عنوان المداخلة

أخطار الهندسة الاجتماعية على المستهلك الالكتروني

أ/ بن شايب كمال
جامعة: الجزائر 3
Email
simplemandz@gmail.com

أ/ بن قيدة عبد الرؤوف
جامعة: الجزائر 3
Email
benkaidaabderraouf@gmail.com

ملخص باللغة العربية:

تهدف هذه الورقة البحثية إلى إبراز ماهية الهندسة الاجتماعية، الفئات المستهدفة ودوافع تنفيذها، وكذلك التعرف على مختلف الأساليب التقنية وغير التقنية المستخدمة في تنفيذ هجمات الهندسة الاجتماعية والتلاعب بالأشخاص واستخراج المعلومات الخاصة بهم وسرقتها واختراق الأجهزة.

وقد تمّ الاعتماد على المنهج الوصفي في الدراسة، الذي ينطلق من محاولة استعراض المفاهيم المرتبطة بالهندسة الاجتماعية والتهديدات التي يمكن أن تلحقها بالمستهلك في ظل الانتشار الواسع لاستخدام تكنولوجيا المعلومات والاتصال.

كما نحاول تقديم بعض الطرق التي يمكن إتباعها للحد من هذا النوع من الهجمات وبعث الوعي لدى المستخدم لتجنب الوقوع ضحية لها.

الكلمات المفتاحية: الهندسة الاجتماعية، فن الخداع، رسائل التصيد، تزوير المواقع الالكترونية، انتحال الهوية.

Abstract:

This study aims to highlight the concept of Social Engineering, categories target of social engineering, motivation and goals of their attacks. As well as to find out the different types of attacks (either as technology based deception, or purely human based deception) which based on psychological manipulation, fooling users into handing over confidential or sensitive data and hack their devices.

The researchers used the descriptive approach on an attempt to review the concepts associated with social engineering and describe their impact on consumers in light of the widespread of information and communications technologies.

We have also attempted to present some of the ways to reduce and prevent social engineering attacks because it is highly unlikely that social engineering techniques will ever be completely eliminated, the most important strategy that can be directed to combat social engineering attacks is to raise awareness among the users on potential threats from the attackers.

Keywords: Social Engineering, Art of deception, phishing, Pharming, Impersonation.

مقدمة:

صاحب التقدم الهائل في تكنولوجيا المعلومات والاتصال زيادة في تنوع أشكال الهجمات الالكترونية التي يتعرض لها المستهلكون والمؤسسات على حد سواء، حيث أصبح المهاجمون باختلاف الدوافع والمكاسب التي يريدون الحصول عليها، يستخدمون في ذلك أساليب مختلفة في شن هجماتهم تتراوح ما بين الأساليب المستندة إلى الإنسان مثل: فن الخداع، القدرة على الإقناع، انتحال الهوية...الخ وأساليب تقنية كالتصيد الالكتروني، وتزوير المواقع الالكترونية وما إلى ذلك .

ومن هذا النوع من الهجمات ما يصطلح عليه بالهندسة الاجتماعية(**Social Engineering**) ، التي هي موضوع هذه الورقة البحثية، حيث تركز غالبية هجماتها على الحلقة الأضعف في سلسلة أمن المعلومات وهي العنصر البشري وذلك لأنه من الصعب ضمان عدم ارتكابه للأخطاء والوقوع ضحية لها.

إن المهندس الاجتماعي (المهاجم) إذا اجتمعت لديه الخبرة التقنية ومهارات استخدام الهندسة الاجتماعية فإنه يستطيع اختراق أي شبكة والوصول إلى المعلومات التي يريدها.

ونظرا لقلة الوعي بهذا النوع من الهجمات والتقنيات والأساليب المستخدمة فيها ومدى الضرر الذي يمكن أن تلحقه بالمستهلكين (الأفراد، المؤسسات...الخ) والطرق والإجراءات المضادة لها، جاءت هذه الدراسة محاولة تسليط الضوء عليها من خلال العناصر التالية:

أولا. مفهوم الهندسة الاجتماعية ومراحل تنفيذها؛

ثانيا. الفئات المستهدفة لهجمات الهندسة الاجتماعية ودوافع تنفيذيها؛

ثالثا. الأساليب المستخدمة في الهندسة الاجتماعية؛

رابعا. أمثلة على هجمات الهندسة الاجتماعية وتقديم بعض الطرق العملية للحد منها.

أولا: مفهوم الهندسة الاجتماعية ومراحل تنفيذها

يمكن تعريف الهندسة الاجتماعية ضمن سياق أمن المعلومات وهذا حسب ما أورده العديد من الباحثين على النحو التالي :

تشير الهندسة الاجتماعية إلى "مختلف الوسائل المستخدمة للحصول على المعلومات الحساسة وتجاوز الأنظمة الأمنية من خلال استغلال نقاط ضعف العنصر البشري"[1].

وعرفت بأنها: "أي فعل يؤثر على الشخص لاتخاذ إجراء معين قد يكون أو لا يكون في مصلحة هذا الشخص"[2].

وهذا التعريف يصب في نفس التعريف الذي قدمه Christopher Hadnagy صاحب كتاب الهندسة الاجتماعية: فن اختراق البشر (Social Engineering: The Art of Human Hacking) ويعتبر من الأوائل الذين وضعوا الأسس المفاهيمية للهندسة الاجتماعية. حيث عرفها بأنها " فعل التلاعب بالشخص لاتخاذ إجراء معين قد يكون أو لا يكون في مصلحته. ويمكن أن يشمل هذا الحصول على المعلومات، حق الوصول أو الحصول على الهدف لاتخاذ إجراءات معينة "[3].

ومن أشهر المهندسين الاجتماعيين نجد Kevin Mitnick صاحب كتاب فن الخداع (The Art of Deception) الذي تم نشره سنة 2002 تكلم فيه عن كيفية الخداع والتحايل في إقناع الناس واختراق عقولهم .

