...." وتبعاً لمستوى قدرة المشاركين على التفكير المجرد، سيقومون إما ببناء ماكينات معينة، أي لتشذيب العشب مثلاً، أو، على سبيل المثال، بناء ماكينة تجعل الشمس تشرق.

٧. للمتعة فحسب
يجلس أحد المشاركين على كرسي ويحاول أربعة مشاركين آخرين رفعه/ رفعها بأصابعهم.

٨. للمتعة فحسب
تخمين الشخصيات – توضع ملصقات على ظهور المشاركين بأسماء شخصيات (من أفلام الكرتون أو من عالم السياسة، أو الأفلام ... الخ). وتكون مهمتهم تخمين الشخصية التي يحملون اسمها. ويمكنهم أن يسألوا الآخرين أسئلة، ولكن تقتصر الإجابات التي يتوقعونها على "نعم" أو "لا" فقط.

٩. التعليقات
السيجارة – يكتب المشاركون تعليقاً ويطوون الورقة واحداً تلو الآخر حتى يكونوا سيجارة في النهاية. ويمكن للمدرب أن يقرر نوع التعليق الذي يريده/ تريده.

١٠. التعليقات
يرسم المشاركون أيديهم على ورقة – مجرد رسم. بعد ذلك يكتبون اسمهم عليها. وبعد ذلك، يطلب منهم عدّ الجوانب الإيجابية التي يتمتعون بها وكتابة العدد. ثم يطلب منهم إضافة رقم ٢ إلى العدد الذي كتبوه ويكون ذلك العدد هو عدد الجوانب التي طلب منهم تسميتها وكتابتها.

١١. التعليقات

يضع المدرب سلطانية في مكان ظاهر ويطلب من المشاركين أن يضعوا فيها تعليقاتهم عنها على ملصقات في كل مرة يرغبون في ذلك.

١٢. تمارين متنوعة

يقسم المشاركون إلى مجموعات ثنائية ويتحدثون عن بعضهم البعض لدقيقة واحدة، ويسجل المشارك الآخر ملاحظات. بعد ذلك تكون مهمتهم رسم كافة الأشياء التي سمعوها وأن يعرضوها للمجموعة ويطلبوا منهم تخمين ما تم رسمه.

١٣. التغلب على التوتر

ما الذي يغضبك في .. (المدرسة، العمل ... الخ)؟ اكتبه بشكل فردي. لن نقرأه. فما تكتبه يخصك وحدك كي تعرفه. والآن مزق الورقة إلى أصغر قطع ممكنة. وتخيل مخلوقاً هزلياً غريباً. والآن الصق قصاصات الورق على ورقة لتشكيل المخلوق الذي تخيلته. ☺

سيف سبيس
Safe Space

منهج التربية الرقمية

ورشة عمل للطلاب: النشاط (٢)
عمل جماعي
الهندسة الاجتماعية

دولة قطر
وزارة التعليم و التعليم العالي

دولة قطر
State Of Qatar
Ministry of Transport & Communications
وزارة المواصلات والاتصالات

سيف سبيس
Safe Space

النشاط ٢ – عمل جماعي
الهندسة الاجتماعية

الموضوع:
نشاط ٢ – لعب أدوار عن الهندسة الاجتماعية.

العنوان:
عنوان النشاط – لعب أدوار.

الأهداف التي يشملها النشاط:
سوف يتعرف المشاركون على مختلف أنواع هجمات الهندسة الاجتماعية وسيكون بمقدورهم التعامل معها.

الوقت:
٣٠ دقيقة

الموارد:
عرض تقديمي، وسيناريوهات من المذكرات التدريبية – الشريحة ١٥.

ملاحظات للمدرب:
اطلب من المشاركين أن ينقسموا إلى مجموعات يتكون كل منها من خمسة أشخاص. وقم بتوزيع سيناريوهين على كل مجموعة. وأتح لهم ثلاثة دقائق للتفكير في السيناريوهات المقدمة لهم ودعهم يختارون شخصاً أو اثنين من المجموعة لتقديم سيناريو ١ وشخصاً آخر أو شخصين آخرين لتقديم سيناريو ٢. وأتح لكل مجموعة مدة خمس دقائق لتقديم نتائج السيناريوهين المقدمين (دقيقتين ونصف لكل سيناريو).
اختتم نشاط لعب الأدوار، وانتقل إلى الشريحة التالية.

