الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي

اعداد
د. مها أحمد إبراهيم محمد
أستاذ علم المعلومات المساعد
قسم علوم المعلومات
كلية الآداب . جامعة بني سويف

ملخص :

تسعى هذه الدراسة إلى تحقيق هدف رئيس ؛ ألا وهو التعرف على مدى وعي المجتمع العربي بحماية حساباتهم الشخصية والتعرف على سبل الاختراق وانتهاك الخصوصية بشكل عام مع التركيز على الهندسة الاجتماعية بشكل خاص وسبل التدريب المتاحة تجاه حماية المواطن الرقمي ، من خلال التعرف بمفهوم الهندسة الاجتماعية (فن اختراق العقول)، وأهمية شبكات التواصل الاجتماعي في الوطن العربي، وأهمية الخصوصية من وجهة نظر مستخدمي شبكات التواصل الاجتماعي في الوطن العربي، وكذلك التعرف على طرق اختراق شبكات التواصل الاجتماعي وطرق الحماية من الهندسة الاجتماعية، ، حيث يعد وعي المجتمع العربي تجاه الهندسة الاجتماعية من أولويات المجتمع العربي لحماية حساباتهم في شبكات التواصل الاجتماعي وتوافر مهارات التصدي لهجمات الهندسة الاجتماعية في شبكات التواصل الاجتماعي. وطبقت الدراسة على عينة قوامها ٣٣٦ مفردة ومن ابرز ما توصلت إليه الدراسة أن مجتمع الدراسة يتم حماية بياناتهم الشخصية بشكل تلقائي وبمعدل مرتفع حيث كانت النتائج إيجابية نحو سلوك مجتمع الدراسة تجاه حماية معلوماتهم الشخصية على شبكات التواصل الاجتماعي. واختيار أسماء مستعارة غير حقيقة يسجل بها ما يزيد عن نصف مجتمع الدراسة على شبكات التواصل الاجتماعي وهذا ما وضحه نسبة ٥٣,٢ %، وعدم إتاحتهم لبياناتك الشخصية تارة وعدم صحة بياناتهم الشخصية المتاحة على حساباتهم تارة أخرى. بالإضافة إلى قلة من تعرض حساباتهم البنكية للاختراق حيث تعرض نسبة ٦,٨% فقط لاختراق الحسابات المصرفية.ومن أكثر الطرق شيوعًا لهجمات الهندسة الاجتماعية للرسائل الاقتحامية المزعجة Spam كتهنئة من صديق وهى ٧٧,١ %، تليها نسبة ٥٣,٢ % يقعون ضحية اقتناعهم بأهمية برامج من مواقع توهمهم بضرورة تحميلها .

تمهيد

نجد أن العالم في العصر الحالي ما كان ليتطور إلا باستخدام التكنولوجيا في جميع مسالك الحياة حيث تدخل التكنولوجيا إلى حياتنا أكثر فأكثر، فأصبحت التكنولوجيا والتقنية أمراً هاماً لا يُستغنى عنه في مجالات الحياة المتعددة، نظرًا لما تقدمه لنا من تسيير وتسهيل مهام ووظائف ومتطلبات الحياة اليومية، نشهد في الوقت الحالي ثورة تقنية هائلة في المجال التكنولوجي والمعلومات الرقمية التي نعيشها تحمل معها الكثير من الإيجابيات والسلبيات للفرد والمجتمع، مما أدى إلى نيل نصيب وافر من تلك التقنيات في حياتنا حتى أضحى من الصعب الاستغناء عنها مما يقع على عاتقنا نحن سواء كأفراد أو مستهلكين للتقنية مهمة نشر ثقافة الوعي المجتمعي للاستخدام الأمثل لتلك التقنيات في نطاقها الصحيح، ومن ثم وجب علينا أن نسعى ونتعاون من أجل توظيف التقنية والتكنولوجيا بالطرق العلمية الصحيحة وأيضًا وفقا لقواعد أخلاقية سليمة، مع الأخذ في الاعتبار مراعاة الضوابط القانونية والدينية، والتي ستعمل على الحد من سلبيات التقنية على المجتمع.

أن مصطلح الهندسة الاجتماعية يطلق عليها في السنوات الأخيرة مفهوم ذات شعبية كبيرة هو علم أو فن اختراق العقول نظرًا للنمو الهائل والمتسارع لشبكات التواصل الاجتماعي والبريد الإلكتروني والاتصالات الإلكترونية بكافة أشكالها حيث لاق هذا المصطلح استخدامًا واسع الانتشار خاصة في مجال

تاريخ استلام البحث : ١٧ أغسطس ٢٠١٩ ، تاريخ القبول : ٢٤ سبتمبر ٢٠١٩

أمن المعلومات الرقمية، حيث أصبح هذا المصطلح مستخدمًا للإشارة إلى مجموعة من الأساليب التي قد يستخدمها المخترقون في حصولهم على المعلومات الخاصة بضحاياهم أو محاولة إقناع ضحاياهم المستهدفَة بتنفيذ بعض الإجراءات التي تساعدهم على اختراق أنظمتهم الشخصية والحاق الضرر بها[١].

يعد نظام الحماية الذاتية والأمن الرقمي للمواطن أحد الركائز الهامة للمواطنة الرقمية حيث نجد حماية المواطن الرقمي من أهم الأولويات للأمن القومي للمواطن، ويتجلى هذا من خلال الإجراءات الوقائية والحماية الالكترونية وقوانين مكافحة الجرائم المعلوماتية؛ وخاصة مع انتشار ظاهرة اختراق العقول أو ما يطلق عليها مصطلح **"الهندسة الاجتماعية "** ويقصد بها **"** قدرة المخترق على الحصول على معلومات هامة وسرية باستخدام أسلوب من أساليب الاحتيال العقلي والتلاعب، حيث يتم من خلاله اقتحام شبكة ما أو نظام تشغيلي ما وذلك نتيجة الخطأ البشري فالهندسة الاجتماعية تكمن في البحث عن أي أخطاء بشرية من أجل أن يتمكن المستخدم من الحصول على غايته كالثقة الزائدة ،أو، الفضول ،أو، عدم التركيز؛ حيث تبدأ اللعبة أو الاختراق عند اكتشاف نقطة الضعف التي يتم الاستغلال من خلالها[٢] وهذا ما دفع الباحثة لإجراء هذه الدراسة حيث أصبحت مشكلة إعداد المواطن الرقمي إعداداً علمياً وعمليًا من أهم التحديات التي تواجه المجتمعات في الوقت الحاضر.

أهمية الدراسة :

أصبح مبدأ احترام خصوصية المستخدم من الأمور التي تؤرق من يتعامل مع التقنية والتكنولوجيا والاتصالات وحماية حساباتهم الشخصية وكيفية التصدي لعمليات الاختراق لحياتنا اليومية من خلال التقنيات الحديثة التي نعتمد عليها في جميع مناحي حياتنا وأصبح الاتصال بشبكة الانترنت اليوم حجر الزاوية في جميع معاملاتنا اليومية، وهنا يطرح السؤال نفسه كيف يمكننا تحقيق الأمن المعلوماتي التقني كأفراد؟ في حين تعمل المؤسسات جاهدة على حمايتها ألا أنها ما زالت غير أمنة حتى وقتنا الحاضر حيث يمكن اختراقها عن طريق الهندسة الاجتماعية التي باتت اليوم مصدرًا أساسيا لمعظم الهجمات الإلكترونية المجهولة المصدر والصعب تتبعها وتستمد الدراسة الحالية أهميتها من أهمية الهندسة الاجتماعية من جهة ومن الأمن المعلوماتي من جهة أخرى ودوره في رفع مستوى حماية واحترام الخصوصية والتعرف على الهندسة الاجتماعية وكيفية التصدي لهجماتها لشبكات التواصل الاجتماعي .

هدف الدراسة:

نظرا للدور الهام والمؤثر الذي تلعبه شبكات التواصل الاجتماعي في أنها تتيح للمستخدمين البحث والتواصل مع الآخرين بيسر وسهولة من خلال المواقع الإلكترونية العامة والحسابات الشخصية، فأضحت شبكات التواصل الاجتماعي اليوم من أقوى أدوات الاتصال الاجتماعي بين أفراد المجتمع حيث تؤكد الإحصائيات التزايد المستمر في استخدام هذه المواقع خاصةFacebook وTwitter وغيرهما من وسائل الاتصال الاجتماعي الأخرى حيث نجد أن استخدام شبكات التواصل الاجتماعي له آثار نافعة وإن كان في نفس الوقت له عواقب سلبية فهناك إجماع بين العديد من الباحثين على أن هذه الشبكات الاجتماعية قد فتحت عصرا جديدا من عصور الاتصال والتفاعل بين البشر، ألا أنها أيضا فتحت الباب على مصرعيه لمزيد من الانتهاكات للمستخدمين.

لذا تهدف هذه الدراسة إلى التعرف على مدى وعي المجتمع في الوطن العربي بحماية حساباتهم الشخصية ووقدرتهم في التعرف على سبل الاختراق وانتهاك الخصوصية بشكل عام مع التركيز على الهندسة الاجتماعية بشكل خاص وسبل التدريب المتاحة تجاه حماية المواطن الرقمي حيث تعتمد الهندسة الاجتماعية في المقام الأول على فن اختراق العقول وانتهاك خصوصية المستخدم أثناء استخدامهم لشبكات

التواصل الاجتماعي و تكنولوجيا المعلومات في حين تحاول أيضا الإجابة على سؤال رئيس في هذا السياق، وهو "كيف يتصرف الأفراد عندما يتعرضون لأي نوع من الاحتيال الهندسة الاجتماعية؟".