من خلال التعاريف السابقة يمكن القول أن الهندسة الاجتماعية تستهدف بشكل أساسي العنصر البشري عن طريق استغلال الثغرات الموجودة في طبيعة الإنسان كالخوف، الثقة، الحزن، الإحباط، الرغبة في المساعدة...الخ، مع توظيف مهارات استخدام الأساليب الكلامية، الحيل النفسية أو النصية لتوجيه عقل وتفكير الضحية والتواصل معه بعدة طرق إما شخصيا أو عن طريق الهاتف أو عن طريق البريد الالكتروني ومواقع التواصل الاجتماعي وغيرها من الطرق وهذا من أجل كسب ثقة الضحية ومحاولة الحصول على المعلومات التي يريدها المهندس الاجتماعي مثل: معلومات حساب معين أو أرقام البطاقات الائتمانية...الخ. كما يكون غرض استعمال الهندسة الاجتماعية في غالب الأحيان لأغراض غير أخلاقية مثل: السرقة، التشهير، المساومة...الخ.

كما تجدر الإشارة إلى أن المهندس الاجتماعي ليس في حاجة إلى معرفة تقنية عالية، وإنما يحتاج المهارات الاجتماعية والتسويقية والإقناع من أجل خداع الضحية وأخذ ما يريده دون إثارة الشبهات. لكن إذا اجتمعت المعرفة التقنية بأساليب الهندسة الاجتماعية غير التقنية فإن ذلك يشكل تهديد أكبر بكثير من مجرد المعرفة التقنية لوحدها.

يقوم المهاجم بتنفيذ الهجمات الاجتماعية في شكل تسلسل عبر المراحل التالية [4] :

1. **جمع المعلومات وتحديد الهدف:** في هذه المرحلة يتم جمع أكبر قدر من المعلومات حول الضحية عن طريق المواقع الالكترونية المختلفة مثل: مواقع التواصل الاجتماعي، المدونات، موقع المؤسسة وما إلى ذلك. كما يتم أيضا البحث في سلة المهملات عن معلومات إضافية حول الضحية. وتمثل هذه المرحلة أساس نجاح الهندسة الاجتماعية. بعد إتمام مرحلة جمع المعلومات، يقوم المهاجم باختيار الضحية المستهدفة من أجل بناء وتطوير العلاقة كمرحلة ثانية .
2. **تطوير العلاقة:** يحاول المهاجم خلال هذه المرحلة بناء علاقة مع الضحية المستهدفة والعمل على تطويرها عن طريق استغلال نقاط الضعف لديها (العاطفة، الثقة...الخ) حتى يتمكن من استخراج وانتزاع المعلومات الحساسة التي يريدها مثل: معلومات الحساب، أرقام بطاقة الائتمانية، معلومات الدخول وما إلى ذلك.
3. **استغلال العلاقة:** بمجرد بناء العلاقة مع الضحية المستهدفة وتطويرها يقوم المهاجم باستغلالها لصالحه.
4. **التنفيذ والوصول إلى الهدف:** في هذه المرحلة يقوم المهاجم بالتنفيذ الفعلي لما تم التخطيط له ومحاولة الوصول إلى الهدف النهائي. وفي حالة عدم وصول المهاجم إلى النتائج المرغوبة، فإنه من الممكن أن يعمل على تكرار الخطوات السابقة.

ثانيا: الفئات المستهدفة لهجمات الهندسة الاجتماعية ودوافع تنفيذيها

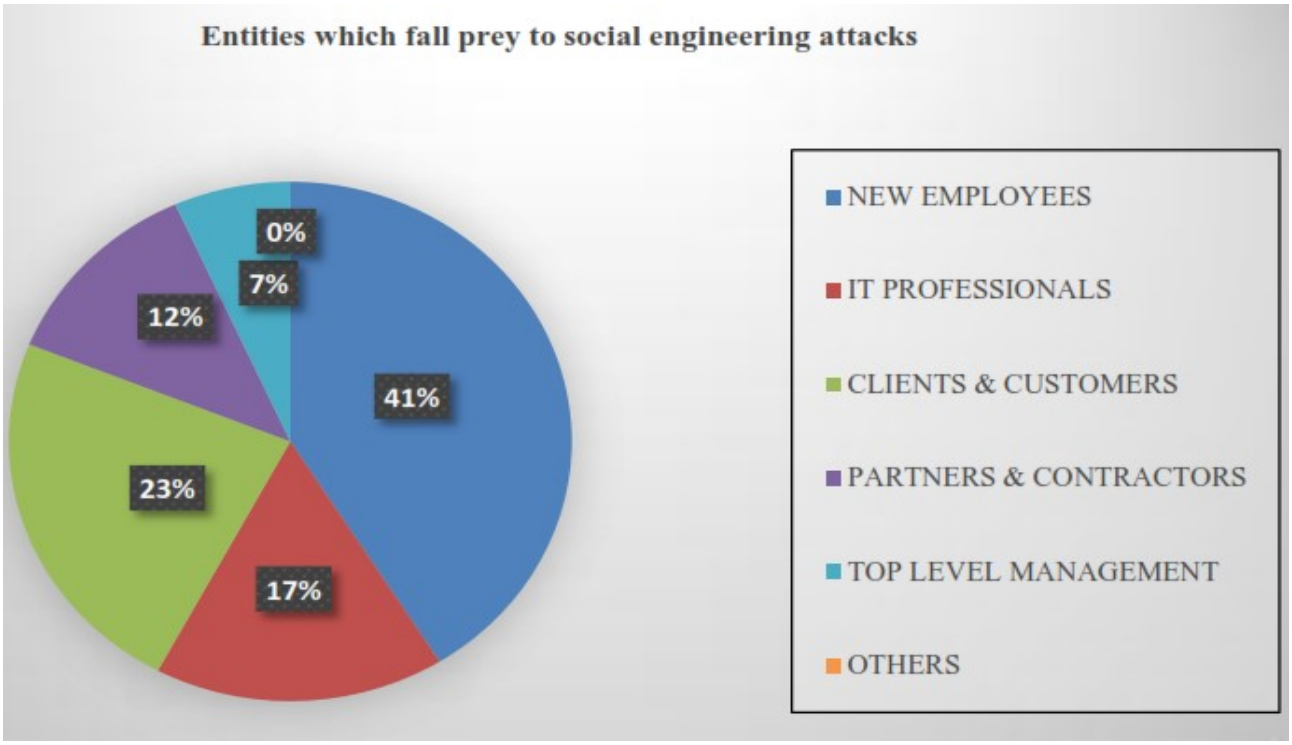
يعتمد المهندس الاجتماعي في تنفيذ هجمات الهندسة الاجتماعية بصورة كبيرة على التفاعل البشري للإيقاع بالضحية المستهدفة وتكون له دوافع من وراء شن هذا الهجوم حسب الأهداف أو المكاسب التي يريد الوصول إليها سواء كانت مادية ملموسة كالمال أو غير ملموسة.