طرق متنوعة لأداء النشاط:
إذا كانت المجموعة صغيرة، دعهم يقومون بعرض لعب أدوار للأربع سيناريوهات واشرح الباقي لهم.
إذا وجدت أن بعض المجموعات تجد صعوبة بالغة في تقديم عرض لعب أدوار عن السيناريوهات، شجعهم وشارك في السيناريوهات المقدمة.
وإذا كان لديك الوقت الكافي، وكنت في معمل للكمبيوتر، اطلب منهم البحث عن مواقف أخرى قد يتعرض لها المرء على شبكة الإنترنت أو بعيداً عنها نتيجة للهندسة الاجتماعية. واطلب منهم تقديم النتائج مع حلول ممكنة للمواقف.

سيف سبيس
Safe Space

السيناريوهات
الهندسة الاجتماعية

سيناريو (١):
تلقيت مكالمة هاتفية من مدير المدرسة يدعي فيها أن معلومات حسابك تحتاج إلى تحديث، وطلب منك بيانات اعتماد حسابك للتحقق من حسابك وتحديثه. كيف ستتصرف وما هو نوع التدابير التي سوف تتخذها بعد المكالمة مباشرة؟
يتضمن هذا السيناريو شخصين؛ متلقي المكالمة (الطالب) والمتصل (من يدعى أنه مسؤول تكنولوجيا المعلومات).

سيناريو (٢):
تلقيت مكالمة هاتفية من شخص ما يدعي أنه من بنك والدك، وطلب/ طلبت منك بعض المعلومات عنك وعن والدك. ما هي النتائج الممكنة، وكيف يجب عليك أن تتصرف؟ وما هو نوع التدابير التي سوف تتخذها بعد المكالمة مباشرة؟
يتضمن هذا السيناريو شخصين، متلقي المكالمة (الطالب) والمتصل (المصرفي المزعوم).

سيناريو (٣):
شخص يعرف نفسه/ نفسها بأنه قريب لأحد زملائك ويريد أن يدخل مبنى المدرسة معك. ما هي النتائج المحتملة، وكيف يجب عليك أن تتصرف؟
يتضمن هذا السيناريو شخصين، (الطالب) و(قريب الزميل المزعوم).

سيناريو (٤):
وجدت عصا USB في معمل الكمبيوتر في المدرسة وعلى عصا USB كتب "اربح الجائزة" أو "جائزة رائعة" أو شيء مثل "إلى صديقتي". ما هي العواقب، وكيف يجب عليك أن تتصرف؟
يتضمن هذا السيناريو شخصين، شخص ترك عصا USB والآخر الذي وجدها في المعمل.

سيناريو (٥):
طلب منك شخص ما أن تعطيه هاتفك لأن بطاريات هاتفه/هاتفها استنفدت أو فُقدت. ما هي العواقب المحتملة، وكيف يجب أن تتصرف؟
يتضمن هذا السيناريو شخصين، المتلقي والطالب.

سيناريو (٦):
عرض عليك شخص لا تعرفه جيداً أن يوصلك إلى المنزل. ما هي النتائج المحتملة، وكيف يجب عليك أن تتصرف؟
يتضمن هذا السيناريو شخصين، الشخص الذي يعرض التوصيل، ومتلقي العرض.

سيناريو (٧):
تقف أمام ماكينة الصراف الآلي لسحب بعض النقد وقبل أن تبدأ في كتابة بعض المعلومات تجد أن شخصاً ما يقف بقربك. ما هي النتائج المحتملة، وكيف يجب أن تتصرف؟

سيناريو (٨):
أنت في البيت وحدك وتلقيت مكالمة هاتفية من شخص ما لا تعرفه وسأل عن والدك لأمر عاجل يتعلق بالعمل أو شيء ما. ما هي النتائج المحتملة، وكيف يجب أن تتصرف؟

سيناريو (٩):
ليس لديك كلمة مرور لحماية هاتفك وقمت بتركه دون إشراف في المعمل أو في دورة المياة خلال فترة الاستراحة.
ما هي العواقب المحتملة، وما الذي كان ينبغي عليك القيام به بشكل مختلف لإزالة الخطر؟

