العنوان:	الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي
المصدر:	المجلة الدولية لعلوم المكتبات والمعلومات
الناشر:	الجمعية المصرية للمكتبات والمعلومات والأرشيف
المؤلف الرئيسي:	محمد، مها أحمد إبراهيم
المجلد/العدد:	مج5, ع3
محكمة:	نعم
التاريخ الميلادي:	2018
الشهر:	سبتمبر
الصفحات:	109 - 128
رقم MD:	931067
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	HumanIndex
مواضيع:	الهندسة الاجتماعية، شبكات التواصل الاجتماعى، الخصوصية، الأمن الرقمى، الجرائم الإلكترونية، المجتمع العربى
رابط:	http://search.mandumah.com/Record/931067

الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي

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

مستخلص :

تأتي هذه الدراسة التي تسعى إلى تحقيق هدف رئيس؛ 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 اليوم ما كان ليتطور إلا باستخدام التكنولوجيا في جميع مناحي الحياة حيث تدخل التكنولوجيا إلى حياتنا أكثر فأكثر، فالتقنية أصبحت جزءًا هاماً لا يُستغنى عنه في نسيج الحياة، لما تقدمه من تسيير وتيسير مهام ووظائف حياتنا اليومية. نشهد حاليا ثورة هائلة في المجال التكنولوجي والمعلومات الرقمية التي نعيشها تحمل معها الكثير من الإيجابيات والسلبيات للفرد والمجتمع، مما أدى إلى توغل تلك التقنيات في حياتنا حتى بات من الصعب الاستغناء عنها مما يقع على عاتقنا كأفراد ومستخدمين للتقنية مهمة نشر ثقافة الوعي المجتمعي للاستخدام الأمثل لتلك التقنيات في نطاقها الصحيح، ومن أن نسعى ونتعاون لتوظيف التقنية بالطرق الصحيحة ووفقا لقواعد أخلاقية سليمة، مع مراعاة الضوابط الدينية والقانونية، والتي ستعمل على الحد من سلبيات التقنية على المجتمع.

لقد أصبحت الهندسة الاجتماعية، التي يُطلَق عليها أحيانًا اسم علم أو فن اختراق العقول، ذات شعبية كبيرة في السنوات الأخيرة نظرًا للنمو الهائل والمتسارع لشبكات التواصل الاجتماعي والبريد الإلكتروني والأشكال الأخرى للاتصالات الإلكترونية. وفي مجال أمن المعلومات، أصبح هذا المصطلح مستخدمًا على نطاق واسع للإشارة إلى مجموعة من الأساليب التي يستخدمها المجرمون في الحصول على المعلومات

تاريخ استلام البحث : ١١ ديسمبر ٢٠١٧ ، تاريخ القبول : ٥ ابريل ٢٠١٨

الحساسة أو إقناع الضحايا المستهدفة بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بها[٣٧].

يعد الأمن الرقمي (الحماية الذاتية) للمواطن أحد ركائز المواطنة 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 "القدرة على الحصول على معلومات سرية وهامة بأسلوب التلاعب العقلي . وبه يتم اقتحام شبكة ما أو نظام تشغيلي ما. نتيجة خطأ بشري . فالهندسة الاجتماعية تبحث عن أخطاء بشرية ليتمكن المستخدم من الحصول على غايته كـ(الثقة الزائدة – عدم التركيز – الفضول) وتبدأ اللعبة عند اكتشاف نقطة الضعف التي يتم الاستغلال من خلالها[٣٨]. وهذا ما دفع 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 احترام الخصوصية من الأمور التي تؤرق من يتعامل مع التكنولوجيا 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 حجز الزاوية في التعاملات اليومية، وهنا يطرح السؤال نفسه كيف يمكننا تحقيق الأمن المعلوماتي كأفراد؟ في حين نجد المؤسسات تعمل جاهدة على حمايتها ألا أنها ما زالت غير أمنة حيث يمكن اختراقها بواسطة "الإنسان "عن طريق ما يسمى بالهندسة الاجتماعية التي باتت اليوم أساسا لمعظم الهجمات الإلكترونية المجهولة المصدر والمعقدة التتبع. تستمد 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 الخطير الذي تلعبه شبكات التواصل الاجتماعي في أنها تتيح للمستخدمين البحث والتواصل مع الآخرين بسهولة ويسر من خلال المواقع الإلكترونية العامة والحسابات الشخصية، فأضحت شبكات التواصل الاجتماعي أقوى أدوات الاتصال الاجتماعي بين أفراد المجتمع. حيث تأكد الإحصائيات التزايد المستمر في استخدام هذه المواقع خاصة الفيسبوك. وتويتر وغيرهما من وسائل الاتصال الأخرى فإن استخدام شبكات التواصل الاجتماعي له آثاره النافعة وعواقبه السلبية فهناك إجماع بين العديد من الباحثين على أن هذه الشبكات قد فتحت عصرا جديدا من عصور الاتصال والتفاعل بين البشر، ألا أنها فتحت الباب على مصرعيه للتجاوزات والانتهاكات للمستخدمين.