تساؤلات الدراسة:

تتركز مشكلة هذه الدراسة في التعرف على مفهوم الهندسة الاجتماعية والواقع الفعلي لتأثيرها على المجتمع في الوطن العربي باستخدام شبكات التواصل الاجتماعي التي أصبحت تشكل آلية في غاية الأهمية في عالم التواصل الالكتروني بين الأفراد والجماعات، والتي يتبادل الأشخاص فيها المعلومات والآراء والأفكار بكل حرية وبدون رقيب مما سهل عملية اختراقها بسهولة والاطلاع على محتوياتها من جانب أي مخترق مهتم بالحصول على معلومات عن المستخدمين، ويمكن استخدام تلك المعلومات في عدة أغراض تخدم مصالحه وبصورة متكررة. (٣)

قد أصبح من السهل وطبيعة التواصل عن طريق التواصل بالانترنت ومن خلال الشبكات الاجتماعية العديد من المستخدمين بتبادل معلوماتهم شخصية فيما بينهم أكثر من أي وقت مضى، مما فتح المجال لقراصنة المعلومات استغلال هذه المعلومات لمصالحهم الخاصة(٤).

هناك بعض التساؤلات تسعى هذه الدراسة إلى الإجابة عليها:

١- المقصود بمفهوم الهندسة الاجتماعية (فن اختراق العقول) ؟

٢- ما أهمية شبكات التواصل الاجتماعي في الوطن العربي؟

٣- ما أهمية الخصوصية من وجهة نظر مستخدمي شبكات التواصل الاجتماعي في الوطن العربي؟

٤- ما هي طرق اختراق شبكات التواصل الاجتماعي؟

٥- . ما هي طرق الحماية من الهندسة الاجتماعية؟

٦- مدى وعي المجتمع العربي تجاه الهندسة الاجتماعية؟

٧- مدى توافر مهارات التصدي لهجمات الهندسة الاجتماعية في شبكات التواصل الاجتماعي؟

٨- كيف يمكن تنمية وعي المجتمع العربي لحماية حساباتهم في شبكات التواصل الاجتماعي؟

مجال الدراسة وحدودها:

- **الحدود الموضوعية**: تتناول الدراسة التعرف على مفهوم الهندسة الاجتماعية وطرق التصدي لها في شبكات التواصل الاجتماعي والواقع الفعلي لمدى وعي المجتمع في الوطن العربي لها من خلال عينة عشوائية من أفراد المجتمع العربي من مستخدمى الإنترنت.
- **الحدود الزمنية**: تتمثل الحدود الزمنية لهذه الدراسة حتى يوليو ٢٠١٧ الخاصة بتجميع البيانات اللازمة لإجراء الدراسة من خلال توزيع الاستبانة على مفردات العينة في الوطن العربي.
- **الحدود الجغرافية**: تشمل الدراسة عينة من أفراد المجتمع المتفاعلين مع الإنترنت بصفة عامة، والمتفاعلين مع شبكات التواصل الاجتماعي في الوطن العربي بصفة خاصة.

منهج الدراسة وأدوات جمع البيانات:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، وقد تم استخدام هذا المنهج حيث يعد ملائماً لطبيعة وأهداف هذه الدراسة.وقد استعانت الدراسة بالاستبانه كأداة لجمع البيانات[٥]، بهدف الحصول على صورة تعبر عن مدى وعي المجتمع العربي بالهندسة الاجتماعية وفن اختراق العقول من خلال شبكات التواصل الاجتماعي وكيفية التصدي لها.

عينة الدراسة :

تم الاستعانة بالاستبانه الالكترونية وطرحها بشكل رقمي تستهدف مستخدمي الشبكات الاجتماعية في الوطن العربي لقياس مدى وعيهم بالهندسة الاجتماعية سبل حمايتهم، نظرًا لصعوبة الحصر الدقيق لمجتمع الدراسة، لجأت الباحثة إلى العينة العشوائية البسيطة **Simple Random Sample**: هذا النوع من العينات يعتمد على تكافؤ الفرص لجميع عناصر المجتمع لتكون أحد مفردات العينة، ويتطلب استخدام هذه الطريقة ضرورة حصر ومعرفة كامل العناصر التي يتكون منها مجتمع الدراسة، وقد تم طرح الاستبانة بمواقع التواصل الاجتماعي فبراير ٢٠١٧ لمدة شهر ومرة أخري شهر يوليو وقد تم تلقي ورود إجابات الاستبانة وعددها (٣٨٢) استبانة تم استبعاد (٤٦) استبانة غير صالحة للدارسة. ومن خلال تحليل هذه الاستبانات تبين أنها تغطي غالبية دول الوطن العربي في المقام الأول (جمهورية مصر العربية، والمملكة العربية السعودية، والعراق، وليبيا،...الخ)، بالإضافة إلى أنها اشتملت على عدة شرائح عمرية واجتماعية وثقافية وتعليمية. مما دفع الباحثة إلى استكمال الدراسة حيث تعد عينة الدراسة ممثلة لمجتمع الدراسة للخروج بمؤشرات صالحة.

الدراسات السابقة:

لقد تبين من خلال مسح الإنتاج الفكري في أدبيات الموضوع عن الكتابات المتصلة بموضوع الدراسة سواء من دراسات عربية وأجنبية في الأدلة والببليوجرافيات، اتضح ندرة الدراسات التي تتعلق بموضوع الهندسة الاجتماعية حيث توجد دراسات عربية مثيلة عديدة تتناول انتهاك الخصوصية والاحتيال الالكتروني والجرائم الالكترونية والجرائم المعلوماتية بشكل مباشر، بل أن الغالبية العظمى من الدراسات والأبحاث المتاحة تتناول قضايا الهندسة الاجتماعية من زوايا أخري على المستويين العربي والعالمي ومن أهم هذه الدراسات هى:

في عام ٢٠٠٤ رصد دراسة تهدف إلى قياس مدى وعي مستخدمين شبكة الانترنت بالهندسة الاجتماعية، حيث قام الباحثين بالادعاء أنهم ينتمون للمؤسسة كموظف في قسم الدعم الفني للحاسب الآلى في المؤسسة وطلب من الموظفين معلومات عديدة من بين تل المعلومات أسم المستخدم وكلمة المرور الخاصة بهم وكانت نتائج الدراسة التى تم التوصل إليها تثير القلق حيث أظهرت أن ما يقرب من٨٠٪ من المشاركين أفصحوا عن اسم المستخدم، في حين أن ما يقرب من ٦٠٪ أفصح عن كلمة المرور الخاصة بهم[٦]

في عام ٢٠٠٦ هناك دراسة تقيم مدى وعي المستخدمين للبريد الالكتروني تجاه الهندسة الاجتماعية حيث يعد استخدام البريد الالكتروني مجالاً لهجمات التصيد الالكتروني حيث ارسل الباحثون نحو ٢٠ رسالة بريد إلكتروني مشروعة وغير مشروعة؛ وطلب من المشاركين فيها التمييز بين رسائل البريد الإلكتروني المشروعة وغير المشروعة، وأظهرت النتائج وعي ١٧٩ فردًا بنسبة ٣٦% استطاعوا تحديد رسائل البريد الإلكتروني المشروعة، في مقابل ٤٥٪ تمكنوا في اكتشاف رسائل البريد الإلكتروني غير المشروعة في حين المشاركين الذين حددوا رسائل البريد الإلكتروني غير المشروعة بشكل صحيح لم يتمكنوا من ذكر أسباب مقنعة لاختيارهم[٧].

في عام ٢٠٠٨ دراسة تهدف إلى التحقق من مستويات قابلية الموظفين تجاه الهندسة الاجتماعية وأجريت الدراسة على نحو ١٥٢ موظفا من موظفي جامعة بليموث بالمملكة المتحدة بإجراء تجربة عن طريق إرسال رسالة الكترونية إليهم، وطلب منهم إتباع الرابط المرسل وتثبيت تحديث البرامج وقد أظهرت النتائج لهذه التجربة أن نحو ٢٣٪ ممن تلقوا الرسالة الالكترونية تم مهاجمتهم بنجاح(٨).

وأجريت دراسة في عام ٢٠١٠ تهدف هذه الدراسة إلى قياس وعي الموظفين والطلاب في الجامعة الأميركية بالشارقة تجاه الهندسة الاجتماعية حيث أجرى الباحثين تجربتان من أجل تحقيق هدف الدراسة حيث تتمثل التجربة الأولى في استخدام طريقة التصيد الالكتروني عن طريق إرسال رسائل بريد إلكتروني وهمية لجميع الموظفين والطلاب، ووفقا للنتائج، بلغ عدد الضحايا من الذكور٤٨٥ و من الإناث ٤٦٩ من أجمالى مجتمع الدراسة البالغ عددهم ٥١٦٦ طالبا و نحو ٣٥١ موظفًا والتجربة الثانية تم خداع الأشخاص المستهدفين عن طريق إرسال بريد إلكتروني مزيف ، وطلب منهم إرسال معلوماتهم الشخصية للمشاركة في استطلاع بحثي أجرته الجامعة الأمريكية، مع التأكيد على أن أي مشارك يجري الاستطلاع سيحصل على **USB Flash Drive** فكان عدد الضحايا في هذه التجربة أقل بكثير من من التجربة السابقة حيث لم يكن هناك سوى ٢٢٠ استجابة للبريد الإلكتروني المزيف ومن المثير للاهتمام أن تحليل النتائج كشف عن وجود عدد كبير من الضحايا بين الطلاب في السنوات المتقدمة؛ بالمقارنة مع الطلاب الجدد(٩).