سيناريو (١٠):
أنهيت الواجب المسند إليك في معمل الكمبيوتر وقمت بحفظه وطباعته. ما هي النتائج المحتملة، وما الذي كان ينبغي عليك القيام به بشكل مختلف لإزالة الخطر؟

سيف سبيس
Safe Space

منهج التربية الرقمية

ورشة عمل للطلاب:
قراءات مرجعية للمدربين
الهندسة الاجتماعية

دولة قطر
وزارة التعليم و التعليم العالي

دولة قطر
State Of Qatar
Ministry of Transport & Communications
وزارة المواصلات والاتصالات

سيف سبيس
Safe Space

قراءات مرجعية
للمدربين

ملاحظة:
الغرض من القراءات في خلفية الموضوع هو تقديم محتوى تفصيلي للمدربين بشأن الموضوعات التي سيتناولونها بالشرح والمشاركة مع الجمهور.

الهندسة الاجتماعية
أكبر تهديد للأمن على الإنترنت

عندما تسمع عن عمليات الاحتيال وخداع الآخرين أو غشهم للحصول على أموالهم عن طريق استخدام بطاقات ائتمان وهمية أو اقتحام المواقع الإلكترونية الحكومية أو مواقع التواصل الاجتماعي الخاصة لشخص ما، لا يمكن أن يمر ذلك عليك مرور الكرام. فقد تعجب كيف يقوم هؤلاء الأشخاص بمثل هذه الأعمال بينما يتم استخدام الكثير من أدوات أمن تكنولوجيا المعلومات. وهنا يجب على المرء أن يعرف ما هي "الهندسة الاجتماعية".

قد يبدو مصطلح "الهندسة الاجتماعية" للشخص العادي كشيء مفيد، شيء له علاقة بالجانب 'الاجتماعي' للهندسة (مثل الهندسة الكهربائية أو الميكانيكية أو الكيمائية). إلا أن له معنى آخر يشير إلى الطرق المختلفة التي تستخدم للتلاعب بالأشخاص للوصول إلى المباني أو الأنظمة أو الحصول على معلومات سرية لارتكاب عمليات الاحتيال. وأكثر الطرق ضرراً لاستخدام الهندسة الاجتماعية يمكن مشاهدتها في أي منزل – بأن تتحايل الطفلة على والدها لكي يشتري لها لعبتها المفضلة. وينطبق نفس مبدأ التلاعب على مواقف مختلفة لأشخاص مختلفين.

ويصرح كيفين ميتنيك Kevin Mitnick[1] مجرم الكمبيوتر الذي خضع للتأهيل والذي يعمل الآن مستشار أمن بأن "أضعف حلقة في سلسلة الأمن هي العنصر البشري". والهدف الوحيد للمهندس الاجتماعي هو كسب ثقة الفرد للحصول على معلومات هامة لتحقيق ربح مادي أو سرقة هوية شخص ما أو الاستعداد لهجوم على هدف أكثر أهميةً.

وقد توقعت مجلة فوربس Forbes[2] أن تكون الهندسة الاجتماعية هي أخطر تهديد للأمن على الإنترنت في عام ٢٠١٣ وقد كنا شهوداً على الكثير من هذه الهجمات على الشركات ومواقع وسائل الاعلام الاجتماعية.
ومع اتساع تغطية تكنولوجيا المعلومات لكافة جوانب التفاعل الإنساني في مجالات التعليم والخدمات المصرفية والتسوق ووسائل الإعلام الاجتماعية، الخ، فقد أصبح الشعور بتهديد الهندسة الاجتماعية يتزايد أيضاً. ويحاول المهندس الاجتماعي بناء الثقة وجمع المعلومات من خلال عدة طرق أو حتى عن طريق إقامة العلاقات بحيث يستطيع استغلالها والاشتراك في أو تنفيذ إجراءات يمكن أن تخدم غرضه.

1 http://resources.infosecinstitute.com/social-engineering-art-human-hacking/
2 http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013-2/

وتتمثل الطرق المختلفة التي يخدع بها المهندس الاجتماعي الآخرين فيما يلي:

- **التحجج الاحتيالي** وهو الأسلوب الأكثر شيوعاً والذي يستخدم على نطاق واسع وفيه يدعي الشخص هوية مزيفة أو وهمية لجمع معلومات شخصية.