لذا تهدف هذه الدراسة إلى 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. حيث تعتمد الهندسة الاجتماعية في المقام الأول

---

٣٧ - الهندسة الاجتماعية: اختراق العقول البشرية.
https://me.kaspersky.com/blog/%d8%a7%d9%84%d9%87%d9%86%d8%af%d8%b3%d8%a9-%d8%a7%d9%84%d8%a7%d8%ac%d8%aa%d9%85%d8%a7%d8%b9%d9%8a%d8%a9-%d8%a7%d8%ae%d8%aa%d8%b1%d8%a7%d9%82-%d8%a7%d9%84%d8%b9%d9%82%d9%88%d9%84-%d8%a7%d9%84%d8%a8/1022 /

٣٨ - الهندسة الأجتماعية .- https://www.security4arabs.com/2010/08/11/social-engineering/

على فن اختراق العقول وانتهاك خصوصيتهم أثناء استخدام تكنولوجيا المعلومات وشبكات التواصل الاجتماعي. 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 العربي باستخدام شبكات التواصل الاجتماعي التي أصبحت تشكل آلية حديثة في عالم التواصل بين الأفراد والجماعات، والتي يتبادل الأشخاص فيها المعلومات والآراء والأفكار بكل حرية وبدون رقيب مما ساعد على اختراقها بسهولة والاطلاع على محتوياتها من جانب أي طرف مهتم بمعلومات عن المستخدمين، ويمكن استخدام تلك المعلومات في عدة أغراض تخدم مصالحه وبصورة متكررة [٣٩]

قد تغري طبيعة التواصل عن طريق الانترنت العديد من المستخدمين بتبادل المعلومات الشخصية عن أنفسهم، من خلال الشبكات الاجتماعية أكثر من أي وقت مضى، مما فتح المجال للمحتالين وقراصنة المعلومات لاستغلال هذه المعلومات لمصالحهم الخاصة[٤٠].

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 العربي لها (عينة عشوائية من أفراد المجتمع) من مرتادي 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(♣)، بهدف الحصول على

٣٩ مركز الدراسات الإستراتيجية، المعرفة وشبكات التواصل الالكترونية، جامعة الملك عبد العزيز، العدد ٣٩، الرياض ٢٠١٢، ص ١٢٦.
40مجلة الحقوق والعلوم الإنسانية - جامعة زيان عاشور ". تريكي، حسان. "التهديدات الامنية المرتبطة بالاستخدامات السيئة لشبكات التواصل الاجتماعي ع ١٩ (٢٠١٤): ١٩٥ - ٢٠٤. بالجلفة - الجزائر

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 يعني 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 هي:

وقام Orgill, G وآخرين بدراسة عنوانها -The Urgency for Effective User Privacy education to Counter Social Engineering Attacks on Secure"[٤١]

تهدف هذه الدراسة إلى قياس مدى وعي المستخدمين للانترنت بالهندسة الاجتماعية، حيث قام الباحثين بالادعاء أنهم ينتمون للمؤسسة كموظف في قسم دعم الكمبيوتر في المؤسسة وطلب من الموظفين معلومات عديدة من بينها أسماء المستخدمين وكلمات السر وما إلى ذلك. وكانت نتائج الدراسة مثيرة للقلق، وأظهرت أن حوالي ٨٠٪ من المشاركين قدمت اسم المستخدم، في حين أن ما يقرب من ٦٠٪ قدمت كلمة المرور الخاصة بهم.

وقام كل من Karakasiliotis A, Furnell MS, Papadaki M. دراسة عنوانها " Assessing end-user awareness of social engineering and phishing"[٤٢] تقدم هذه الدراسة تقييما لوعي المستخدمين تجاه الهندسة الاجتماعية من طريق استخدام البريد الالكتروني مجالاً لهجمات التصيد حيث أجرى الباحثون مزيجا من ٢٠ رسائل البريد الإلكتروني المشروعة وغير المشروعة؛ التي طلب من

(*) نص الاستبانة في الملحق .

41 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.

42 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.

المشاركين فيها التمييز بين رسائل البريد الإلكتروني المشروعة وغير المشروعة، وأظهرت النتائج وعي ١٧٩ فردًا بنسبة ٣٦% نجحوا في تحديد رسائل البريد الإلكتروني المشروعة، مقابل ٤٥٪ ناجحة في اكتشاف غير المشروعة. بالإضافة إلى ذلك، في كثير من الحالات، فإن المشاركين الذين حددوا رسائل البريد الإلكتروني غير المشروعة بشكل صحيح لم يتمكنوا من ذكر أسباب مقنعة لاختيارهم.