أما في عام ٢٠١١ اجريت دراسة استعرضت فيها أنه على الرغم من أن معظم المؤسسات في جميع أنحاء العالم تولي اهتماماً متزايدًا في الأونة الاخيرة في تأمين نظم المعلومات عن طريق استخدام أدوات أمنية متطورة، ينتج عنها نظم المعلومات الخاصة بهم لا يمكن اختراقها مما دفع القراصنة للجوء إلى استخدام الهندسة الاجتماعية بدلا من استخدام مهاراتهم التقنية للحصول على المعلومات وتهدف هذه الدراسة في إثبات أن مستخدمي نظم المعلومات يعدون التهديد الحقيقي لأنفسهم وأن عدم وعي المستخدمين بالهندسة الاجتماعية يجعل نظم المعلومات عرضة للمزيد من الانتهاكات كما تهدف إلى التعرف على ما إذا كان طلاب تكنولوجيا المعلومات لديهم قدر من الوعي بالهندسة الاجتماعية مقارنة بالطلاب من كليات أخرى وقد تم جمع البيانات اللازمة من ٢٤٥ طالبا من الجامعة الإسلامية الدولية في ماليزيا (**IIUM**)، من خلال استبيان الكتروني، بالإضافة إلى إجراء تجربة التصيد الهاتفي التي أجريت على عينة من تلك الطلاب وأظهرت النتائج أن نحو ١١٤ طالبا قد تعرضوا لهجمات الهندسة الاجتماعية خلال الستة الأشهر الماضية، وما يقرب من ٣٨٪ من هذه الهجمات تمت من خلال البريد الإلكتروني(١٠).

وفي العام نفسه أجريت دراسة على ٤٠ موظفا في **Federal Polytechnic, Ilaro, Ogun State, Nigeria** تهدف هذه الدراسة إلى قياس مستويات الوعي فيما يتعلق بالحماية من الهندسة الاجتماعية وقد أظهرت النتائج أن مستوى الوعي والحماية ضد الهندسة الاجتماعية لا يزال في مراحله الأولى ولذلك، اقترح الباحثون زيادة الوعي بين الموظفين تجاه الهندسة الاجتماعية(١١).

وأيضا في عام ٢٠١١ أجريت دراسة تقيم مدى وعي المستخدمين تجاه الهندسة الاجتماعية من طريق استخدام البريد الالكتروني كأحد مجالات هجمات التصيد الالكتروني حيث تم تقديم مجموعة من السيناريوهات الإلكترونية المشروعة وغير المشروعة إلى نحو ١٥٣ مشاركا من خلال دراسة استقصائية على شبكة الإنترنت وقد طلب من المشاركين تحديد أي من سيناريوهات البريد الإلكتروني والموقع الإلكتروني كانت شرعية أو غير شرعية وتوصلت الدراسة أن ٤٣٪ من بين المشاركين نجحوا في تحديد رسائل البريد الإلكتروني المشروعة بشكل صحيح، وبالإضافة إلى ذلك، قدمت شهادة معتمدة على شبكة الإنترنت في الدراسة وطلب من المشاركين الإشارة إلى ما إذا كانوا قد تحققوا من أي وقت مضى للحصول على شهادة معتمدة على شبكة الانترنت وكان من المطلوب من المشاركين الذين أجابوا بالإيجاب أن يشيروا إلى كيفية تحديد موقع شهادة موقع على شبكة الانترنت وعلاوة على ذلك، سئل المشاركون في

الاستقصاء عما إذا كانوا يعرفون أهمية شهادة موقع على شبكة الانترنت وكشفت نتائج الدراسة عن نقص واضح في الوعي لدى غالبية الخاضعين للدراسة بسبب نسبة كبيرة من سوء تصنيف رسائل البريد الإلكتروني والمواقع الإلكترونية وبالإضافة إلى ذلك، كشفت النتائج أن تحديد المؤشرات الأمنية مثل شهادة موقع على شبكة الانترنت غير فعالة ضد التصيد الاحتيالي كما ذكر غالبية الخاضعين للدراسة أنهم لم يتحققوا من شهادة موقع على شبكة الانترنت ولا يعرفون أهميته ومع ذلك كشفت النتائج أن هناك من اعتمد على **(EV SSL) An Extended Validation SSL Certificate** كمؤشر أمني فعال جدا ضد التصيد الاحتيالي والتحقق من الشهادة ويتضح جليا مما سبق أن جميع الدراسات التي تم عرضها أن هناك نسبة كبيرة من المجتمع مازال عرضه للهجوم والتصيد بإتباع أساليب الهندسة الاجتماعية، وأن عدم وجود الوعي الكافي في مجال الهندسة الاجتماعية بين أفراد المجتمع هو السبب الرئيسي وراء هذه المشكلة [١٢].

مصطلحات ومفاهيم:

الشبكات الاجتماعية:

قاموس Online Dictionary for Library and Information Science عرف الشبكات الاجتماعية هي عبارة خدمة إلكترونية تتيح للعديد من المستخدمين بإنشاء وتنظيم ملفات شخصية لهم، كما تتيح لهم أيضًا بالتواصل الالكتروني مع مستخدمين آخرين[١٣].

وتعرف الموسوعة البريطانية الشبكات الاجتماعية بأنها عبارة عن مواقع الكترونية يتشارك فيها أعضائها في حياتهم الاجتماعية والتواصل الاجتماعي فيما بينهم، ويتفاعلون مع بعضهم البعض لينتج مجتمعا أفتراضيًا؛ يعبرون فيه بحرية عن آرائهم وتطلعاتهم المستقبلية[١٤].

الخصوصية:

عرف قاموس Online Dictionary for Library and Information Science الخصوصية معتمدًا على القانون الذي وضعته جمعية المكتبات الأمريكية حيث تنص على أن حرية المستفيد تتمثل فى حصوله على الخدمات والمعلومات التي يحتاجها بمساعده أمناء المكتبات دون محاولة التدخل في الأسباب التي دفعت المستفيد إلى طلب هذه المعلومات، ويجب احترام تفكيره وحقوقه في حصوله على ما يريد في الوقت المناسب له دون تدخل من الآخرين[١٥].

الاختراق:

يقصد **بالاختراق** هو عبارة عن إعادة تنظيم وترتيب نظام موجود مسبقًا أو موارد شبكة بطريقة تتسم بالمهارة والذكاء، والمخترق هنا ليس بالضرورة أن يكون مجرم تقني، وعرف الاختراق أيضًا بأنه عبارة عن عمل يتم انجازه سريعا يحرز نتائج دون اتباع أي إجراءات منظمة وقد ينتج عن الاختراق تحسين النظام الموجود حيث يقوم المخترق بتعديل البرامج بلا تفويض من الجهات المعنية بتلك البرامج وذلك بتغيير الكود ذاته ولكن عملية الدخول على الأنظمة بدون وجه حق **Hacking** والوصول إلى البرامج والملفات والبيانات وغيرها بهدف التخريب أو السرقة أو التلاعب في محتويات نظام معين ،فإن محترفي الحاسب الآلى يطلقون على من يقوم بهذه العمليات اسم مخرب أومخترق أو محطم **Cracker**[١٦]

الاحتيال:

الاحتيال هو عبارة عن الاستيلاء على مال الغير عن طريق خداعه وجعله يقوم بتسليم ذلك المال طواعية والاحتيال يأتي بالاعتداء على حق الملكية أيا كانت ويتميز الأسلوب الذي يتحقق عن طريقه هذا الاعتداء ذلك أن المحتال يصدر عنه فعل الخداع من نوع ما حدده القانون فيترتب عليه وقوع المجني عليه

في الغلط وإقدامه على تصرف مالي أوحى به إليه المحتال وجعله يعتقد أنه في مصلحته أو في مصلحة غيره ومن شأن هذا التصرف تسليم مال إلى المحتال الذي يستولي عليه بنية تملكه. (١٧)

التصيد الالكتروني:

يعرف التصيد بأنه عبارة عن عملية احتيالية يتم فيها الحصول على معلومات شخصية أو معلومات سرية كمعلومات بطاقات الائتمان أو اسم المستخدم، أو كلمة المرور عن طريق الإيهام بأنه كيان يمكن الوثوق فيه في البيئة الرقمية(١٨).

الجرائم الإلكترونية:

تعرف الجرائم الإلكترونية **(Electronic crime "or" e-crime)** بأنهاعبارة عن مجموعة من الممارسات التي توقع ضد فرد أو مجموعة مع توفر دافع إجرامي يهدف إلى التسبب بالأذى لسمعة الضحية عمداً، أو إلحاق الضرر النفسي والبدني به سواءً أكان بأسلوب مباشر أو غير مباشرعن طريق الاستعانة بشبكات الاتصال الالكترونية كشبكة الانترنت وغيرها على سبيل المثال لا الحصر البريد الإلكتروني، وغرف المحادثة، والهواتف المحمولة وغيرها(١٩)

مفهوم الهندسة الاجتماعية :

هو عبارة عن أسلوب من أساليب الاختراق التي تعتمد في المقام الأول على العنصر البشري تماما وليس لها أيه متطلبات تقنية خاصة حيث يستخدم المخترق مهاراته الشخصية في التواصل مع الآخرين ويستعمل فن الخداع والكذب ليحصل منهم على معلومات ذات طابع تقني تمكنه بواسطتها قيامه بعملية الاختراق وفي الأغلب تتم هذه العملية من خلال المحادثات الهاتفية(٢٠)

مصطلح **الهندسة الاجتماعية** كمصطلح قد يوحي للوهلة الأولى أنه شكل من أشكال الهندسة المتعارف عليها التي عمرت الحياة البشرية، ألا أنه في حقيقة الأمر هو خطر يحيط بالمعلومات الشخصية للمواطن كفرد وأمن معلومات القطاع الحكومي والخاص من كلِّ جهة وفقا لتقرير المخابرات الأمنية الماليزية والتي أعلنت عنه شركة مايكروسوفت في ١٢ مايو ٢٠١١ الذي يتضمن أن" مجرمي الإنترنت يستخدمون في هجماتهم أساليب تتسم بالسهولة من بينها أساليب الهندسة الاجتماعية والاستفادة من المكاسب التي أنشأتها المجرمين الأكثر مهارة لاتخاذ مبالغ مالية صغيرة من عدد كبير من الأشخاص "(٢١).