- **القراءة التلصصية** وتتم في الغالب عندما يراقب شخص ما من وراء الكتف شخصاً آخر أثناء كتابته الكلمة المرور على جهاز كمبيوتر محمول/ معاملة بنكية/ باستخدام بطاقة الصراف الآلي، الخ.

- **السرقة التحويلية** وتعرف أيضاً بلعبة الشّرك، وتحدث عندما يقوم الشخص بإقناع شركة توصيل البريد أو شركة النقل بأنه هو الشخص المقصود بالفعل لاستلام الشحنة المرسلة.

- **التفتيش في سلة المهملات** ويحدث عندما يبحث شخص ما في سلة المهملات للحصول على معلومات من خلال قصاصات الورق التي تحتوي على كلمات مرور/ عناوين/ بريد إلكتروني.

- **التصيد** وهو احتيال يتم على الإنترنت تظهر فيه رسالة البريد الإلكتروني وكأنها قادمة من مؤسسة شرعية – كبنك أو شركة لبطاقات الائتمان تطلب "التحقق" من المعلومات الشخصية وتحذر من عواقب وخيمة إذا لم يتم تقديمها.

- **التتبع** ويحدث عندما يستطيع شخص ما الدخول إلى مبنى مرفق ما من خلال تضليل أو خداع شخص مرخص له بالدخول.

- **الاصطياد** يحدث عندما يترك قرص مضغوط أو جهاز به فيروس مهملاً في مكان ما لإثارة فضول شخص ما لكي يتحقق من المحتويات بتركيبهما على نظام ما، وبذلك يمكن اختراق النظام.

- **طريقة "الشيء بالشيء" أو "سياسة الأخذ والعطاء"** ويقال أنها تستخدم عندما يعرض شخص ما المساعدة عادة في صورة هدية مجانية أو دعم فني مقابل الحصول على المعلومات الشخصية.

- **النوافذ المنبثقة الوهمية** وهي برامج مصممة تظهر أثناء القيام بعمل شرعي وتطلب من الشخص إعادة إدخال هويته وكلمة المرور الخاصة به لاستئناف العمل لأسباب تتعلق بالاتصال بالشبكة، وبالتالي جمع البيانات الشخصية.

وباختصار، فإن الطرق الموضحة أعلاه يتم استخدامها للحصول على بياناتك الشخصية التي لم يكن ليتم الكشف عنها أبداً في الظروف العادية. وإذا كانت شركات مثل جوجل ومواقع وسائل الإعلام مثل موقع فيسبوك لم تنج من الهجمات الإلكترونية، فإن الأشخاص الأقل استعداداً سوف يتم الوصول إليهم دون أن ينتبهوا. إن معرفة "الهندسة الاجتماعية" لن ينبهك للمخططات التي يستخدمها الأشخاص سيئو النية فحسب، بل سيجعلك مستعداً لإحباط خططهم. وكما يقول ميغيل دي سرفانتس Miguel de Cervantes: "لقد أعذر من أنذر؛ فالاستعداد نصف الانتصار"

سيف سبيس
Safe Space

منهج التربية الرقمية

ورشة عمل للطلاب:
قراءات تدريبية للطلاب
الهندسة الاجتماعية

دولة قطر
وزارة التعليم و التعليم العالي

دولة قطر
State Of Qatar
Ministry of Transport & Communications
وزارة المواصلات والاتصالات

سيف سبيس
Safe Space

قراءات مرجعية للطلاب

ملاحظة:
اجعل الطلاب يقومون بقراءة وثيقة المعلومات عن خلفية الموضوع قبل الحضور إلى ورشة العمل أو قبل بدء دورة ورشة العمل.