توصلت الدراسة التي قام بها الباحثون (Chitery, Singh, Bag, & Singh) في 2012 حول الفئات الأكثر استهدافا لهجمات الهندسة الاجتماعية إلى النتائج التالية :

- ✓ الموظفين الجدد؛
- ✓ الزبائن والمستهلكين؛
- ✓ المتخصصين في تكنولوجيا المعلومات؛
- ✓ الشركاء والمتعاقدين؛
- ✓ المدراء في المستوى الإدارة العليا؛
- ✓ فئات أخرى.

والشكل التالي يوضح النتائج سابقة الذكر.

الشكل رقم (01): الفئات المستهدفة لهجمات الهندسة الاجتماعية



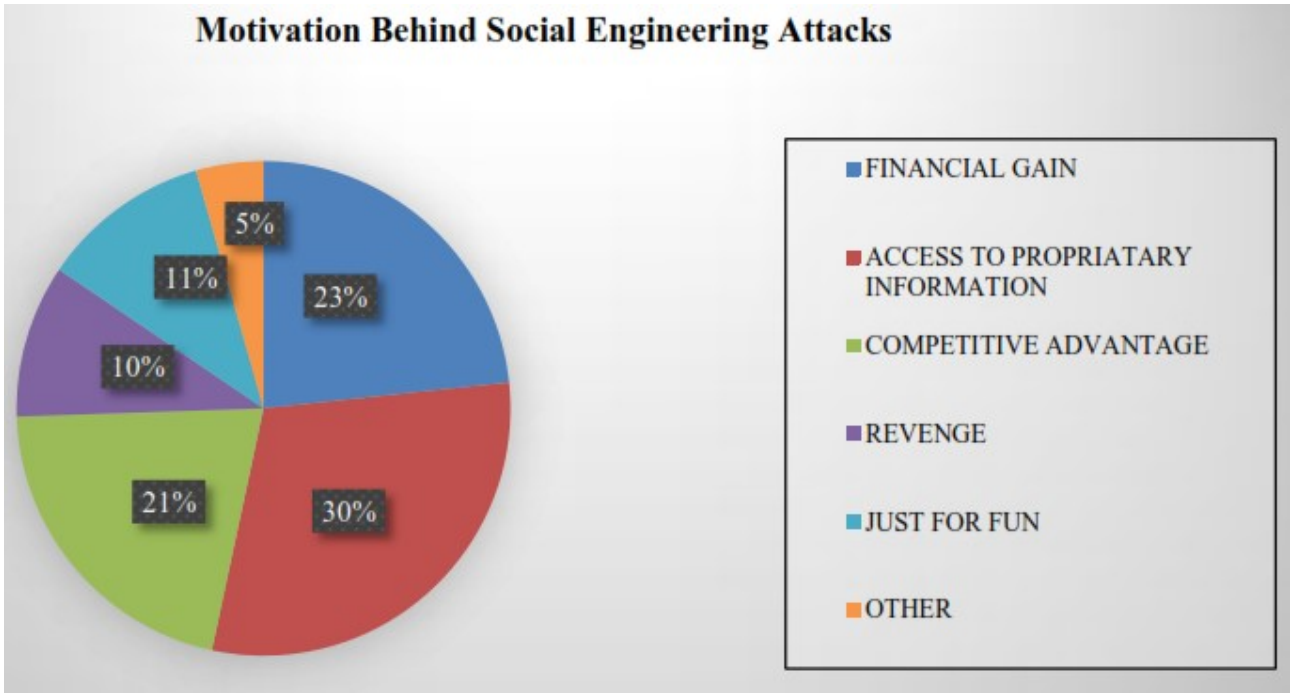
المصدر: **http://dx.doi.org/10.19101/IJACR.2016.623006 [5]**

فمن خلال نتائج الدراسة السابقة، يمكن القول أن أي شخص في الوقت الحاضر معرض لهجمات الهندسة الاجتماعية على اعتبار أنها تركز بشكل أساسي على العنصر البشري .

وأوردت نفس الدراسة السابقة وجود عدة دوافع وراء استخدام هجمات الهندسة الاجتماعية، حيث كانت النتائج على النحو التالي وكما هي موضحة في الشكل أدناه.

- ✓ تحقيق مكاسب مالية؛
- ✓ الحصول على المعلومات؛
- ✓ الحصول على معلومات حول المنافسة؛
- ✓ دوافع الانتقام؛
- ✓ الترفيه والتسلية؛
- ✓ دوافع أخرى.

الشكل رقم (02): دوافع تنفيذ هجمات الهندسة الاجتماعية



المصدر: [6] http://dx.doi.org/10.19101/IJACR.2016.623006

ثالثا. الأساليب المستخدمة في الهندسة الاجتماعية

يمكن تقسيم الأساليب المستخدمة في هجمات الهندسة الاجتماعية إلى نوعين:

- **هجمات الهندسة الاجتماعية المستندة إلى الإنسان (غير تقنية)؛**
- **هجمات الهندسة الاجتماعية قائمة على أساس تقني (استخدام الحاسوب والهاتف .)**

1. هجمات الهندسة الاجتماعية المستندة إلى الإنسان:

يعتمد هذا النوع من الهجمات على التفاعل مع الأشخاص وتوجد عدة طرق نذكر منها:

أ- **التظاهر والتستر مع انتحال الهوية** :(**Pretexting**) يقوم المهندس الاجتماعي بخلق سيناريو معين لإقناع الضحية المستهدفة للكشف عن المعلومات الحساسة وسرقتها. يشمل هذا السيناريو في بعض الحالات على إنشاء هوية جديدة كاملة لخداع والتلاعب بالضحية [7].