ودراسة اخرى قام بها T.Bakhshi, M. Papadaki, and S. M. furnell بعنوان " A practical Assessment of social engineering Vulnerability "[٤٣] هدفت هذه الدراسة التحقيق من مستويات قابلية الموظفين تجاه الهندسة الاجتماعية. وقد أجريت الدراسة على ١٥٢ موظفا من جامعة بليموث (المملكة المتحدة) بإجراء تجربة عن طريق إرسال رسالة إلى المشاركين، وطلب منهم إتباع رابط وتثبيت تحديث البرامج المطالب بها. وأظهرت نتيجة هذه التجربة أن ٢٣٪ من المتلقين نجحوا في الهجوم بنجاح.

وأجريت دراسة أخرى في عام ٢٠١٠ قام بها كلاً من Jamshaid Mohebzada, Ahmed El Zarka, Arsalan Bhojani, بعنوان " An Awareness Study on Account Phishing, Spam Emails & Social Engineering Attacks"[٤٤] وكان الهدف من هذه الدراسة قياس مدى وعي الموظفين والطلاب في الجامعة الأميركية (American University of Sharjah (AUS تجاه الهندسة الاجتماعية. وقد أجرى الباحثين عددا من التجارب من أجل تحقيق هدف الدراسة. التجربة الأولى استخدموا طريقة التصيد عن طريق إرسال رسائل بريد إلكتروني وهمية لجميع الموظفين والطلاب، ووفقا للنتائج، بلغ عدد الضحايا ٤٨٥ من الذكور و ٤٦٩ من الإناث من مجموع ٥١٦٦ طالبا و ٣٥١ من الموظفين. في التجربة الثانية، تم خداع الأشخاص المستهدفين عن طريق إرسال بريد إلكتروني مزيف لهم، وطلب منهم إرسال معلوماتهم الشخصية للمشاركة في استطلاع بحثي أجرته الجامعة الأمريكية، مع وعد بأن أي مشارك سيحصل على USB Flash Drive فكان عدد الضحايا في هذه التجربة أقل بكثير من السابق. لم يكن هناك سوى ٢٢٠ ردا على البريد الإلكتروني المزيف. ومن المثير للاهتمام أن تحليل النتائج كشف عن وجود عدد كبير من الضحايا بين الطلاب الكبار؛ بالمقارنة مع الطلاب الجدد والناشئين.

قام كلا من Mutasim Elsadig Adam وآخرون بدراسة عنوانها Awareness of Social Engineering Among IIUM Students [٤٥] تستعرض هذه الدراسة أنه على الرغم من أن معظم المنظمات في جميع أنحاء العالم تولي حاليا المزيد من الاهتمام لتأمين نظم المعلومات عن طريق أدوات أمنية متطورة، لا تزال نظم المعلومات الخاصة بهم لا يمكن اختراقها. مما يدفع القراصنة اللجوء إلى استخدام الهندسة الاجتماعية بدلا من استخدام مهاراتهم التقنية للحصول على المعلومات. كما تتناول مفهوم الهندسة الاجتماعية وتهدف هذه الدراسة هو إثبات أن مستخدمي نظم المعلومات يعتبرون التهديد الحقيقي لأنفسهم. حيث من فروض هذه الدراسة، أن عدم وعي المستخدمين بالهندسة الاجتماعية يجعل نظم المعلومات عرضة لأنواع عديدة من الانتهاكات. كما تهدف إلى التعرف على ما إذا كان طلاب تكنولوجيا المعلومات لديهم المزيد من الوعي بالهندسة الاجتماعية من الطلاب من الكليات الأخرى. تم جمع البيانات اللازمة من ٢٤٥ طالبا من الجامعة الإسلامية الدولية في ماليزيا (IIUM)، من خلال استبيان على الإنترنت، بالإضافة إلى ذلك تم إجراء تجربة التصيد الهاتفي التي أجريت على عدد قليل من الطلاب.

43 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.
44 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.
45 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

وأظهرت النتائج أن نحو ١١٤ طالبا تعرضوا لهجمات الهندسة الاجتماعية خلال الأشهر الستة الماضية، وما يقرب من ٣٨٪ من هذه الهجمات من خلال البريد الإلكتروني.

وأجري Fagoyinbo, I.S وآخرين دراسة عنوانها "Statistical analysis on the awareness and safeguarding against social engineering"[٤٦] على ٤٠ موظفا في Federal Polytechnic, Ilaro, Ogun State, Nigeria وكان الهدف من هذه الدراسة 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 الجهود الرامية إلى زيادة الوعي بين الموظفين.