وليس لمصطلح الهندسة الاجتماعية **Social Engineering** تعريف أو مفهوم متفق عليه، وأن كان أقرب تلك التعريفات: " أنه عبارة عن استخدام المخترق لمجموعة من الحيل النفسية من شأنها خداع مستخدمي الحاسب الآلي تمكنه من الوصول إلى أجهزة الحاسب أو المعلومات المخزنة فيها كنتيجة لما قد يتوهم به بعض الناس، فإن الهندسة الاجتماعية يجب أن تكون على رأس قائمة وسائل الاختراق والهجمات الالكترونية التي يتوجب علينا حماية المعلومات منها(٢٢). وهناك العديد من المصطلحات التى تطلق على الهندسة الاجتماعية منها " مصطلح الخدع الاجتماعية، مصطلح الاحتيال الصوتي، مصطلح الاحتيال الإلكتروني، مصطلح المهندس الاجتماعي"(٢٢).

ونعرف الهندسة الاجتماعية بأنها عبارة عن "أي عمل يؤثر على الشخص في اتخاذ إجراء قد يكون أو لا يكون في مصلحتهم عن طريق استخدام مجموعة من التقنيات تجعل الناس يقومون بعمل ما أو يفشون معلومات سرية خاصة بهم. وعلى الرغم من أننا نركز على الأشكال التقنية إلا أنه من المهم أن نفهم الجوانب الفسيولوجية، والجوانب النفسية، للتأثير على شخص بشكل عام. ويمكن أيضا استخدام نفس المبادئ التي تستخدم في المعنى الإيجابي بشكل ضار(٢٣).

أنواع الهندسة الاجتماعية

انتحال الهوية: عادة تتطلب الهندسة الاجتماعية شكلاً من أشكال انتحال الهوية لكسب ثقة الشخص المستهدف ويستخدم في كثير من الأحيان انتحال شخصية دعم تكنولوجيا المعلومات الذي يحدث يقوم بالتحقق من الشبكة، ويطلب كلمة مرور، أو يطلب تحميل برمجيات معينة[٢٤]

النوع الثاني وهو **التصيد الاحتيالي**: عبارة عن عمل احتيال قد ينتج عنه ملاحقه قضائية فهو عملية يتم استخدامها للحصول على معلومات شخصية للأفراد عن طريق إدعاؤه ككيان موثوق به في أي تبادل للمعلومات كرسالة بريد الكتروني من بنك أو شركة ائتمان تطلب التحقق من معلوماتك الشخصية[٢٥]

النوع الثالث يطلق عليه **الاحتيال الصوتي** عبر الهاتف يحدث هذا عندما يكون الأفراد لا يدركون قيمة المعلومات التي يمتلكونها. وهذا يمكن أن يتم ذلك بعدة طرق منها أدلة سياسة الشركة، وكذلك دفتر الهاتف للشركة[٢٦].

المهندس الاجتماعي:

الهدف من الاختراق عموماً بغض النظر عن الطريقة المستخدمة هو الحصول على المعلومات الشخصية والسرية أياً كان نوعها. وهنا يأتي دور الهندسة الاجتماعية في عملية الاختراق عن طريق شخص يطلق عليه المهندس الاجتماعي؛ حيث يتمتع هذا المهندس الاجتماعي بمهارات اجتماعية وتقنية عالية ولدية القدره على التمثيل والخداع وإقناع الضحية بشكل غير مباشر بشتى الطرق للوصول إلى المعلومات المطلوبة. وتختلف الطرق المستخدمة في الهندسة الاجتماعية منها على سبيل المثال لا الحصر أن المهندس الاجتماعي قد يتصل بأحد عملاء البنك منتحل شخصية موظف بنك ويقوم بطريقته الخاصة بالحصول على المعلومات والبيانات البنكية وهذه الطريقة منتشرة على نطاق واسع وخاصة بين كبار السن. أو طريقة اخري بحيث ينتحل شخصية عامل صيانة أجهزة وشبكات حاسب إلى أو يعمل بشكل مؤقت في إحدى المؤسسات من بين الموظفين الذين لديهم صلاحيات الدخول لأنظمة المؤسسة[٢٧] .

أقسام الهندسة الاجتماعية: [٢٨]

تصنف جرائم الهندسة الاجتماعية إلى صنفين:

الهندسة الاجتماعية القائمة على أساس تقني:

هي برامج وتقنيات تساعد المخترق للوصول للمعلومات ومن أمثلة ذلك :

١. **الاحتيال الالكتروني phishing:** يعد الاحتيال الالكتروني من أهم الطرق المتبعة في الهندسة الاجتماعية، والاحتيال الالكتروني عن طريق ارسال رسالة بريد الكتروني من شركة ائتمان أو بنك تطلب التحقق من معلوماتك وتتضمن هذه الرسالة على رابط صفحة ويب مشابهة تماما للموقع الرسمي للشركة إلا أنها صفحة احتيالية، وهذه الصفحة تطلب منك إدخال اسم المستخدم وكلمة المرور ومن ثم توجهك للصفحة الصحيحة بعد أن حصلت منك على كافة بياناتك السرية.

٢. **الاحتيال الصوتي Vising**: أكثر هجمات الهندسة الاجتماعية استخدامًا للهاتف. حيث يتصل المهاجم مدعياً أنه شخص له صلاحيات ويقوم تدريجياً بالحصول على المعلومات من الضحية طواعية[٢٩]. يعتمد هذا النوع على برنامج **War Dialler** وهو برنامج يقوم بالاتصال بالعديد من أرقام الهواتف المختلفة في المنطقة وبعد الاتصال يقوم المخترق بانتظار ضحاياه، ويبدأ الخطر من لحظة رفع السماعة والإجابة على الرسالة الآلية التي تخبره أن بطاقته الائتمانية تخضع

لسرقة وعمليات احتيالية طالب منك رقم البطاقة وبعض البيانات السرية وحينها يحصل المخترق على ما يريده من معلومات سرية.

٣. **الرسائل الاقتحامية المزعجة Spam**: هي رسائل الكترونية بعناوين مشوقة للقراءة مثل تهنئة من صديق أو تأكيد بيع أو غيرها وبداخل تلك الرسائل ما ينتج عنها الحصول على المعلومات الشخصية أو تدمير جهاز الحاسب الالى.

٤. **البرامج الهامة:** وهي ما نشهده في بعض المواقع من روابط تحميل برامج ولكنها تكون مدعومة بكلمات احتيالية اقناعية عن أهمية ذاك البرنامج للجهاز وبمجرد تحيل الرابط يتم سرقة المعلومات الحساسة(٣٠).

<u>الهندسة الاجتماعية القائمة على أساس بشري أو إنساني:</u>

جرائم تعتمد على الإنسان وأن صح الوصف فهي جرائم من الإنسان وللإنسان دون تدخل التقنية بينهم ومن أمثلة ذلك:

١. **الإقناع:** فمن خلال التحدث مع الضحية وتشجيعها على الافصاح بمعلومات سرية أو ذو علاقة بهدف المخترق وذلك من خلال ترك انطباع جيد لدى الضحية بالعديد من الأساليب لإقناع الضحية بالسماح للمخترق الحصول على المعلومات التي يريدها.

٢. **الهندسة الاجتماعية المعاكسة:** وهي عن طريق وهم الضحية بأنك شخص مهم أو ذو صلاحيات عليا بحيث يقوم المهاجم بالافصاح بمعلومات يريدها الضحية وبمجرد نجاح الأمر وسارت الأمور كما خُطط لها من قبل المخترق يبدأ في انتهاز أكبر فرصة له تمكنه الحصول على معلومات ذات قيمة كبيرة من الضحية، وهذا الأسلوب معقد نسبياً كونه يعتمد على مدى التحضير المسبق وحجم المعلومات الصحيحة التي بحوزة المخترق قبل بدء عملية الاختراق(٣١)

٣. **الانتحال:** يتم الانتحال في الأغلب عبر الهاتف عن طريق عدة سيناريوهات مختلفة تستهدف شيئا ما، فهي لا تتطلب الحضور وجها لوجه ولكنها تتطلب بعض المعلومات مثل الاسم أو تاريخ الميلاد وغيرها. (٣٢)

٤. **سلة المهملات:** يمكن الحصول على الكثير من المعلومات الهامة عن المؤسسة من خلال سلة المهملات للاشخاص المنتمون للمؤسسة (٣٣). أن رمي أى ورقة غير مرغوب فيها دون تمزيقها في سلة المهملات حيث تعد سلة المهملات ذات أهمية للمخترق في سرقة بياناته من أجل إقناع ضحيته فيما بعد للحصول على المعلومات السرية للمؤسسة، بالإضافة إلى ذلك أن معظم المؤسسات تعتقد أن مسح بيانات الأقراص تكفي لازالة البيانات عليها تماما ولكن هناك طرق تقنية عديدة لاستعادة تلك البيانات بعد مسحها.

٥. **التجسس والتصنت:** يتم التجسس والتصنت عن طريق مراقبة الضحية حين كتابتها أو التصنت والاستماع لمحادثة هاتفية لسرقة كلمة المرور ومعلومات مهمة خاصة بها ، لذا يتعين تجنب كتابة كلمات المرور والمعلومات المهمة على ورق ووضعها تحت لوحة المفاتيح(٣٤)

الطرق التي يمكن من خلالها اختراق الحسابات الشخصية يمكن حصرها في تطبيقات الطرف الثالث المستخدمة في حساباتنا، صفحات تسجيل الدخول المزيفة، السماح للمتصفح بحفظ كلمات المرور، تخمين كلمة المرور، تخمين الإجابات لاستعادة كلمة المرور(٣٥)

النصائح التي يجب مراعاتها لتجنب الوقوع ضحية للهندسة الاجتماعية: [٣٦]

١. عدم الوثوق بأي مكالمة هاتفية أو بريد الكتروني من أي شخص يطلب فيها معلومات شخصية أو بنكية ويجب التأكد من هوية هذا الشخص عن طريق الاتصال بالبنك أو الجهة المنتمى لها الشخص للتحقق من هويته.

٢. تجنب استخدم البطاقة الائتمانية في المواقع الالكترونية إلا عند الضرورة القصوى، ويفضل استخدام البطاقات مسبقة الدفع بدلا عنها .

٣. يفضل عدم اتاحة المعلومات الشخصية على الانترنت مثل الاسم واللقب ورقم الجوال أو أي معلومات بنكية.