ب- **اختلاس النظر من الكتف** :(**Shoulder Surfing**) عملية مراقبة أو النظر إلى الشخص والوقوف بجانبه وهو يقوم بكتابة أو إدخال المعلومات الخاصة به مثل: كلمة المرور، أرقام الحسابات وغيرها من المعلومات [8].

ت- **تتبع الشخص من خلال الباب** :(**Tailgating**) عبارة عن تقنية تسمح لشخص غير مصرح له بالدخول بتتبع شخص أخر (موظف) مصرح له بالدخول والاستفادة من امتيازات هذا الأخير من أجل الدخول إلى منطقة آمنة والحصول على معلومات حساسة [9].

ث- **التنكر في هيئة الدعم الفني** :(**Support Staff/ Tech Support**) يقوم المهندس الاجتماعي بالتنكر في هيئة الدعم الفني للمؤسسة للحصول على المعلومات ويوهم الضحية بوجود خلل أو مشكلة ما في النظام ويطلب منها تقديم معلومات الدخول لحل المشكلة [10].

ج- **الهندسة الاجتماعية العكسية :(Reverse Social Engineering)** يقوم المهاجم بإقناع الضحية المستهدفة بوجود مشكلة من نوع ما أو قد تكون هناك مشكلة في المستقبل ومن ثم يعرض نفسه لحلها. وهذا الأمر يسمح له بالحصول على المعلومات المطلوبة [11].

كما توجد أنواع أخرى من الأساليب كالبحث عن المعلومات في سلة المهملات (Dumpster Diving) ومحاولة استرجاعها، التنصت (Eavesdropping) ويشير إلى عملية الاستماع غير المصرح به أو القراءة غير مصرح بها للرسائل. ويشمل أي شكل من أشكال اعتراض الاتصال، بما في ذلك الصوت والفيديو، أو المكتوب. كما يمكن للمهاجم أن ينتقل شخصيا (Inperson) إلى موقع الهدف وفحص منظومة المعلومات...الخ .

2. هجمات الهندسة الاجتماعية قائمة على أساس تقني:

يعتمد المهندس الاجتماعي في تنفيذ هذا النوع من الهجمات بصفة عامة على التكنولوجيا (البرامج الخبيثة المختلفة، التطبيقات والبرمجيات مثل رسائل البريد الالكتروني، الدردشة...الخ) للحصول على المعلومات المطلوبة ومن أمثلة ذلك نذكر:

أ- **رسائل التصيد الالكتروني**: (**Phishing**) عبارة عن إرسال البريد الإلكتروني لعدد كبير من الضحايا يظهر على أنه مرسل من مصدر شرعي (بنك، مؤسسة، دعم فني، مصلحة الزبائن...) لخداع الضحية المستهدفة والحصول على المعلومات [12]. هذه المعلومات يمكن أن تكون بيانات الدخول، تفاصيل حساب معين أو أرقام بطاقة ائتمانية...الخ. ويعتبر هذا النوع من الاحتيال الأكثر انتشارا اليوم.

تحتوي رسالة التصيد الالكترونية على رابط لموقع مزيف مشابه تماما للموقع الرسمي للمؤسسة وعند الضغط عليه وملأ البيانات يتم توجيه الضحية للموقع الرسمي للمؤسسة بعدما حصل المهاجم على البيانات. كما يكمن إرسال احتيال الكتروني في شكل ملف مرفق يطلب من الضحية أن يفتحه بغرض اختراق جهازه.

ب- **رسائل التصيد الالكتروني مع تحديد الهدف: (Spear Phishing)** هو نفسه التصيد الالكتروني عن طريق الرسائل الالكترونية لكن الفرق هنا أن **Spear Phishing** يتم إرساله إلى أهداف معينة ومحددة وليس بصفة عشوائية (التركيز على شخص معين، قسم معين في المؤسسة...) [13]**.** أي أن المهاجم سوف يقوم بتوظيف أسلوب أكثر شخصية في تنفيذ الهجوم مستهدفا إدارات محددة أو أفراد داخل المؤسسة لضمان تحقيق الاستجابة المطلوبة.

ت- **التصيد الصوتي: (Vishing or Voice Phishing)** يحاول المهاجم التأثير والتحايل على الضحية عن طريق الاتصال الهاتفي مستخدما في ذلك مختلف الأدوات والتقنيات [14]**.**

يستخدم المهاجم نظام نقل الصوت عبر الانترنت Voice over Internet Protocol وينتحل هوية معينة مثل البنك أو شركة اتصالات أو ويستطيع حتى تزييف رقم الهاتف ليظهر بصفة شرعية وعند الرّد يتم توجيه الضحية إلى رقم هاتفي آخر أو في حالة الاتصال بالرقم الجديد يطلب المعلومات الشخصية.

وقد يتلقى الضحية اتصالا من رقم مزيّف ويكون عبارة عن اتصال مسجّل مسبّقا يقوم بتوجيه الضحية إلى موقع على الانترنت يفترض وجود مشكلة ما تتعلق بحسابه، وهذا الموقع ما هو إلا موقع تصيد إلكتروني.

كما يوجد نوع أخر من التصيد الالكتروني وهو **(Smishing)** باستخدام الرسائل النصية الفورية والوسائط المتعددة.

ث- **تزوير المواقع الإلكترونية: (Pharming)** تهدف هذه الطريقة الاحتيالية إلى إلحاق الضرر بخادم نظام أسماء النطاقات DNSمما يؤدي إلى إعادة توجيه طلب الضحية إلى موقع احتيالي الذي يقع تحت سيطرة المهاجم [15]**.**

عندما يكتب الضحية عنوان الموقع، فإنه يقوم بإعادة التوجيه إلى موقع مزور على شبكة الانترنت يكون مشابه تماما للموقع الأصلي. كما يمكن للمهاجم أن يصيب جهاز الضحية بـ Trojan Horse لسرقة اسم المستخدم وكلمات المرور وغيرها من المعلومات الحساسة.