كما قام كل من Ugiomo S. Odaro & Benjamin G. Sanders بدراسة تقييما لوعي المستخدمين تجاه الهندسة الاجتماعية من طريق استخدام البريد الالكتروني مجالاً لهجمات التصيد أيضا عنوانها "Social Engineering: Phishing for a Solution"(٤٧) حيث تم تقديم مجموعة من السيناريوهات الإلكترونية وغير الشرعية المشروعة وغير المشروعة إلى ١٥٣ مشاركا من خلال دراسة استقصائية على الإنترنت. وقد طلب من المشاركين تحديد أي من سيناريوهات البريد الإلكتروني والموقع الإلكتروني كانت شرعية أو غير شرعية حيث نجد أن ٤٣٪ من 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 An Extended Validation SSL Certificate (EV SSL) 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.

مصطلحات ومفاهيم:

الشبكات الاجتماعية:

جاء تعريف الشبكات الاجتماعية social networking service في قاموس ODLIS هي خدمة الإلكترونية تسمح للمستخدمين بإنشاء وتنظيم ملفات شخصية لهم، كما تسمح لهم بالتواصل مع الآخرين[٤٨].

46 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.
47 Ugiomo S. Odaro & Benjamin G. Sanders, "Social Engineering: Phishing for a Solution",http://www.kaspersky.com/images/odaro,_ugiomo_susan_sanders,_benjamin__social_engineering_phishing_for_a_solution-10-98480.pdf.
48 ODLIS-Online Dictionary for Library and Information Science.

وتعرف الموسوعة البريطانية الشبكات الاجتماعية بأنها مواقع تشاركية يتشارك فيها الأعضاء في الحياة الاجتماعية والتواصل الاجتماعي، ويتفاعلون بعضهم البعض مكونين مجتمعا على شبكة الإنترنت؛ يعبر كل فرد فيه بحرية عن آرائه وآماله[٤٩].

الخصوصية:

عرف قاموس ODLIS مصطلح الخصوصية بناءً على القانون الذي وضعته جمعية المكتبات الأمريكية حيث تنص على أن حرية الفرد في الحصول على جميع الخدمات والمعلومات التي يحتاجها، ويساعده في هذا أمناء المكتبات دون التدخل في الأسباب التي دفعت المستفيد إلى طلب هذه المعلومات، ويجب احترام تفكير المستفيد وحقوقه في الحصول على ما يريد في الوقت المناسب، وتناول أيضا قوانين الخصوصية من ناحية حرية الفرد في الحصول على خدمات المعلومات دون تدخل من الآخرين[٥٠].

الاختراق:

يقصد **بالاختراق**: إعادة تنظيم وترتيب نظام موجود أو موارد شبكة بطريقة تتسم بالمهارة والذكاء والمخترق في هذه الحالة لا يكون بالضرورة مجرم كمبيوتر، وما عرف الاختراق بأنه عبارة عن عمل سريع يحرز نتائج لا تتبع في انجازه أي إجراءات منظمة وقد ينتج عنه تحسين النظام الموجود بأن يقوم المخترق HACKER بتعديل البرامج بلا تفويض من الجهات المعنية 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 الكمبيوتر يطلقون على من يقوم بهذه العمليات اسم كراكر أو مخرب أو محطم Cracker[٥١]

الاحتيال:

الاحتيال هو الاستيلاء على مال مملوك للغير بخداعه وحمله على تسليم ذلك المال والاحتيال يأتي بالاعتداء على حق الملكية سواء في ذلك ملكية منقولة أو عقارية ويتميز بالأسلوب 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 [٥٢]

التصيد الالكتروني:

يعرف التصيد على أنه عملية احتيالية يتم فيها الحصول على معلومات شخصية أو حساسة كمعلومات بطاقات الائتمان أو اسم المستخدم ، أو كلمة المرور عن طريق الإيهام بأنه كيان موثوق فيه في الفضاء الرقمي.[٥٣]

---

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

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

50 ODLIS-Online Dictionary for Library and Information Science. http://lu.co/odlis/index.cfm.

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

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

٥٣ التصيد الالكتروني أنواعه وتقنياته .٢٠١٢

http://uaecyber.com/%D8%A7%D9%84%D8%AA%D8%B5%D9%8A%D8%AF-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D8%A3%D9%86%D9%88%D8%A7%D8%B9%D9%87-%D9%88%D8%AA%D9%82%D9%86%D9%8A%D8%A7%D8%AA%D9%87 /

الجرائم الإلكترونية:

تعرف **الجرائم الإلكترونية** (Electronic crime "or" e-crime) بأنها الممارسات التي توقع ضد فرد أو مجموعة مع توفر باعثٍ إجرامي بهدف التسبب بالأذى لسمعة الضحية عمداً، أو إلحاق الضرر النفسي والبدني به سواءً أكان ذلك بأسلوب مباشر أو غير مباشر بالاستعانة بشبكات الاتصال الحديثة كالإنترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحادثة، والهواتف المحمولة وما تتبعها من أدوات كرسائل الوسائط المتعددة[٥٤]

مفهوم الهندسة الاجتماعية :

هو أسلوب من أساليب الاختراق التي تعتمد على العنصر البشري تماما وليس لها أيه أبعاد تقنية حيث يستخدم الهاكر مهاراته في الاتصال مع الآخرين ويستعمل الخداع والكذب ليحصل منهم على معلومات ذات طابع تقني يتمكن بواسطتها من القيام بعملية الاختراق وغالبًا ما تتم هذه العملية من خلال المحادثات الهاتفية[٥٥]

مصطلح **الهندسة الاجتماعية** اسم يوحي في ظاهره أنه من أشكال الهندسة المحمودة التي عمرت البشرية علما ونفعا بينما هو في الحقيقة خطر محدق على المعلومات الشخصية للمواطن كفرد وأمن معلومات القطاع الحكومي والخاص. وفقا لتقرير المخابرات الأمنية بشأن ماليزية ، والتي أعلنت عنه شركة مايكروسوفت في ١٢ مايو ٢٠١١: الذي تتضمن أن" مجرمي الإنترنت يستخدمون في هجماتهم أساليب أكثر سهولة من بينها تكتيكات الهندسة الاجتماعية والاستفادة من المآثر التي أنشأتها المجرمين الأكثر مهارة لاتخاذ صغيرة مبلغ المال من عدد كبير من الناس "[٥٦].

وليس لمصطلح الهندسة الاجتماعية **Social Engineering** معنى متفق عليه، ولكن من أقرب التعريفات: "أنها استخدام المهاجم لحيل نفسية كي يخدع مستخدمي الحاسوب ليمكنوه من الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها وخلافا لما قد يتوهم بعض الناس، فإن الهندسة الاجتماعية يجب أن تكون على رأس قائمة وسائل الهجوم التي يجب أن نحاول حماية المعلومات منها[٥٧]. وهناك عدة تسميات للهندسة الاجتماعية ومنها((الاحتيال الإلكتروني، المهندس الاجتماعي، الاحتيال الصوتي، الخدع الاجتماعية.))[٥٨]

ونعرف الهندسة الاجتماعية بأنها عبارة عن "أي عمل يؤثر على الشخص لاتخاذ إجراء قد يكون أو لا يكون في مصلحتهم عن طريق مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفضون بمعلومات سرية.وعلى الرغم من أننا نركز على الأشكال التقنية إلا أنه من المهم أن نفهم الجوانب النفسية، والجوانب الفسيولوجية، والتكنولوجية للتأثير على شخص بشكل عام. ويمكن أيضا استخدام نفس المبادئ التي تستخدم في المعنى الإيجابي بشكل ضار[٥٩].

---

٥٤ الحياري، إيمان(٢٠١٧) أنواع الجرائم الإلكترونية.
http://mawdoo3.com/%D8%A3%D9%86%D9%88%D8%A7%D8%B9_%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85_%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9
55 cole,Eric (2002). Hackers Beware: Defending your Network from the Wilty Hacker .Indianapolis, Indianan: New Riders Publishing
56 Microsoft security Intelligence Report: Cybercriminals Targeting Consumers
http://www.cybersecurity.my/en/knowledge_bank/news/2011/main/detail/2032/index.html
٥٧ 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
٥٨ أحمد، عبدالخالق محمد. "الهندسة الإجتماعية ".المال والاقتصاد (بنك فيصل الاسلامي السوداني) - السودان ع٧٥ (٢٠١٤): ٢٢ - ٢٣ .
59 The Social Engineering Framework
https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

أنواع الهندسة الاجتماعية

انتحال الهوية: تتطلب الهندسة الاجتماعية عادة بعض أشكال انتحال الهوية من أجل كسب ثقة الهدف. التكتيك الذي يستخدم في كثير من الأحيان يتكون من انتحال شخصية دعم تكنولوجيا المعلومات الذي يحدث أن "التحقق من الشبكة" ويطلب كلمة مرور، أو يطلب تحميل برمجيات معينة[٦٠]

النوع الثاني وهو **التصيد الاحتيالي**: عبارة عن عمل احتيال يمكن ملاحقته قضائيا. التصيد الاحتيالي هو عملية يتم استخدامها للحصول على معلومات شخصية للأفراد أو تفاصيل عن طريق التظاهر ككيان موثوق به في أي تبادل للمعلومات كرسالة بريد الكتروني من شركة ائتمان أو بنك وصلتك وتطلب التحقق من معلوماتك[٦١]

النوع الثالث يطلق عليه **الاحتيال الصوتي عبر الهاتف** يحدث هذا عندما لا يكون الناس على بينة من قيمة المعلومات التي يمتلكونها. وهذا يمكن أن يتم ذلك بعدة طرق منها أدلة سياسة الشركة، وكذلك دفتر الهاتف للشركة[٦٢].