٤. التأكد من تمزيق وإتلاف الأوراق والمستندات المهمة بواسطة أجهزة مخصصة.

٥. تجنب كل الرسائل الإلكترونية التي تحتوي على روابط مشبوهة في البريد الالكتروني أو رسائل الجوال أو على المواقع الاجتماعية.

الجانب التطبيقي :

فيما يتعلق بمدى **وعي مستخدمي شبكات التواصل الاجتماعي في المجتمع العربي بالهندسة الاجتماعية** أجريت الدراسة على عينة من مستخدمي شبكات التواصل الاجتماعي في الوطن العربي والتي تم استجابتها كعينة عشوائية من خلال طرح استبانه إلكترونية حيث استجابت عينة قدرت بـ ٣٣٦ مفردة كانت خصائصها كما يوضحها الجدول التالي رقم[٣٧]:

جدول رقم (١) السمات الشخصية لعينة الدراسة

السمات الشخصية لعينة الدراسة		ع	%
الجنس	ذكر	١٨٠	% ٥٣,٦
	أنثى	١٥٦	% ٤٦,٤
المجموع الكلى		٣٣٦	١٠٠
العمر	أقل من ٣٠ سنة	٥٢	%١٥,٥
	من ٣٠ إلى ٣٩ سنة	١٢٤	% ٣٦,٩
	من ٤٠ إلى ٤٩ سنة	١٤٨	% ٤٤,٠
	من ٥٠ إلى ٥٩ سنة	٨	% ٢,٤
	من ٦٠ سنة فأكثر	٤	% ١,٢
المجموع الكلى		٣٣٦	١٠٠
المستوى التعليمي	ابتدائي	٣	% ٠,٩
	إعدادي	٢١	% ٦,٢٥
	ثانوي	٤٩	% ١٤,٩
	دبلوم	٤٥	% ١٣,٤
	شهادات عليا	١٤٩	% ٤٤,٣
	ماجستير / دكتوراه	٦٩	% ٢٠,٥
المجموع الكلى		٣٣٦	١٠٠

السمات الشخصية لعينة الدراسة		ع	%
المهنة	موظف	١٦	% ٤,٨
	طالب	١٣٦	% ٤٠,٠
	معاشات	٢٨	% ٨,٣
	مهن حرة	٦٤	% ١٩,٠
	لا يعمل	٩٢	% ٢٧,٤
المجموع الكلى		٣٣٦	١٠٠
الجنسية	مصري	١٦٤	%٤٨,٨
	سعودي	١٣٢	%٣٩,٣
	عراقي	١٦	%٤,٧
	ليبي	١٢	% ٣,٦
	غير مبين	١٢	% ٣,٦
المجموع الكلى		٣٣٦	١٠٠

يختص الجدول رقم واحد ببيان السمات العامة لمجتمع الدراسة حيث كشفت النتائج أن ٥٣,٦% من المشاركين في الدراسة من الذكور، بينما نسبة المشاركات من الإناث بلغت ٤٦,٤ % وبفارق أقل من المشاركين الذكور، وفيما يتعلق بأعمار المشاركين كانت نسبهم كالتالي: من عمر ٤٠-٤٩سنة هي الأعلى بواقع ٤٤,٣ %، تليها نسبة من تتراوح أعمارهم بين ٣٠ – ٣٩ بنسبة ٣٦,٩ %، ثم من أعمارهم أقل من ٣٠سنة بنسبة بلغت ١٥,٥%، وبفارق واضح بلغت نسبة من أعمارهم من ٥٠-٥٩ سجلت ٢,٤%،وفي المرتبة الأخيرة فوق ٦٠سنة بنسبة ١,٢%.

كما يشير الجدول إلى نسبة عينة الدراسة بحسب المهنة حيث جاء في المرتبة الأعلى الطلاب بمختلف مراحلهم التعليمية مدارس وجامعات بنسبة بلغت ٤٠,٠ %؛ والجدير بالذكر أنه هذه الفئة يجب أن تحظى بالتوعية والتدريب المناسب لحماية حساباتهم من الاختراق والانتهاك[٣٨] حيث تمثل السواد الأكبر من مستخدمي شبكات التواصل الاجتماعي، يليه بنسبة ٢٧,٤ % لا يعملون ،ثم المهن الحرة بنسبة ١٩,٠ %، وقبل الأخير أصحاب المعاشات بنسبة ٨,٣ %، بعدها الموظفون بنسبة ٤,٨%، أما فيما يتعلق بالمستوى التعليمي رصدت الدراسة ١٤٩ مفردة تمثل نسبة ٤٤,٣ % حاملي شهادات عليا (بكالوريوس/ ليسانس)، تليها نسبة ٢٠,٥ % للحاصلين على درجة الماجستير أو الدكتوراه، ثم تتقارب النسب للمرحلة الثانوية والدبلوم بفارق ضئيل لا يتعدى ١,٥ % ثم المرحلة الإعدادية وتسجل أدني نسبة وهى ٠,٩ نجدها تخص المرحلة الابتدائية

وبما أن الجمهور المشارك في الدراسة كان من مستخدمي شبكات التواصل الاجتماعي بشكل عام في العالم العربي فقد تم تحديد جنسيات المشاركين في الدراسة، ورصدت النتائج النسبة الأعلى من للجنسية المصرية بنسبة ٤٨,٨%، يليهم المشاركين السعوديين بنسبة بلغت ٣٩,٣%، ثم العراقيين بفارق كبير يتبين من النسبة التي لم تتجاوز ٤,٧%، وبنسبة متساوية هي الأقل اشترك من لم تتحدد جنسيتهم و المشاركين الليبيين بنسبة ٣,٦ %.

مدى الوعي بالهندسة الاجتماعية (فن اختراق العقول):

جدول رقم (٢) درجة الوعي بالهندسة الاجتماعية والمفاهيم ذات الصلة

م		درجة كبيرة		درجة متوسطة		درجة قليلة	
		ع	%	ع	%	ع	%
١	الهندسة الاجتماعية	٣٣	% ٩,٨	٦٧	١٩,٩ %	٢٣٦	٧٠,٢ %
٢	فن اختراق العقول	٥٢	١٥,٥ %	١٩٨	٥٨,٩ %	٨٦	٢٥,٦ %
٣	انتهاك الخصوصية	٨١	٢٤,١ %	١٨٥	٥٥,٠ %	٧٠	٢٠,٨ %
٤	الامن المعلوماتي	٥٢	١٥,٥ %	٨١	٢٤,١ %	٢٠٣	٦٠,٤ %
٥	الاختراق الرقمي	٧٦	٢٢,٦ %	١٧٩	٥٣,٢ %	٨١	٢٤,١ %
٦	انتحال الهوية	٥٢	١٥,٥ %	١٩٨	٥٨,٩ %	٨٦	٢٥,٦ %
٧	التصيد الالكتروني	٣٣	% ٩,٨	٦٧	١٩,٩ %	٢٣٦	٧٠,٢ %
٨	الاحتيال الالكترونيphishing	٢٣٦	٧٠,٢ %	٦٧	١٩,٩ %	٣٣	% ٩,٨
٩	الاحتيال الصوتي Visingعبر الهاتف	٣٣	% ٩,٨	٢٣٦	٧٠,٢ %	٦٧	١٩,٩ %
١٠	الرسائل الاقتحامية المزعجةSpam	٧٦	٢٢,٦ %	١٧٩	٥٣,٢ %	٨١	٢٤,١ %

ويشير الجدول رقم (٣) إلى مدى درجة الوعي بالهندسة الاجتماعية والمفاهيم ذات الصلة لدى المشاركين في الدراسة، حيث تم توجيه سؤال لهم حول درجة استيعاب وفهم مفهوم الهندسة الاجتماعية وغيرها من المفاهيم وثيقة الصلة، وكانت النتائج تشير في مجملها إلى قلة إدراكهم بما يعني مفهوم الهندسة الاجتماعية والتصيد الالكتروني حيث سجلت نسبة كل منهما ٧٠,٢%، والأمن المعلوماتي نسبة ٦٠,٤ %، ومن أفاد أنه يعي ماذا يقصد بالاحتيال الصوتي Vising عبر الهاتف بدرجة متوسطة نسبة قدرها ٧٠,٢ %، تليها نسبة ٥٨,٩ % لكل من أفاد أنه على درجة وعي متوسطة بمفهوم "فن اختراق العقول، انتحال الهوية "ويرجع السبب في ذلك إلى شيوع مصطلح الانتحال الهوية والشخصية وما إلى ذلك تليها نسبة ٥٥,٠ % تخص " انتهاك الخصوصية " ، وتقل النسبة تدريجي لكل من" الاختراق الرقمي، الرسائل الاقتحامية المزعجة Spam" حيث سجل كل منهما ٥٣,٢ % كنتيجة منطقية للاستخدام الواسع للبريد الالكتروني، وإذا انتقلنا لمن على دراية وعلم بمفهوم الهندسة الاجتماعية والمفاهيم المرتبطة بدرجة كبيرة تدني النسب بشكل عام حيث نجد أعلى نسبة سجلها الاحتيال الالكتروني phishing قدرها ٧٠,٢ %، في حين تنخفض بقية النسب انخفاضًا ملحوظًا ليصل إلى ٢٤,١ % فيما يخص انتهاك الخصوصية . ومن استعراضنا لما سبق يتضح ضرورة العمل على رفع وعي المجتمع العربي بمفهوم الهندسة الاجتماعية

والمفاهيم وثيقة الصلة حتى يتمكنوا من حماية حساباتهم على شبكة الانترنت بصفة عامة وشبكات التواصل الاجتماعي بصفة خاصة.