ج- **التصيد عن طريق (Scareware) للإيقاع بالضحية:** عبارة عن برمجيات ضارة تظهر في شكل نوافذ وإعلانات منبثقة تخبر الضحية أنه مصاب ببرنامج خبيث أو يوجد خلل في نظام التشغيل ويجب عليه الضغط على النافذة لتحميل مكافح فيروسات وهمي وعمل فحص للجهاز [16]**.**

في حقيقة الأمر يتم التحايل على الضحية عن طريق الضغط على النافذة المنبثقة أو الإعلان ليقوم بتحميل برنامج وهمي الهدف منه زرع برنامج خبيث في الجهاز لسرقة المعلومات الحساسة. وفي المقابل يظن الضحية أنه قام بتثبيت برنامج حماية في جهازه .

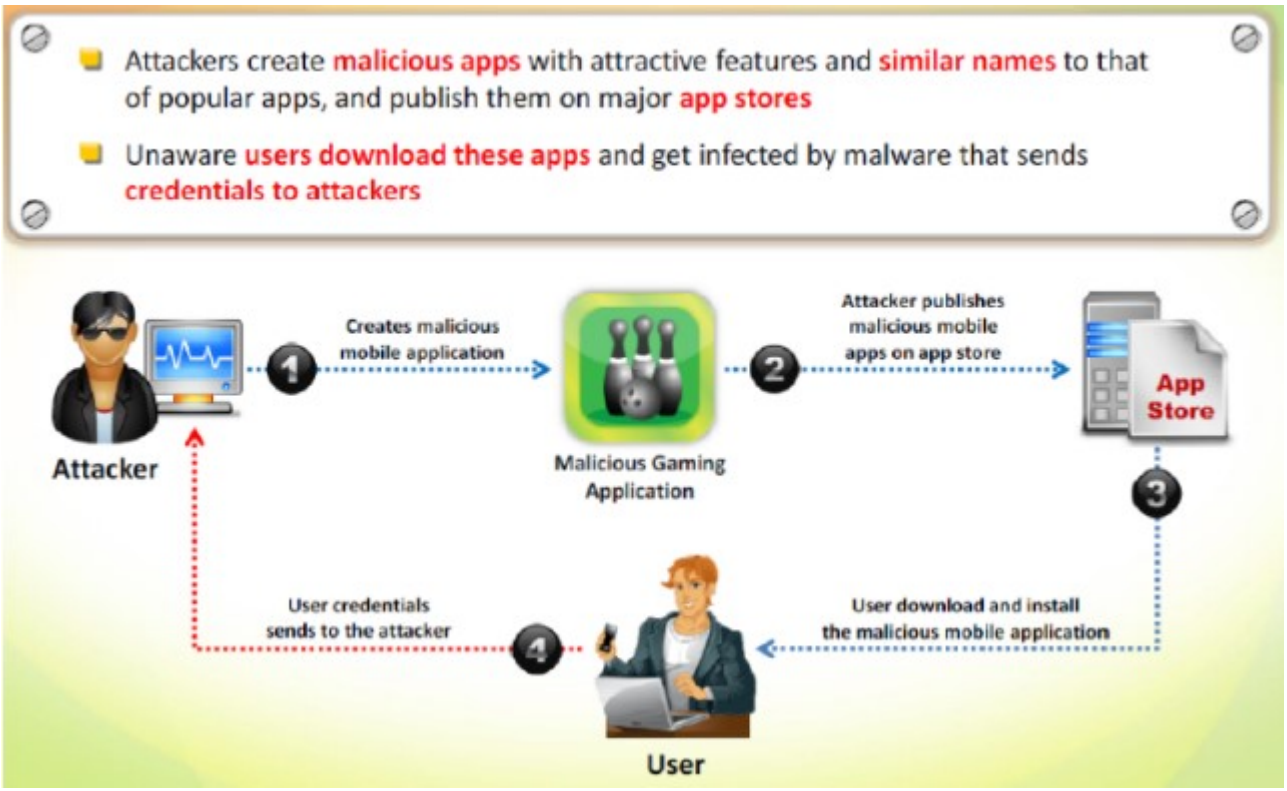
ح- **التصيد عن طريق الطعم: (Baiting)** يقوم المهاجم بإغراء الضحية وإيهامه بجدية الموضوع وأهميته بدخول موقع معين لتحميل الملفات أو ما شابه (برامج، موسيقى، أفلام...الخ) وبهذه الطريقة يسعى إلى الحصول على بياناته الخاصة. ولا يقتصر هذا النوع من الهجمات على شبكة الانترنت وإنما يستطيع المهاجم استخدام أدوات مادية مثل ترك جهاز USB مصاب ببرنامج خبيث في مكان يسهل إيجاده وبمجرد ربطه بالجهاز يبدأ البرنامج الخبيث في عمل اتصال مع جهاز المهاجم [17].

خ- **التصيد عن طريق تطبيقات الهاتف الذكي:** يقوم المهاجم بتنفيذ هجمات الهندسة الاجتماعية عن طريق استغلال تطبيقات الهاتف الذكي وذلك من خلال:

- **تصميم ونشر تطبيقات خبيثة في مختلف متاجر التطبيقات (Play Store, Apple Store...)؛**
- **تنزيل تطبيقات شرعية من متاجر التطبيقات ودمجها ببرامج خبيثة وإعادة تجميعها ورفعها إلى متاجر التطبيقات؛**
- **استخدام التطبيقات الأمنية الوهمية.**

والأشكال التالية توضح مختلف الأساليب السابقة.