المهندس الاجتماعي وطريقة عمله:

الهدف من الاختراق عموماً بغض النظر عن الطريقة المستخدمة هو الحصول على المعلومات السرية أياً كان نوعها. وهنا يأتي دور الهندسة الاجتماعية في عملية اختراق الأجهزة والأنظمة عن طريق شخص يسمى (مهندس اجتماعي) يتمتع بمهارات اجتماعية وتقنية عالية وأيضا مقدره على التمثيل 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 ينتحل شخصية موظف بنك ويقوم بالاتصال على أحد عملاء البنك وبطريقته الخاصة يحصل على جميع البيانات البنكية وهذه الطريقة للأسف منتشرة بكثرة وأغلب الضحايا هم من كبار السن. أيضا قد ينتحل شخصية عامل صيانة أجهزة وشبكات حاسب إلى أو يعمل بشكل مؤقت في إحدى الشركات ويختلط بالموظفين الذين لديهم صلاحيات الدخول لأنظمة المنشأة[٦٣] .

أقسام الهندسة الاجتماعية:[٦٤]

تصنف جرائم الهندسة الاجتماعية إلى صنفين:

- **هندسة قائمة على أساس تقني:**

هي برامج وتقنيات تساعد الهاكر للوصول للمعلومة ومن أمثلة ذلك :

- **الاحتيال الالكتروني phishing:** يعد أحد أهم طرق الهندسة الاجتماعية ، ويعكس هذا المصطلح على رسالة بريد الكتروني من شركة ائتمان أو بنك وصلتك وتطلب التحقق من معلوماتك وتحتوي هذه الرسالة على وصلة لصفحة ويب احتيالية تظهر مشابهة تماما للموقع

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

61 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.

62 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.

٦٣ الزهراني ،أحمد عيضه (٢٠١٤). الهندسة الاجتماعية

. http://www.saudiacademics.com/article/computer-tech/item/1120-%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9.html

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

الرسمي للشركة، هذه الصفحة تطلب منك إدخال كلمة السر واسم المستخدم ومن ثم توجهك للصفحة الصحيحة بعد أن حصلت على كافة بياناتك السرية.

- **الاحتيال الصوتي Vising**: أكثر هجمات الهندسة الاجتماعية تقع عن طريق الهاتف. يتصل المهاجم مدعياً أنه شخص ذو منصب له صلاحيات ويقوم تدريجياً بسحب المعلومات من الضحية[٦٥]. يعتمد هذا النوع على برنامج **War Dialler** وهو برنامج يقوم بالاتصال بالعديد من أرقام الهواتف المختلفة في المنطقة وبعد الاتصال يقوم الهاكر 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 الهاكر على ما يريد.
- **الرسائل الاقتحامية المزعجة Spam**: هي رسائل الكترونية بعناوين مشوقة للقراءة مثل تهنئة من صديق أو تأكيد بيع أو غيرها وبداخل تلك الرسائل ما يسبب تدمير الجهاز وسرقة معلوماته.
- **برامج مهمة** :وهي ما نشهده في بعض المواقع من روابط تحميل برامج ولكنها تكون مدعومة بكلمات اقناعية عن أهمية ذاك البرنامج المكر للجهاز والسارق للمعلومات الحساسة[٦٦].

- **<u>هندسة قائمة على أساس بشرى أو إنساني:</u>**

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

١) **الإقناع:** حيث يحصل المهاجم على المعلومات التي يريدها من خلال التحدث مع الضحية وحثها على الإدلاء بمعلومات حساسة أو ذو علاقة بهدف المهاجم وذلك من خلال إثارة انطباع جيد لدى الضحية والتملق وغيرها من الأساليب. الغرض من هذه الطرق إقناع الضحية بالسماح للمهاجم الحصول على المعلومات التي يريدها.