وننتقل إلى التعرف على استخدام مجتمع الدراسة لشبكات التواصل الاجتماعي لنتعرف عن قرب عن اتجاهاتهم نحو الإفصاح عن بياناتهم الشخصية فهذا ما يوضحه الجدول التالي:

جدول رقم (٣) استخدام شبكات التواصل الاجتماعي

م		نعم		لا		احيانا	
		ع	%	ع	%	ع	%
١	هل تسجل في الشبكات الاجتماعية باسمك الحقيقي	٤٥	%١٣,٤	١٧٩	%٥٣,٢	١١٢	٣٣,٣ %
٢	هل تتيح بياناتك الشخصية على شبكات التواصل الاجتماعي	٣٧	%١١,٠	٢٥١	%٧٤,٧	٤٨	١٤,٢ %
٣	هل بياناتك الشخصية المتاحة على شبكات التواصل الاجتماعي صحيحة	٦٧	١٩,٩ %	٢٢٧	%٦٧,٥	٤٢	١٢,٥ %
٤	هل تتيح صورك الشخصية وصور عائلتك على شبكات التواصل الاجتماعي	٣٧	%١١,٠	٤٨	%١٤,٢	٢٥١	٧٤,٧ %
٥	هل تمتلك معلومات كافية عن شبكات التواصل الاجتماعي	٢٨٣	٨٤,٢ %	١٥	%٤,٤٦	٣٨	١١,٣ %
٦	معلوماتك الشخصية على شبكات التواصل الاجتماعي سهلة الوصول إليها ولا تحتاج إلى حماية أمنية	١١٢	%٣٣,٣	١٧٥	%٥٢,١	٤٩	١٤,٦ %
٧	معلوماتك الشخصية على شبكات التواصل الاجتماعي يجب حمايتها فقط إذا كانت هناك محاولات لسرقتها	–	—	–	—	٣٣٦	١٠٠,٠ %
٨	معلوماتك الشخصية على شبكات التواصل الاجتماعي يجب حمايتها في كل وقت لتفادى سرقة الهوية	٣٣٦	١٠٠,٠ %	–	—	—	—
٩	تعتقد أنه يمكن نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي دون توخي الحذر	٦٨	٢٠,٢ %	٢٥١	%٧٤,٧	١٧	٥,٠٥ %
١٠	تعتقد أنه يمكن نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي مرتبط بالالتزام بقوانين الشبكات الاجتماعية	٩٦	%٢٨,٥	٢٨	%٨,٣	٢١٢	٦٣,١ %
١١	تعتقد أنه يمكن نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي طالما مقتصرا في نطاق العائلة والأصدقاء	٣٣٦	%١٠٠,٠	–	—	—	—

وعند قراءة الجدول السابق رقم (٣) يتضح لنا حماية مجتمع الدراسة لبياناتهم الشخصية بشكل تلقائي وبمعدل مرتفع حيث كانت النتائج إيجابية نحو سلوك مجتمع الدراسة تجاه حماية معلوماتهم الشخصية على شبكات التواصل الاجتماعي حيث أفاد ١٠٠,٠% بأنه يجب حماية معلوماتهم الشخصية ليس فقط إذا كانت هناك محاولات لسرقتها ، بل يجب حمايتها في كل وقت لتفادى سرقة الهوية ، وهذا ما وضحه

نسبة ٥٣,٢ % لا يسجلون بأسمائهم الحقيقة على شبكات التواصل الاجتماعي واختيار أسماء مستعارة غير حقيقة . وفي نفس السياق عدم إتاحتهم لبياناتك الشخصية على شبكات التواصل الاجتماعي سجلت نسبة قدرها ٧٤,٧ % ، وبالنسبة لمن يتيح بياناته الشخصية على شبكات التواصل الاجتماعي فتم سؤالهم عن مدى صحة هذه البيانات الشخصية فأجاب ٢٢٧ فردًا بعدم صحة بياناتهم الشخصية المتاحة على حساباتهم ويدل هذا على درجة وعيهم لحماية بياناتهم ، وأفاد نسبة ١١,٠% ممن يضع صوره الشخصية وصور عائلته على شبكات التواصل الاجتماعي وهذا يجعلنا نستفسر عن معلومات مجتمع الدراسة تجاه شبكات التواصل الاجتماعي فتبين ارتفاع نسبة من لديه خلفية معلوماتية عن شبكات الاتصال الاجتماعي سجلت ٨٤,٢ %، وبالنسبة للحماية الأمنية للمعلومات الشخصية على شبكات التواصل الاجتماعي بلغت نسبة من أفاد بأنها سهلة الوصول إليها ولا تحتاج إلى حماية أمنية ٥٢,١ %، بتوجيه سؤال عن عدم توخي الحذر تجاه نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي فأجاب ٢٥١ فردًا بنسبة ٧٤,٧ %بأنه يجب توخي الحذر عند النشر على شبكات التواصل الاجتماعي، كما سجل نسبة ٢٨,٥% أن نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي مرتبط بالالتزام بقوانين الشبكات الاجتماعية في المقام الأول. في حين سجل جميع مفردات مجتمع الدراسة أنهم يمكنهم نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي طالما مقتصرا في نطاق العائلة والأصدقاء دون الخوف من الاختراق وانتهاك خصوصياتهم أو الوقوع تحت اختراق عقولهم (ما نطلق عليه الهندسة الاجتماعية).

وتحاول الجداول التالية رصد الحالات التي تم تعرضها لانتهاك خصوصيتها واختراقها بالوسائل والأنواع المستخدمة في اختراق العقول " الهندسة الاجتماعية" فيوضح الجدول التالي رقم (٤) أنه على الرغم من وعي مجتمع الدراسة وحذرهم من الوقوع في براثن الانتهاك والاختراق ألا أنه أفاد نسبة ٥٣,٢ % تعرضت للتجسس والانتهاك لمعلوماته الشخصية على شبكة التواصل الاجتماعي وأيضًا تعرض البريد الالكتروني للاختراق ، تليها نسبة ٤٤,٠ % تعرضوا لسرقة هويتهم من خلال شبكات التواصل الاجتماعي ، وتقل النسبة لتصل إلى أقل نسبة وهى ٦,٨ % تعرض حساباتهم البنكية للاختراق ويشير ذلك إلى تعرضهم للهندسة الاجتماعية حيث يصعب الاختراق للحسابات المصرفية نظرًا لارتفاع معدلات أنظمة الأمن المعلوماتي للبنوك .

جدول رقم (٤) تعرضك لانتهاك خصوصيتك واختراقك

		نعم		لا	
		ع	%	ع	%
	هل تعرضت للتجسس ولانتهاك معلوماتك على شبكة التواصل الاجتماعي	١٧٩	٥٣,٢ %	١٥٧	%٤٦,٧
	هل تعرضت لسرقة الهوية من خلال شبكات التواصل الاجتماعي	١٤٨	%٤٤,٠	١٨٨	%٥٦,٠
	هل تعرضت لعملية التصيد الإلكتروني	٧٩	%٢٣,٥	٢٥٧	%٧٦,٥
	هل تعرض بريدك الالكتروني للاختراق	١٧٩	٥٣,٢ %	١٥٧	%٤٦,٧
	هل تعرض حساباتك البنكية للاختراق	٢٣	%٦,٨	٣٣٤	%٩٣,٢

والجدول رقم (٥) يرصد الطرق التي قد يتعرض لها مجتمع الدراسة للهندسة الاجتماعية ودرجة الاستجابة والوقوع ضحية لها.

جدول رقم (٥) في حالة تعرضك للهندسة الاجتماعية (فن اختراق العقول) أي الطرق التالية تعرضت لها ودرجة استجابتك لها

		نعم		لا	
		ع	%	ع	%
	انتحال الهوية والتحقق من الشبكة وتم طلب كلمات المرور الخاصة بك	٣٤	%١٠,١	٣٠٢	%٨٩,٩
	انتحال الهوية والتحقق من الشبكة وتم طلب تحميل برمجيات معينة على حاسبك الخاص	٧٩	%٢٣,٥	٢٥٧	%٧٦,٥
	الاحتيال عن طريق رسالة بريد الكتروني من شركة ائتمان/ بنك وتم طلب التحقق من معلوماتك	١٢	% ٣,٦	٣٢٤	%٩٦,٤
	الاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب التحقق من معلوماتك	٨٨	%٢٦,١	٢٤٨	%٧٣,٨
	الاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب عبر الرسالة الآلية بإدخال رقم بطاقتك الائتمانية	١٢	% ٣,٦	٣٢٤	%٩٦,٤
	الرسائل الاقتحامية المزعجةSpam كتهنئة من صديق	٢٥٩	%٧٧,١	٧٧	%٢٢,٩
	تحميل برامج من مواقع تقنعك بأهمية البرنامج	١٧٩	%٥٣,٢	١٥٧	%٤٦,٧
	تعرضك للتجسس والتصنت وسرقة كلمة المرور ومعلومات مهمة	٧٧	%٢٢,٩	٢٥٩	%٧٧,١
	تعرضك للانتهاك من خلال رمي أوراق مهمة وكلمة المرور في سلة المهملات بمكان العمل	٢٣	%٦,٨	٣٣٤	%٩٣,٢

يشير الجدول السابق رقم (٥) ارتفاع نسبة من تعرض للرسائل الاقتحامية المزعجة Spam كتهنئة من صديق وهى ٧٧,١ % وهذا يعد من أكثر الطرق شيوعًا، تليها نسبة ٥٣,٢ % يقعون ضحية اقتناعهم بأهمية برامج من مواقع توهمهم بضرورة تحميلها .وتنخفض النسب بشده لتصل لمن يقع تحت الاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب التحقق من معلوماته الشخصية بلغت ٢٦,١ %، ثم نسبة ٢٣,٥ % لمن تم انتحال هويته والتحقق من الشبكة وتم طلب تحميل برمجيات معينة على حاسبه الخاص ،وبأقل من ٠,٩% تخص من تعرض للتجسس والتصنت وسرقة كلمة المرور ومعلومات مهمة. وتستمر في الانخفاض الملحوظ حتى تسجل أقل نسبة وهى ٣,٦ % تخص كل من تعرض للاحتيال عن طريق رسالة بريد الكتروني من شركة ائتمان/ بنك؛ وتم طلب التحقق من معلوماته أو تعرض للاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب عبر الرسالة الآلية بإدخال رقم البطاقة الائتمانية.