الشكل رقم (03): التصيد عن طريق نشر التطبيقات الخبيثة في متاجر التطبيقات

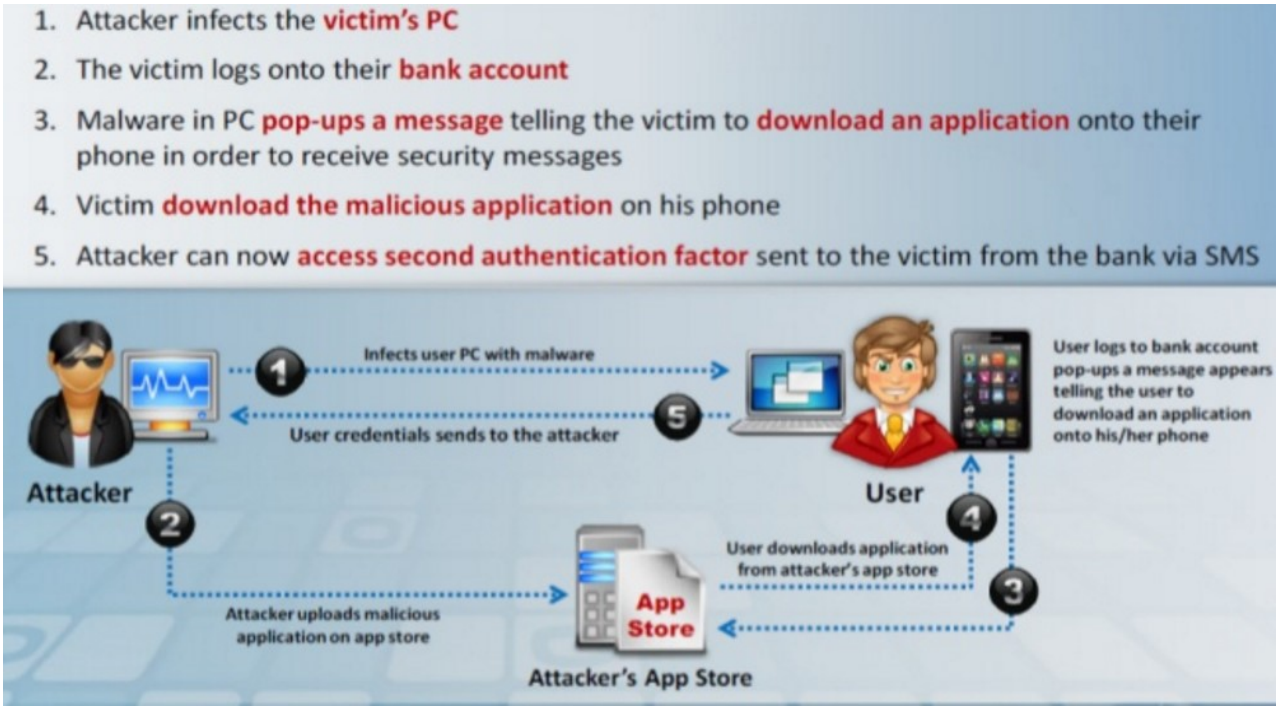


المصدر: **https://www.eccouncil.org/programs/certified-ethical-hacker-ceh[18]**

الشكل رقم (04): التصيد عن طريق دمج برامج خبيثة داخل تطبيقات شرعية

المصدر: **https://www.eccouncil.org/programs/certified-ethical-hacker-ceh [19]**

الشكل رقم (05): التصيد عن طريق استخدام تطبيقات أمنية وهمية



المصدر: **https://www.eccouncil.org/programs/certified-ethical-hacker-ceh [20]**

ويوجد أسلوب ثالث من أساليب تنفيذ هجمات الهندسة الاجتماعية وهو يجمع بين التفاعل البشري والجانب التقني وذلك عن طريق استخدام مواقع التواصل الاجتماعي بمختلف أنواعها.

رابعا: أمثلة على هجمات الهندسة الاجتماعية وتقديم بعض الطرق العملية للحد منها

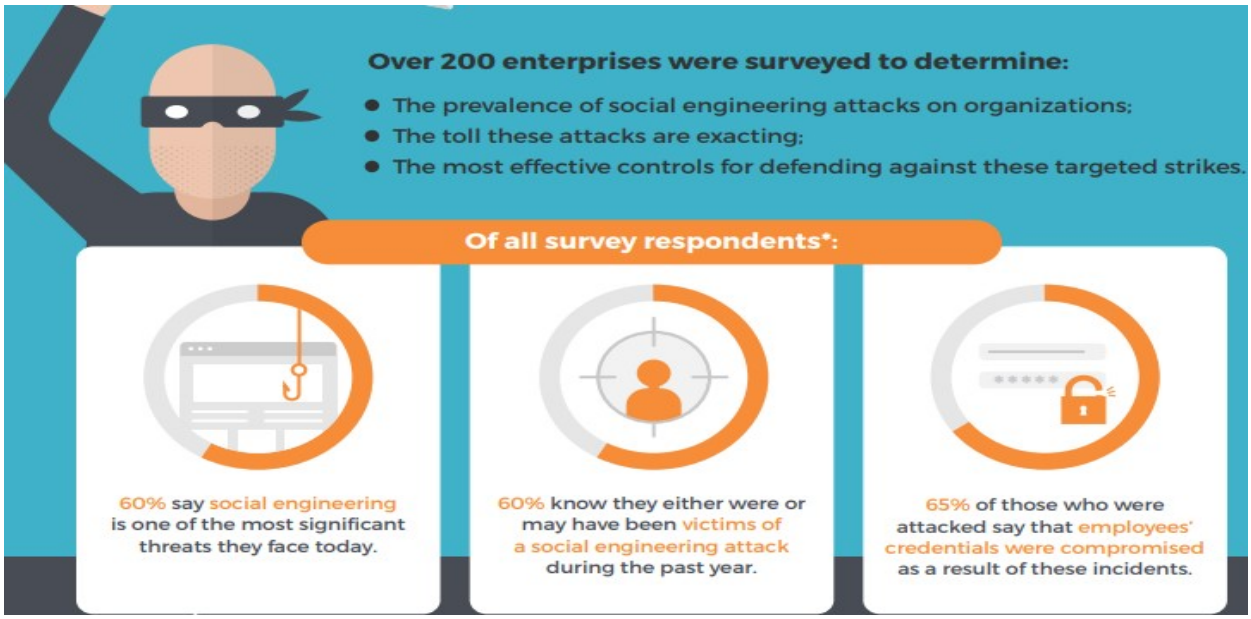
نستعرض في مايلي بعض الأمثلة الواقعية حول هجمات الهندسة الاجتماعية التي تعرض لها الأفراد والمؤسسات مع توضيح الأساليب التي اعتمدها المهاجم في تنفيذ الهجوم. بالإضافة إلى تقديم بعض الطرق العملية التي يمكن إتباعها للحد منا.