٢) **الهندسة الاجتماعية المعاكسة:** وهي إيهام الضحية بأنك شخص مهم أو ذو صلاحيات عليا بحيث يقوم المهاجم بالإدلاء بمعلومات يريدها الضحية وإذا ما نجح الأمر وسارت الأمور كما خُطط لها فقد يحصل المهاجم على فرصة أكبر للحصول على معلومات ذات قيمة كبيرة من الضحية، وهذا الأسلوب معقد نسبياً كونه يعتمد على مدى التحضير المسبق وحجم المعلومات التي بحوزة المهاجم [٦٧]

٣) **الانتحال:** وذلك عن طريق سيناريوهات مختلفة تستهدف شيئا ما، وغالبا ما تكون عبر الهاتف فهي لا تتطلب الحضور وجها لوجه ولكنها تتطلب بعض المعلومات مثل الاسم أو تاريخ الميلاد وغيرها.[٦٨]

٤) **سلة المهملات:** حيث يوجد الكثير من المعلومات الهامة عن المنظمة يمكن الحصول عليها من سلة مهملات الشخص أو الضحية[٦٩]. من الخطأ الشائع رمي البريد أو ورقة غير مرغوب فيها في سلة المهملات دون تمزيق أو إزالة بياناتها فقد تكون سلة المهملات جسر الهاكر الأقوى

---

٦٥ الهندسة الاجتماعية Social engineering و أساليب الإختراق
https://ainkermesinfo.blogspot.com.eg/2016/01/social-engineering.html

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

٦٧ الهندسة الاجتماعية . مصدر سابق.

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

٦٩ الهندسة الاجتماعية . مصدر سابق.

لسرقة الهوية وبالتالي يستطيع إقناع ضحيته، وكذلك الأقراص فمعظم المؤسسات تعتقد أن مسح بيانات القرص كفيلة بإزالتها تماما ولكن هناك طرق تقنية عديدة لاستعادتها حتى بعد مسحها.

٥) **التجسس والتصنت:** يمكن سرقة كلمة المرور ومعلومات مهمة عن طريق مراقبة الضحية حين كتابتها أو التصنت والاستماع لمحادثة هاتفية لذلك ينصح دائما بتجنب كتابة كلمات السر والمعلومات المهمة على ورق تحت لوحة المفاتيح أو حتى تبادلها[٧٠].

الطرق التي يمكن من خلالها اختراق الحسابات الشخصية وهي[٧١] :

١- صفحات تسجيل الدخول المزيفة (Phishing Attacks)
٢- تطبيقات الطرف الثالث المستخدمة في حساباتنا (Third party Applications)
٣- تخمين كلمة المرور (Brute force attacks)
٤- تخمين إجابات لاستعادة كلمة المرور
٥- كلمات المرور المسجلة على متصفحك

النصائح التي يجب مراعاتها لتجنب الوقوع ضحية للهندسة الاجتماعية[٧٢]:

١- لا تثق بأي مكالمة هاتفية أو بريد الكتروني من أي شخص يطلب منك معلومات شخصية أو بنكية ويجب التأكد من هوية هذا الشخص عن طريق الاتصال بالمصدر للتحقق من هوية طالب المعلومات.
٢- تجنب استخدم البطاقة الائتمانية إلا عند الضرورة القصوى واستخدام البطاقات مسبقة الدفع عوضا عن ذلك.
٣- تجنب وضع المعلومات الشخصية على الانترنت مثل الاسم واللقب ورقم الجوال أو أي معلومات بنكية.
٤- التأكيد على ضرورة إتلاف الأوراق والمستندات المهمة بواسطة أجهزة مخصصة لهذا الغرض.
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(١):

٧٠ أحمد ،عبد الخالق محمد. (٢٠١٤). مصدر سابق.
٧١ حجازي، إبراهيم (٢٠١٣). ٥ طرق لأختراق حسابك على "الفيس بوك " .. ونصائح لحماية خصوصيتك http://www.digitalqatar.qa/2013/10/02/3698
٧٢ الزهراني ،أحمد عيضه (٢٠١٤). الهندسة الاجتماعية .مصدر سابق

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
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 الإختراق والانتهاك(*) 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 الالكتروني phishing	٢٣٦	% ٧٠,٢	٦٧	% ١٩,٩	٣٣	% ٩,٨
٩.	الاحتيال الصوتي Vising عبر الهاتف	٣٣	% ٩,٨	٢٣٦	% ٧٠,٢	٦٧	% ١٩,٩
١٠.	الرسائل الاقتحامية المزعجة Spam	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

(*) مها أحمد إبراهيم محمد ، مدى وعي الطلاب بالهندسة الاجتماعية: دراسة تطبيقية على طلاب جامعة بني سويف أنموذجا. قيد الإعداد

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		أحيانا	
		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

* باقي الجدول في الصفحة التالية

م		نعم		لا		أحيانا	
		ع	%	ع	%	ع	%
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