الهندسة الاجتماعية للطلاب

ما الذي يجب أن يعرفه الشباب عن الهندسة الاجتماعية ؟

الهندسة الاجتماعية هي فعل يتمثل في التلاعب بالأشخاص لجعلهم يقومون ببعض التصرفات. والهدف من ذلك هو خداع شخص ما لكي يقوم بتقديم معلوماته الهامة أو مدخل لهذه المعلومات. وقد استُخدمت هذه الطريقة بشكل أساسي من قبل القراصنة بهدف الوصول إلى المباني أو الأنظمة أو المعلومات عن طريق استخدام علم النفس البشري بدلاً من الاقتحام أو استخدام طرق القرصنة التقنية. وقد تمت ممارسة هذه الطريقة لعقود؛ واشتهرت باسم "الهندسة الاجتماعية" في التسعينيات من خلال القرصان الشهير كيفين ميتنيك Kevin Mitnick. وهو حالياً مستشار دولي لأمن المعلومات، ويقوم بإجراء اختبار لنقاط قوة وضعف أمن الشركات.

وقد لا يأخذ الشباب مخاطر الهندسة الاجتماعية على محمل الجد لأنهم يعتقدون أن هذه التقنيات تدير بشكل أساسي للوصول إلى معلومات المؤسسات الكبرى. إلا أن الحقيقة هي أن المجرمين في الجيل الحالي يقومون باستخدام هذه الطريقة للوصول إلى المنازل وحسابات البنوك بهدف الحصول على الأموال في المقام الأول، والشباب يشكلون أهدافاً سهلة. ومجرمو الهندسة الاجتماعية يوجدون في كل مكان ويستهدفون الحصول على معلومات بهدف خداع شخص ما والاستفادة من ذلك. ونحن عرضة أو قد نكون قد وقعنا ضحية لهذه الهجمات دون علمنا.

ونحن قد نصبح هدفاً للكشف عن معلومات عن مدرستنا أو أولياء أمورنا أو منزلنا، الخ. وقد لا يبدو الأمر مريباً إلا أنه قد يستخدم لتنفيذ عمل إجرامي. إن المهندسين الاجتماعيين أشخاص ماهرون باستطاعتهم كسب ثقتنا. وهم يتخفون في صورة أشخاص عاديين ويكون لديهم القدرة على استخلاص أي نوع من المعلومات. ومن أهم حوادث الاحتيال عن طريق الهندسة الاجتماعية والتي استرعت انتباه الجمهور في عام ٢٠١٠ كان هو موضوع ويكيليكس[1] WikiLeaks الشهير الذي بدأه جوليان أسانج Julian Assange للحصول على معلومات حساسة من عدة دول. وقد سببت مثل هذه الأنواع من الهجمات تهديداً كبيراً لمعلومات المؤسسات وممتلكاتها والتي يتم اتخاذ إجراءات أمنية عديدة لحمايتها.

[1] http://news.idg.no/cw/art.cfm?id=57716384-1A64-6A71-CE2AE8785D9CF7BF

ونحن نكون عرضة لهجمات الهندسة الاجتماعية عندما يتصل بنا شخص ما ويقدم نفسه كمختص الكمبيوتر في المدرسة للحصول على كلمة المرور الخاصة بنا. فإذا لم تنتبه إلى التأكد جيداً من هويته، فقد تقوم بتقاسم كلمة المرور الخاصة بك مع القرصان. كما قد يصل إلى حساباتنا على شبكة الإنترنت عندما نقوم بالدخول إلى حسابنا باستخدام كلمة المرور نفسها. وقد يشرع القرصان في عمل من أعمال التعدي الإلكتروني على أي من الجهات الموجودة على قائمة اتصالاتنا ويتسبب في تدمير سمعتنا على شبكة الإنترنت. وهذه هي إحدى طرق الحصول على معلوماتنا، إلا أن المهندسين الاجتماعيين يستخدمون طرقاً أخرى مثل التحدث إليك بصورة ودية عند دخولهم إلى المدرسة مدعين أنهم أقرباء زميلك في المدرسة، وبهذه الطريقة يتمكنون من دخول مبنى المدرسة. وقد يدخل مثل هؤلاء القراصنة المدرسة بهدف سرقة الوثائق الخاصة بها أو لمحاولة الحصول على معلومات عن مكان ممتلكات قيمة للسطو عليها فيما بعد.

وقد تحدث الهندسة الاجتماعية أيضاً عند زيارتنا لأحد المراكز التجارية حيث يتوجه إلينا أحد الأشخاص لدعوتنا إلى المشاركة في مسابقة حظ ذات جوائز بذكر أن الفائز فيها سوف يحصل على سيارة أو أحد الأجهزة الذكية، الخ. فنتحمس بشأن الجائزة ونقوم بتقديم معلوماتنا الشخصية. وتسمى هذه الطريقة "الشيء بالشيء" أو "سياسة الأخذ والعطاء" وقد لا تتسبب لنا في أي خسارة، ولكن من يستخدمون معلوماتنا يحققون أرباحاً من خلال بيعها للتجار على شبكة الإنترنت أو لشركات جمع البيانات، الخ.