مثال (1) بعض إحصائيات 2016 حول الهندسة الاجتماعية

في 2016، قامت المؤسسة **AGARI** المتخصصة في أمن المعلومات بدراسة على أكثر 200 مؤسسة من أجل معرفة مدى تعرض المؤسسات والأشخاص لهجمات الهندسة الاجتماعية، فكانت نتائج الدراسة كما يلي:

- 60% من الذين تم استجوابهم أكدوا أن الهندسة الاجتماعية تشكل أحد أكبر التهديدات في الوقت الراهن.
- 60% قالوا إنهم تعرضوا لهجمات الهندسة الاجتماعية في السنة الماضية.
- 65% من الذين تعرضوا لهجمات الهندسة الاجتماعية قالوا أن البيانات الخاصة بالموظفين تعرضت للخطر كنتيجة لهذا النوع من الهجمات.

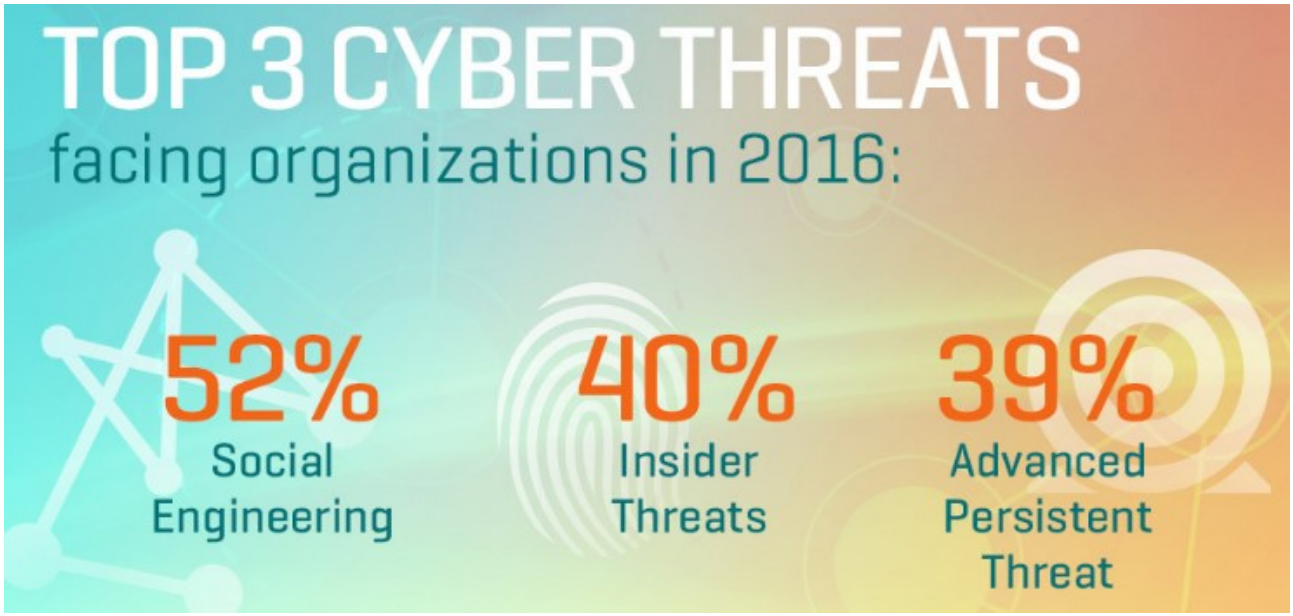
الشكل رقم (06): بعض إحصائيات 2016 حول هجمات الهندسة الاجتماعية



المصدر: https://www.agari.com [21]

وحسب اتحاد تدقيق ومراقبة أنظمة المعلومات Information Systems Audit and Control Association (**ISACA**) فإن أكبر التهديدات التي تعرضت لها المنظمات في 2016 هي من نوع هجمات الهندسة الاجتماعية كما هو موضح في الشكل التالي.

الشكل رقم (07): أكبر التهديدات التي تعرضت لها المؤسسات في 2016



المصدر: https://www.isaca.org/pages/2016-cybersecurity-snapshot.aspx [22]

مثال (2): إنشاء صفحة مزيفة Fake profiles وخداع الضحية المستهدفة

في جانفي 2017 تم استخدام حساب مزور تحت اسم "**Mia Ash**" على مواقع التواصل الاجتماعي Facebook، Instagram، DeviantArt، LinkedIn على أساس أنها مصوّرة فوتوغرافية وقامت بنشر عدّة صور وكتابات على صفحاتها لإضفاء نوع من الشرعية [23].

طريقة التنفيذ

جاء ضمن التقرير الذي نشره باحثوا شركة Secure Works Counter Threat Unit في 2017 حول الهجمات التي تتعرض لها المؤسسات وجدوا أن العديد من الهجمات كانت تستهدف مؤسسات في الشرق الأوسط وشمال أفريقيا.

وحسب الباحثين فإن المهاجم استخدم حساب LinkedIn المزور "Mia Ash» في شن هجمات الهندسة الاجتماعية وفق المراحل التالية:

1- إنشاء صفحة مزورة؛

2- البحث عن الضحية في موقع LinkedIn للشركة المستهدفة؛

3- إضافة الضحية والتواصل معه (بناء العلاقة وكسب الثّقة)؛

4- تطوير العلاقة إلى مواقع أخرى Facebook واستخدام البريد الالكتروني وتطبيقات WhatsApp؛

5- بعد مدّة من استقرار العلاقة وكسب الثّقة أرسل المهاجم ملف Microsoft Excel إلى الضحية عن طريق البريد الالكتروني للمؤسسة وطلب منه فتحه في مكان العمل وكانت النتيجة تسميم كل حواسيب المؤسسة ببرنامج خبيث PupyRAT واستطاع فيما بعد الولوج إلى بيانات المؤسسة.