ويرصد الجدول التالي رقم (٦) الطرق التي تم التعرض لها مجتمع الدراسة عبر شبكات التواصل الاجتماعي حيث تعرض نسبة ٥٦,٠ % لهجوم تخمين الإجابات كطرق استعادة كلمة المرور ويقصد بتخمين تخمين الإجابات كطرق استعادة كلمة المرور" أنه يقوم المخترق بمحاولة استعادة كلمة المرور الخاصة بك. وفي هذه الحالة سيظهر له سؤال الأمان الذي قمت أنت باختياره حتى تتمكن من خلاله باسترجاع كلمة مرورك في حالة فقدانها. للأسف الكثير يختارون أسئلة سهله مثل محل الميلاد، المنطقة التي تعيش بها ، اسم الأب وخلافه من هذه الأسئلة التي يمكن تخمينها بسهوله وهو ما يعرض حسابك للاختراق"[٣٩]. تليها نسبة ٤٦,٧ % من تعرض لهجوم صفحات تسجيل الدخول المزيفة (Phishing Attacks)" وهي صفحة تشبه صفحة الموقع الأصلي ، و الصفحة المزورة للفيس بوك ، هي صفحة تشبه

موقع الفيس بوك تماماً ، بحيث توهم المستخدم أنها في موقع الفيس بوك ، و في حال قيامه بإدخال معلومات حسابه في هذه الصفحة ، سيتم نقلها تلقائياً إلى الهكر و من ثم يخترق حسابه [٤٠]. في حين سجل نسبة من تعرض لتخمين كلمة المرور (Brute force attacks) ٢٦,١ % وتقل النسبة لتصل الى ١٤,٠ % لمن تعرضوا لهجوم كلمات المرور المسجلة في متصفحهم ، وأخيرًا نسبة ٦. % تخص من تعرضوا لهجوم برمجيات الطرف الثالث المستخدمة في حساباتهم (Third party Applications) ، وتري الباحثة أنه يجب التعريف بمثل هذه الوسائل المستخدمة للاختراق والتدريب عليها لحماية حساباتهم من تعرضها للاختراق والانتهاك حيث يعد ذلك مطلبًا ملحًا لكل من يستخدم الانترنت بشكل عام وشبكات التواصل الاجتماعي بشكل خاص.

جدول رقم (٦) في حالة اختراقك عبر شبكات التواصل الاجتماعي أي الطرق التالية تعرضت لها

		نعم		لا	
		ع	%	ع	%
	صفحات تسجيل الدخول المزيفة (Phishing Attacks)	١٥٧	٤٦,٧%	١٧٩	٥٣,٢ %
	برمجيات الطرف الثالث المستخدمة في حساباتنا (Third party Applications)	٢٣	٦,٨%	٣٣٤	٩٣,٢%
	تخمين كلمة المرور (Brute force attacks)	٨٨	٢٦,١%	٢٤٨	٧٣,٨%
	تخمين الإجابات كطرق استعادة كلمة المرور	١٨٨	٥٦,٠%	١٤٨	٤٤,٠%
	كلمات المرور المسجلة في متصفحك	٤٧	١٤,٠%	٢٨٩	٨٦,٠%

الخاتمة:

النتائج:

من خلال محاولة تحليل درجة وعي المجتمع العربي بالهندسة الاجتماعية وشبكات التواصل الاجتماعي، ولعل من أبرز ملامح هذه الصورة ما توصلت إليه من نتائج هي كما يلي:

١. أن مفهوم الهندسة الاجتماعية والتصيد الالكتروني تشير النتائج في مجملها إلى قلة إدراك مجتمع الدراسة بما يعني بالمفهوم والآثار المترتبة عليه. في حين مصطلح "فن اختراق العقول ، انتحال الهوية " قد لاقي رواجًا بين مجتمع الدراسة ويرجع السبب في ذلك إلى انتشار تلك المصطلحين.

٢. يتم حماية مجتمع الدراسة لبياناتهم الشخصية بشكل تلقائي وبمعدل مرتفع حيث كانت النتائج إيجابية نحو سلوك مجتمع الدراسة تجاه حماية معلوماتهم الشخصية على شبكات التواصل الاجتماعي.

٣. اختيار أسماء مستعارة غير حقيقة يسجل بها ما يزيد عن نصف مجتمع الدراسة على شبكات التواصل الاجتماعي وهذا ما وضحه نسبة ٥٣,٢ %. و عدم إتاحتهم لبياناتك الشخصية تارة وعدم صحة بياناتهم الشخصية المتاحة على حساباتهم تارة أخرى.

٤. أن الحماية الأمنية للمعلومات الشخصية على شبكات التواصل الاجتماعي وتوخي الحذر لمجتمع الدراسة تقع في المقام الأول لديهم ويدل هذا على درجة وعيهم لحماية بياناتهم.

٥. أن حرية نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي مقتصرا في نطاق العائلة والأصدقاء دون الخوف من الاختراق وانتهاك خصوصياتهم أو الوقوع تحت اختراق عقولهم (ما نطلق عليه الهندسة الاجتماعية).

٦. السبب الرئيس للاختراق يكمن في التجسس والانتهاك لمعلوماتهم الشخصية على شبكة التواصل الاجتماعي وأيضًا تعرض البريد الالكتروني للاختراق بنسبة ٥٣,٢ %.

٧. قلة من تعرض حساباتهم البنكية للاختراق حيث تعرض نسبة ٦,٨% فقط لاختراق الحسابات المصرفية.

٨. من أكثر الطرق شيوعًا لهجمات الهندسة الاجتماعية للرسائل الاقتحامية المزعجة Spam كتهنئة من صديق وهى ٧٧,١ % ، تليها نسبة ٥٣,٢ % يقعون ضحية اقتناعهم بأهمية برامج من مواقع توهمهم بضرورة تحميلها .

٩. يعد هجوم تخمين الإجابات كطرق استعادة كلمة المرور من أكثر الطرق التي تعرض لها مجتمع الدراسة عبر شبكات التواصل الاجتماعي حيث تعرض نسبة ٥٦,٠ % لهجوم تخمين الإجابات كطرق استعادة كلمة المرور.

١٠. برمجيات الطرف الثالث المستخدمة في حساباتهم (Third party Applications) سجلت أدني نسب في استخدامها لهجوم الهندسة الاجتماعية عبر شبكات التواصل الاجتماعي.

التوصيات:

في ضوء النتائج الموضوعية للدراسة وبناء على تحليل درجة وعى المجتمع العربي بالهندسة الاجتماعية "فن اختراق العقول " عبر شبكات التواصل الاجتماعي موضوع الدراسة توصى الباحثة بما يلي:

١. لابد من رفع درجة وعي المواطن العربي بالهندسة الاجتماعية وحماية حساباتهم الشخصية عبر شبكات التواصل الاجتماعي والحرص على نشر الوعي التقني.

٢. وضع استراتيجية عربية واضحة وميثاق أخلاقي تمكن المواطن العربي من التصرف بشكل نظامي مع الجهة المسئولة في حالة الوقوع ضحية للهندسة الاجتماعية.

٣. يجب أن تحظى الطلاب بقدر كافٍ من التوعية والتدريب المناسب لحماية حساباتهم من الاختراق والانتهاك وأن تتولى المدارس والجامعات الدورات التدريبية وورش عمل في هذا الشأن.

٤. لابد من تفعيل قوانين الجرائم الالكترونية وانتهاك الخصوصية بشكل فعال في الوطن العربي لمواجهة وردع الاختراقات والانتهاكات.

٥. لابد من صياغة قوانين عربية لحماية المستخدم من اختراق العقول وحساباتهم الشخصية عبر شبكات التواصل الاجتماعي.

مصادر الدراسة:

١. الهندسة الاجتماعية: اختراق العقول البشرية.

https://me.kaspersky.com/blog

2. https://www.security4arabs.com/2010/08/11/social-engineering /

٣. مركز الدراسات الإستراتيجية، المعرفة وشبكات التواصل الالكترونية، جامعة الملك عبد العزيز، العدد ٣٩، الرياض ٢٠١٢، ص ١٢٦.

٤. تريكي، حسان. "التهديدات الامنية المرتبطة بالاستخدامات السيئة لشبكات التواصل الاجتماعي ".مجلة الحقوق والعلوم الإنسانية - جامعة زيان عاشور بالجلفة - الجزائر ع ١٩ (٢٠١٤): ١٩٥ - ٢٠٤.

5. Orgill, G., Romney, G., Bailey, M., Orgill, P. (2004)"The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure", Computer Systems, Proceedings of SIGITE'04, Salt Lake City, UT 2004.

6. Karakasiliotis A, Furnell MS, Papadaki M."Assessing end-user awareness of social engineering and phishing", Proceedings of 7th Australian Information Warfare and Security Conference; 2006. pp. 60-72.

7. T.Bakhshi, M. Papadaki, and S. M. furnell, "A practical Assessment of social engineering Vulnerability", Proceeding of the second International Symposium on Human Aspects of Information Security & Assurance. (HAISA).2008.

8. Jamshaid Mohebzada, Ahmed El Zarka, Arsalan Bhojani, "An Awareness Study on Account Phishing, Spam Emails & Social Engineering Attacks", 2010, COE444 Spring 2010, Research Project Report.

9. Mutasim Elsadig Adam, etc.(2011) Awareness of Social Engineering Among IIUM Students .- World of Computer Science and Information Technology Journal (WCSIT) Vol. 1, No. 9, 409-413, 2011

10. Fagoyinbo, I.S, Akinbo, R.Y, Ajibode, I. A and Dosunmu, A. O. P, "Statistical analysis on the awareness and safeguarding against social engineering", Journal of Educational and Social Research, Vol. 1, No. 2, September 2011, pp 115-120.