ويجب علينا أن نعرف أن معلوماتنا الشخصية تمثل هويتنا ويجب أن نقوم بحمايتها.

الهندسة الاجتماعية
أكبر تهديد للأمن على الإنترنت

عندما تسمع عن عمليات الاحتيال وخداع الآخرين أو غشهم للحصول على أموالهم عن طريق استخدام بطاقات إئتمان وهمية أو اقتحام المواقع الإلكترونية الحكومية أو مواقع التواصل الاجتماعي الخاصة لشخص ما، لا يمكن أن يمر ذلك عليك مرور الكرام. فقد تعجب كيف يقوم هؤلاء الأشخاص بمثل هذه الأعمال بينما يتم استخدام الكثير من أدوات أمن تكنولوجيا المعلومات. وهنا يجب على المرء أن يعرف ما هي "الهندسة الاجتماعية".

قد يبدو مصطلح "الهندسة الاجتماعية" للشخص العادي كشيء مفيد، شيء له علاقة بالجانب 'الاجتماعي' للهندسة (مثل الهندسة الكهربائية أو الميكانيكية أو الكيمائية). إلا أن له معنى آخر يشير إلى الطرق المختلفة التي تستخدم للتلاعب بالأشخاص للوصول إلى المباني أو الأنظمة أو الحصول على معلومات سرية لارتكاب عمليات الاحتيال. وأكثر الطرق ضرراً لاستخدام الهندسة الاجتماعية يمكن مشاهدتها في أي منزل – بأن تتحايل الطفلة على والدها لكي يشتري لها لعبتها المفضلة. وينطبق نفس مبدأ التلاعب على مواقف مختلفة لأشخاص مختلفين.

ويصرح كيفين ميتنيك Kevin Mitnick [٢] مجرم الكمبيوتر الذي خضع للتأهيل والذي يعمل الآن مستشار أمن بأن "أضعف حلقة في سلسلة الأمن هي العنصر البشري". والهدف الوحيد للمهندس الاجتماعي هو كسب ثقة الفرد للحصول على معلومات هامة لتحقيق ربح مادي أو سرقة هوية شخص ما أو الاستعداد لهجوم على هدف أكثر أهمية.

وقد توقعت مجلة فوربس Forbes [٣] أن تكون الهندسة الاجتماعية هي أخطر تهديد للأمن على الإنترنت في عام ٢٠١٣، وقد كنا شهوداً على الكثير من هذه الهجمات على الشركات ومواقع وسائل الاعلام الاجتماعية.

ومع اتساع تغطية تكنولوجيا المعلومات لكافة جوانب التفاعل الإنساني في مجالات التعليم والخدمات المصرفية والتسوق ووسائل الإعلام الاجتماعية، الخ، فقد أصبح الشعور بتهديد الهندسة الاجتماعية يتزايد أيضاً. ويحاول المهندس الاجتماعي بناء الثقة وجمع المعلومات من خلال عدة طرق أو حتى عن طريق إقامة العلاقات بحيث يستطيع استغلالها والاشتراك في أو تنفيذ إجراءات يمكن أن تخدم غرضه.

٢ http://resources.infosecinstitute.com/social-engineering-art-human-hacking/
٣ http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013-2/

وتتمثل الطرق المختلفة التي يخدع بها المهندس الاجتماعي الآخرين فيما يلي:

- **التحجج الاحتيالي** وهو الأسلوب الأكثر شيوعاً والذي يستخدم على نطاق واسع وفيه يدعي الشخص هوية مزيفة أو وهمية لجمع معلومات شخصية.

- **القراءة التلصصية** وتتم في الغالب عندما يراقب شخص ما من وراء الكتف شخصاً آخر أثناء كتابته الكلمة المرور على جهاز كمبيوتر محمول/ معاملة بنكية/ باستخدام بطاقة الصراف الآلي، الخ.