م		نعم		لا	
		ع	%	ع	%
١	هل تعرضت للتجسس ولانتهاك معلوماتك على شبكة التواصل الاجتماعي	١٧٩	٥٣,٢ %	١٥٧	%٤٦,٧
٢	هل تعرضت لسرقة الهوية من خلال شبكات التواصل الاجتماعي	١٤٨	%٤٤,٠	١٨٨	%٥٦,٠
٣	هل تعرضت لعملية التصيد الإلكتروني	٧٩	%٢٣,٥	٢٥٧	%٧٦,٥
٤	هل تعرض بريدك الالكتروني للاختراق	١٧٩	٥٣,٢ %	١٥٧	%٤٦,٧
٥	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	%
١	انتحال الهوية والتحقق من الشبكة وتم طلب كلمات المرور الخاصة بك	٣٤	%١٠,١	٣٠٢	%٨٩,٩
٢	انتحال الهوية والتحقق من الشبكة وتم طلب تحميل برمجيات معينة على حاسبك الخاص	٧٩	%٢٣,٥	٢٥٧	%٧٦,٥
٣	الاحتيال عن طريق رسالة بريد الكتروني من شركة ائتمان/ بنك وتم طلب التحقق من معلوماتك	١٢	٣,٦ %	٣٢٤	%٩٦,٤
٤	الاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب التحقق من معلوماتك	٨٨	%٢٦,١	٢٤٨	%٧٣,٨
٥	الاحتيال عن طريق الاتصال الهاتف من شركة ائتمان/ بنك وتم طلب عبر الرسالة الآلية بإدخال رقم بطاقتك الائتمانية	١٢	٣,٦ %	٣٢٤	%٩٦,٤
٦	الرسائل الاقتحامية المزعجة Spam كتهنئة من صديق	٢٥٩	%٧٧,١	٧٧	%٢٢,٩
٧	تحميل برامج من مواقع تقنعك بأهمية البرنامج	١٧٩	%٥٣,٢	١٥٧	%٤٦,٧
٨	تعرضك للتجسس والتصنت وسرقة كلمة المرور ومعلومات مهمة	٧٧	%٢٢,٩	٢٥٩	%٧٧,١
٩	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"(٧٣). 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 (٧٤). 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	%
١	صفحات تسجيل الدخول المزيفة (Phishing Attacks)	١٥٧	%٤٦,٧	١٧٩	% ٥٣,٢
٢	برمجيات الطرف الثالث المستخدمة في حساباتنا (Third party Applications)	٢٣	%٦,٨	٣٣٤	%٩٣,٢
٣	تخمين كلمة المرور (Brute force attacks)	٨٨	%٢٦,١	٢٤٨	%٧٣,٨
٤	تخمين الإجابات كطرق استعادة كلمة المرور	١٨٨	%٥٦,٠	١٤٨	%٤٤,٠
٥	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.

٧٣ حجازي، إبراهيم (٢٠١٣). مصدر سابق.

٧٤ طرق اختراق الفيس بوك : الصفحات المزورة و كيفية الحماية منها .
http://expertcet.blogspot.com.eg/2015/07/fack-page.html

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 % ، تليهانسبة 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 كاف 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.

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 أى 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	[ ]	[ ]	[ ]
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	[ ]	[ ]	[ ]

		نعم	لا	احيانا
	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) أى 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	[ ]	[ ]
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.

.....

.....

Social engineering and social networks and their impact on the Arab society

D. Maha Ahmed Ibrahim Mohamed
Assistant Professor of Information Science
college of Literature . Beni-Suef University

Abstract:

The present study aims at recognizing to extreme the Arab community is aware of how to protect their personal accounts and ways of penetration (hacking) of privacy on general level and focusing on social engineering on particular. In addition to other available ways of training of the digital citizen. The concept of social engineering (the art of penetrating minds), the significance of of social networks in the Arab world, and the importance of privacy from the point of view of social networks' users in the Arab world, as well as recognizing ways of social networks penetration and ways of social engineering protection . So we can point out that the Arab community awareness of social engineering is one of its priorities for protecting their accounts in all social networks and the required skills to prevent attacks of this social engineering in all social networks.

A sample of 336 individuals was applied to the current study. The study also comes up with the following results: positively, individuals of the academic community succeeded at protecting their personal data automatically and at a high rate. Selection of fake names constitutes half of the academic community (53.2%), who use social networks and this is explored by their deny of personal data or by writing fake personal data. In addition to hacking their banking accounts since 6.8% of the individuals were slightly hacked. One of the most common methods of social engineering attacks are spam messages sent by a friend as congratulations (77.1%), followed by 53.2% who are convinced by the significance of programs to be downloaded, the importance of social networks in the Arab world, the importance of privacy from users' point of view of social networks in the Arab world, as well as the identification of penetrate ways of the social networks and how to be protected from social engineering.