11. Odaro, Ugiomo S. and Benjamin George Sanders. "Social Engineering : Phishing for a Solution."(2011).

http://www.kaspersky.com/images/odaro,_ugiomo_susan_sanders,_benjamin__social_engineering_phishing_for_a_solution-10-98480.pdf

12. ODLIS-Online Dictionary for Library and Information Science.

http://lu.co/odlis/index.cfm .

13. Encyclopedia Britannicaonline.- http://www.britannica.com/eb/blogs

14. ODLIS-Online Dictionary for Library and Information Science.

http://lu.co/odlis/index.cfm.

١٥. الشامي، أحمد محمد (٢٠٠٥). مصطلحات المكتبات والمعلومات والأرشيف /http://www.elshami.com

١٦. عبدو، سورية.(٢٠١٤) الاحتيال ، تعريفه ، أساليبه ، عقوبته .- الوحدة ع 8246

١٧. التصيد الالكتروني أنواعه وتقنياته .٢٠١٢

http://uaecyber.com

١٨. الحياري، إيمان(٢٠١٧) أنواع الجرائم الإلكترونية.

http://mawdoo3.com/

19. cole,Eric (2002). Hackers Beware: Defending your Network from the Willy Hacker .Indianapolis, Indianan: New Riders Publishing

20. Microsoft security Intelligence Report: Cybercriminals Targeting Consumers

http://www.cybersecurity.my/en/knowledge_bank/news/2011/main/detail/2032/index.html

٢١. القحطاني ، محمد عبد الله علي.أمن المعلومات بلغة ميسرة / محمد عبد الله علي القحطاني ، خالد سليمان عبد الله الغثير .- جامعة الملك سعود. مركز التميز لأمن المعلومات ، ١٤٢٩ . ص ٣١

٢٢. أحمد، عبدالخالق محمد. "الهندسة الإجتماعية ".المال والاقتصاد (بنك فيصل الاسلامي السوداني) - السودان ع٧٥ (٢٠١٤): ٢٢ - ٢٣ .

23. The Social Engineering Framework

https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

24. S. Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics," vol. 2006: SecurityFocus, 2001

25. Orgill, G., Romney, G., Bailey, M., Orgill, P. “The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure”, (2004) Computer Systems, Proceedings of SIGITE'04, Salt Lake City, UT 2004.

26. Karakasiliotis A, Furnell MS, Papadaki M. “Assessing end-user awareness of social engineering and phishing”, Proceedings of 7th Australian Information Warfare and Security Conference; 2006. pp. 60-72.

٢٧. **الزهراني ،أحمد عيضه (٢٠١٤). الهندسة الاجتماعية**

http://www.saudiacademics.com/article/computer-tech/item/1120

٢٨. أحمد ،عبد الخالق محمد، (٢٠١٤). مصدر سابق.

٢٩. الهندسة الاجتماعية Social engineering و أساليب الإختراق

https://ainkermesinfo.blogspot.com.eg/2016/01/social-engineering.html

٣٠. أحمد ،عبد الخالق محمد. (٢٠١٤). مصدر سابق.

٣١. الهندسة الاجتماعية . مصدر سابق.

٣٢. أحمد ،عبد الخالق محمد. (٢٠١٤). مصدر سابق

٣٣. الهندسة الاجتماعية . مصدر سابق.

٣٤. أحمد ،عبد الخالق محمد. (٢٠١٤). مصدر سابق.

٣٥. حجازي، إبراهيم (٢٠١٣). ٥ طرق لأختراق حسابك على "الفيس بوك " .. ونصائح لحماية خصوصيتك

http://www.digitalqatar.qa/2013/10/02/3698

٣٦. **الزهراني ،أحمد عيضه (٢٠١٤). الهندسة الاجتماعية .مصدر سابق**

٣٧. حجازي، إبراهيم (٢٠١٣). مصدر سابق.

٣٨. طرق اختراق الفيس بوك : الصفحات المزورة و كيفية الحماية منها .

http://expertcet.blogspot.com.eg/2015/07/fack-page.html

ملحق

استبانة عن مدى وعي المجتمع العربي بالهندسة الاجتماعية وشبكات التواصل الاجتماعي.

البيانات الشخصية :

الاسم (اختياري) : .....
الجنس: ذكر [ ] أنثى [ ]
مجال العمل: .....
الجنسية: .....
السن: أقل من ٣٠ سنة [ ]
من ٣٠ إلى ٣٩ سنة [ ]
من ٤٠ إلى ٤٩ سنة [ ]
من ٥٠ إلى ٥٩ سنة [ ]
من ٦٠ سنة فأكثر [ ]

مدى الوعي بالهندسة الاجتماعية (فن اختراق العقول)

إلى أي درجة أنت على علم بعبارة:

		درجة كبيرة	درجة متوسطة	درجة قليلة
١.	الهندسة الاجتماعية	[ ]	[ ]	[ ]
٢.	فن اختراق العقول	[ ]	[ ]	[ ]
٣.	انتهاك الخصوصية	[ ]	[ ]	[ ]
٤.	الامن المعلوماتي	[ ]	[ ]	[ ]
٥.	الاختراق الرقمي	[ ]	[ ]	[ ]
٦.	انتحال الهوية	[ ]	[ ]	[ ]
٧.	التصيد الالكتروني	[ ]	[ ]	[ ]
٨.	الاحتيال الالكتروني phishing	[ ]	[ ]	[ ]
٩.	الاحتيال الصوتي Visingعبر الهاتف	[ ]	[ ]	[ ]
١٠.	الرسائل الاقتحامية المزعجة Spam	[ ]	[ ]	[ ]

عند استخدامك شبكات التواصل الاجتماعي :

		نعم	لا	احيانا
١.	هل تسجل في الشبكات الاجتماعية باسمك الحقيقي	[ ]	[ ]	[ ]
٢.	هل تتيح بياناتك الشخصية على شبكات التواصل الاجتماعي	[ ]	[ ]	[ ]
٣.	هل بياناتك الشخصية المتاحة على شبكات التواصل الاجتماعي صحيحة	[ ]	[ ]	[ ]
٤.	هل تتيح صورك الشخصية وصور عائلتك على شبكات التواصل الاجتماعي	[ ]	[ ]	[ ]

		نعم	لا	احيانا
٥.	هل تمتلك معلومات كافية عن شبكات التواصل الاجتماعي	[ ]	[ ]	[ ]
٦.	معلوماتك الشخصية على شبكات التواصل الاجتماعي سهلة الوصول اليها ولا تحتاج إلى حماية أمنية	[ ]	[ ]	[ ]
٧.	معلوماتك الشخصية على شبكات التواصل الاجتماعي يجب حمايتها فقط إذا كانت هناك محاولات لسرقتها	[ ]	[ ]	[ ]
٨.	معلوماتك الشخصية على شبكات التواصل الاجتماعي يجب حمايتها في كل وقت لتفادى سرقة الهوية	[ ]	[ ]	[ ]
٩.	تعتقد أنه يمكن نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي دون توخى الحذر	[ ]	[ ]	[ ]
١٠	تعتقد أنه يمكن نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي مرتبط بالالتزام بقوانين الشبكات الاجتماعية	[ ]	[ ]	[ ]
١١	تعتقد أنه يمكن نشر أي معلومات بسهولة على شبكات التواصل الاجتماعي طالما مقتصرا في نطاق العائلة والأصدقاء	[ ]	[ ]	[ ]

تعرضك لانتهاك خصوصيتك واختراقك

		نعم	لا
١)	هل تعرضت للتجسس ولانتهاك معلوماتك على شبكة التواصل الاجتماعي	[ ]	[ ]
٢)	هل تعرضت لسرقة الهوية من خلال شبكات التواصل	[ ]	[ ]
٣)	هل تعرضت التصيد الإلكتروني	[ ]	[ ]
٤)	هل تعرض بريدك الالكتروني للاختراق	[ ]	[ ]
٥)	هل تعرض حساباتك المصرفية للاختراق	[ ]	[ ]

في حالة تعرضك للهندسة الاجتماعية (فن اختراق العقول) أي الطرق التالية تعرضت لها:

		نعم	لا
١.	انتحال الهوية والتحقق من الشبكة وتم طلب كلمات المرور الخاصة بك	[ ]	[ ]
٢.	انتحال الهوية والتحقق من الشبكة وتم طلب تحميل برمجيات معينة على حاسبك الخاص	[ ]	[ ]
٣.	الاحتيال عن طريق رسالة بريد الكتروني من شركة ائتمان/ بنك وتم طلب التحقق من معلوماتك	[ ]	[ ]
٤.	الاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب التحقق من معلوماتك	[ ]	[ ]
٥.	الاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب عبر الرسالة الآلية بإدخال رقم بطاقتك الائتمانية	[ ]	[ ]
٦.	الرسائل الاقتحامية المزعجةSpam كتهنئة من صديق	[ ]	[ ]
٧.	تحميل برامج من مواقع تقنعك بأهمية البرنامج	[ ]	[ ]
٨.	تعرضك للتجسس والتصنت وسرقة كلمة المرور ومعلومات مهمة	[ ]	[ ]

		نعم	لا
٩.	تعرضك للانتهاك من خلال رمي أوراق مهمة وكلمة المرور في سلة المهملات	[ ]	[ ]

في حالة اختراقك عبر شبكات التواصل الاجتماعي أى الطرق التالية تعرضت لها:

		نعم	لا
١.	صفحات تسجيل الدخول المزيفة (Phishing Attacks)	[ ]	[ ]
٢.	برمجيات الطرف الثالث المستخدمة في حساباتنا (Third party Applications)	[ ]	[ ]
٣.	تخمين كلمة المرور (Brute force attacks)	[ ]	[ ]
٤.	تخمين الإجابات لطرق استعادة كلمة المرور	[ ]	[ ]
٥.	كلمات المرور المسجلة في متصفحك	[ ]	[ ]

يسعدنا تلقي آرائك ومقترحاتك :

-

-

فضلاً أضف أية معلومات أو تعليقات أو أفكار ترغب في عرضها تتعلق بهذا الموضوع.

-

-

-

-