- **السرقة التحويلية** وتعرف أيضاً بلعبة الشّرك، وتحدث عندما يقوم الشخص بإقناع شركة توصيل البريد أو شركة النقل بأنه هو الشخص المقصود بالفعل لاستلام الشحنة المرسلة.

- **التفتيش في سلة المهملات** ويحدث عندما يبحث شخص ما في سلة المهملات للحصول على معلومات من خلال قصاصات الورق التي تحتوي على كلمات مرور/ عناوين/ بريد إلكتروني.

- **التصيد** وهو احتيال يتم على الإنترنت تظهر فيه رسالة البريد الإلكتروني وكأنها قادمة من مؤسسة شرعية كبنك أو شركة لبطاقات الائتمان تطلب "التحقق" من المعلومات الشخصية وتحذر من عواقب وخيمة إذا لم يتم تقديمها.

- **التتبع** ويحدث عندما يستطيع شخص ما الدخول إلى مبنى مرفق ما من خلال تضليل أو خداع شخص مرخص له بالدخول.

- **الاصطياد** يحدث عندما يترك قرص مضغوط أو جهاز به فيروس مهملاً في مكان ما لإثارة فضول شخص ما لكي يتحقق من المحتويات بتركيبهما على نظام ما، وبذلك يمكن اختراق النظام.

- **طريقة "الشيء بالشيء" أو "سياسة الأخذ والعطاء"** ويقال أنها تستخدم عندما يعرض شخص ما المساعدة عادة في صورة هدية مجانية أو دعم فني مقابل الحصول على المعلومات الشخصية.

- **النوافذ المنبثقة الوهمية** وهي برامج مصممة تظهر أثناء القيام بعمل شرعي وتطلب من الشخص إعادة إدخال هويته وكلمة المرور الخاصة به لاستئناف العمل لأسباب تتعلق بالاتصال بالشبكة، وبالتالي جمع البيانات الشخصية.

وباختصار، فإن الطرق الموضحة أعلاه يتم استخدامها للحصول على بياناتك الشخصية التي لم يكن ليتم الكشف عنها أبداً في الظروف العادية. وإذا كانت شركات مثل جوجل ومواقع وسائل الإعلام مثل موقع فيسبوك لم تنج من الهجمات الإلكترونية، فإن الأشخاص الأقل استعداداً سوف يتم الوصول إليهم دون أن ينتبهوا. إن معرفة "الهندسة الاجتماعية" لن ينبهك للمخططات التي يستخدمها الأشخاص سيئو النية فحسب، بل سيجعلك مستعداً لإحباط خططهم. وكما يقول ميغيل دي سرفانتس Miguel de Cervantes: "لقد أعذر من أنذر؛ فالاستعداد نصف الانتصار"

سيف سبيس
Safe Space

الهندسة الاجتماعية
لماذا يقوم أحدهم باختراق معلوماتك؟

المؤسسات تعتبر المعلومات بمثابة دماء المؤسسة. وأي اختراق في الوصول للمعلومات قد يدمر سمعة المؤسسة. واليوم، وبفضل الخدمات التي تقدم على شبكة الإنترنت والتي تجعل هويتنا معروفة على مستوى العالم، فإن معلوماتنا هي هويتنا. إن معظمنا يعرف بعضه بعضاً الآن ويتم الاتصال بينه وبين الآخرين من خلال هويته على الإنترنت. وكشباب فإننا حريصون على أن يكون لدينا هوية على شبكة الإنترنت وقد قمنا بعلمنا أو بدون علمنا بإنشاء سمعة لنا على شبكة الإنترنت.

وتساعدنا هويتنا على شبكة الإنترنت على أداء الكثير من الأعمال دون القيام بها بالطريقة التقليدية. وقد كانت هويتنا على الإنترنت تستخدم قبل ذلك في إرسال رسائل البريد الإلكتروني وتداول الصور الخ. إلا أن ما تقدم كان يتم بالإضافة إلى القيام بالكثير من العمليات المالية. وكشباب فقد لا تكون لنا وظيفة بعد، أو قد نمتلك حسابات بنكية، إلا أن المجرمين على شبكة الإنترنت يمكن أن يستخدموا معلوماتنا للقيام بالكثير من الأمور التي قد تكون مضرة بنا.

إن الأسباب التي قد تدعو شخصاً ما لسرقة معلوماتك مختلفة:

السبب الأول قد يكون '**الجشع**'؛ فالآن تتم سرقة معلوماتنا لبيعها للتجار على شبكة الإنترنت والذين يرسلون لنا رسائل البريد الإلكتروني أو يحاولون الاتصال بنا للترويج لمنتجاتهم وخدماتهم. وعندما نتلقى هذه المكالمات فإننا ندرك أننا لم نتوخى الحذر بشأن معلوماتنا في مكان ما. فهناك أشخاص يبحثون في سلة المهملات (التفتيش في سلة المهملات)، أو اختلاس النظر إلى جهاز الكمبيوتر المحمول أو الهاتف الذكي أثناء التواجد في الكافيتريا أو المطار، الخ. ويسمى هذا (القراءة التلصصية) للحصول على معلومات. وهناك مؤسسات تقوم بسرقة المعلومات الشخصية وبيعها للشركات على شبكة الإنترنت وتحقيق أرباح جيدة. وجشعهم لا يُشبع أبداً.

والسبب الثاني هو '**الكراهية**'؛ وهذا يتعلق بجرائم التعدي الإلكتروني. ففي بعض الأحيان قد يكره بعض الشباب شابا آخر في المدرسة أو الملعب ويحاولون إيذائه بشكل سري. وهذه الأنواع من الهجمات يبدأها أشخاص يعرفون الضحية أو قد يقوم بها غرباء تماماً. فمرتكب الجريمة يقوم بجمع المعلومات عن الضحية من الأصدقاء ويرسل سلسلة من الرسائل الجارحة لحساب الضحية على شبكة الإنترنت للتشهير به / بها وجعله يشعر بحالة بالغة من البؤس.

والسبب الثالث هو' **الضرورة**'؛ عندما يكون شخص ما في حاجة ماسة للمال باستخدام معلوماتك. وقد تحدث خدعة انتحال الشخصية عندما يستخدم الجاني معلوماتك ويحاول التقدم للحصول على قرض يتطلب منك أن تقوم بالسداد لاحقاً. وهذا الأمر شائع هذه الأيام وغالباً ما يتم القبض على هؤلاء الجناة وسجنهم. وكشباب فقد لا نملك حسابات بنكية، إلا أن المحتالين قد يحاولون الحصول على حسابات أولياء أمورنا من خلالنا.

والنقطة التي يجب التفكير فيها هي أنه لا يمكن إخفاء نشاط خاطئ لمدة طويلة، فكل شيء سوف ينكشف. غير أنه وإلى أن يتم القبض على الجاني، فسوف تعاني الضحية، كما إن ذلك يمثل تهديداً للآخرين كذلك. إن علينا أن نقوم بحماية معلوماتنا وتحذير الآخرين كذلك إذا كانوا لا يبالون بمعلوماتهم الشخصية.

سيف سبيس
Safe Space

الهندسة الاجتماعية
الأسئلة الشائعة

لماذا سيستهدفني المهندس الاجتماعي، فأنا مجرد طالب؟

يعتقد الطلاب أن المهندسين الاجتماعيين لن يستهدفونهم أبداً للحصول على معلوماتهم لأنهم مجرد طلاب وليس لديهم حسابات بنكية أو ممتلكات. في الواقع، فإن المهندسين الاجتماعيين يمكن أن يسرقوا الهويات لاستخدامها لشراء بطاقة SIM لهاتف نقال باسم الضحية ومن ثم يتم تغريم الضحية الفاتورة بعد ذلك. ولهذا، فلا تتهاون بشأن معلوماتك بل قم بحمايتها لأن المهندسين الاجتماعيين قادرون على عمل أي شئ باستخدام معلوماتك.

نصائح

١. لا تكتب كلمات مرور تحت نظر وبصر الجميع.
٢. احرص على إنشاء كلمات مرور منيعة على الهواتف الخلوية وغيرها من الأجهزة المتاح عليها الإنترنت.
٣. لا تترك أبداً أي مستندات سرية دون رقابة.
٤. مزق المستندات تماماً قبل إلقائها في سلة المهملات.
٥. لا تفتح مرفقات البريد الإلكتروني أبداً عندما تكون غير متأكد من المرسل.