ومن خلال ما يأتي نستعرض بعض الطرق العملية التي يمكن اعتمادها للحد من خطر هجمات الهندسة الاجتماعية [24]:

- ✓ الحرص على الخصوصية وعدم نشر كافة المعلومات الشخصية على شبكة الانترنت ومواقع التواصل الاجتماعي؛
- ✓ التحقق من رسائل البريد إلكتروني والمكالمات الهاتفية خاصة التي تطلب معلومات شخصية أو تطلب تحديثها؛
- ✓ الحذر من الروابط في الرسائل الالكترونية أو الملفات المرفقة حتى لو ظهر أن البريد الإلكتروني مرسل من مصدر شرعي لأنه في الغالب ما تكون مواقع التصيد الالكتروني عبارة عن نسخ مطابقة تماما للمواقع الأصلية؛
- ✓ عدم تنزيل تطبيقات الهواتف الذكية من مصادر غير موثوقة؛
- ✓ تدريب المستخدمين بشكل دوري في المؤسسات وتوعيتهم بالأساليب المستخدمة في هجمات الهندسة الاجتماعية؛
- ✓ إجراء اختبار الهندسة الاجتماعية على الموظفين تقوم بها مؤسسات متخصصة في أمن المعلومات الذي من شأنه إبقاء الموظفين على إطلاع دائم على أحدث المستجدات فيما يخص هذا النوع من الهجمات؛

بالإضافة إلى ما سبق، يمكن استخدام النصائح التالية:

- ✓ وضع سياسة أمنية صارمة بالنسبة للمؤسسات للحد من خطر الهندسة الاجتماعية
- ✓ استخدام كلمة مرور مختلفة لكل موقع مع الحرص على تغييره بشكل دوري وتفعيل خاصية الحماية المزدوجة* Two-Factor Authentication (**2FA**)؛
- ✓ تحديث برامج الحاسوب المختلفة بشكل دوري، حيث يستغل المهاجم الثغرات المكتشفة في البرامج المستخدمة بشكل كبير مثل نظام التشغيل، البرامج المكتبية (**Office**) ومتصفحات الانترنت ...الخ؛
- ✓ التأكد من عناوين المواقع في شريط العنوان من أنها تبدأ بـ: هو: "**https**" وليس "**http**"؛
- ✓ الحرص عند استخدام الحواسيب العمومية (في مقاهي انترنت، المحلات التجارية، مطارات...الخ).

وبصفة عامة يبقى نشر ثقافة أمن المعلومات على مستوى الفرد والمؤسسات أمر ضروري.

خاتمة:

إن زيادة الاعتماد على شبكة الانترنت كوسيلة للتسوق الإلكتروني وتحويل الأموال خلال السنوات الماضية، ساعد ذلك على ظهور خدمات جديدة تسمح بربط المستخدمين بشكل مباشر لتبادل المنافع وشراء المنتجات والخدمات والتي شكلت بدورها مرتعا خصبا للمهاجمين لاستغلال تلك الخدمات ونصب حبائل الاحتيال من خلال تنفيذ هجمات الهندسة الاجتماعية.

ومن خلال هذه الورقة البحثية تم التعرف على الهندسة الاجتماعية التي تعتبر من أكبر المشكلات التي تواجه الأفراد والمؤسسات في الوقت الحالي وهذا حسب الدراسات التي قام بها الباحثون والمؤسسات المتخصصة في أمن المعلومات.

فالهندسة الاجتماعية تركز هجماتها بشكل أساسي على استغلال العنصر البشري وهذا ما يجعلها من أخطر الهجمات التي يصعب التنبّؤ بها والتصدي لها، وذلك لكون أساليب الهندسة الاجتماعية دائما في تطوّر مستمر، ولهذا يتطلب الأمر نشر التوعية حول مدى خطورتها من خلال القيام بدورات تدريبية للموظفين ووضع سياسات وإجراءات تحدد فيها سياسة الأمن بالنسبة للمؤسسات ونشر ثقافة أمن المعلومات بالنسبة للأفراد بصفة عامة.

التوصيات والمقترحات:

لقد أصبح المستهلك في ظل التطوّر المستمر لتكنولوجيا المعلومات والاتصال عرضة للتلاعب بمصالحه ومحاولة غشه وخداعه والتحايل عليه عن طريق استخدام أساليب الهندسة الاجتماعية التي تعتبر من أنجع الوسائل التي يتمّ استخدامها نظرا لسهولتها مقارنة بالوسائل التقنية الأخرى. وأن عدم وجود الوعي الكافي في مجال الهندسة الاجتماعية لدى المستهلك هو السبب الرئيسي وراء هذه المشكلات، لذلك لابد من رفع درجة وعي المستهلك بالهندسة الاجتماعية وأساليبها في الحفاظ على الخصوصية الرقمية، وحماية المعلومات الحساسة، خاصة والجزائر مقبلة على إجراء مختلف التعاملات في إطار التجارة الالكترونية.

الإحالات:

(*):**"FA2"** هي طريقة تتيح للمستخدم التعريف عن نفسه باستخدام أسلوبين مختلفين للتوثيق، فعلى سبيل المثال عند تفعيل خاصية الحماية المزدوجة لموقع معين فبالإضافة إلى إدخال اسم المستخدم وكلمة المرور، الموقع يطلب رمز أو مفتاح أمان من أجل الدخول وهذا حسب طريقة تفعيل الخاصية (رسالة نصية تصل على الهاتف أو البريد الالكتروني، مفتاح أمان مسجل...الخ).

قائمة المراجع (الهوامش):

1. M. Bezuidenhout, F. Mouton, and H. S. Venter, “Social engineering attack detection model: SEADM”,in Information Security for South Africa, 2010, page 1.

2. https://www.social-engineer.org/framework/general-discussion/social-engineering-defined, [accessed 10 September 2017].

3. Christopher Hadnagy, “Social Engineering: The Art of Human Hacking”, Wiley publishing, 2011, page 32.

4. I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, “Social engineering attack strategies and defence approaches”, in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud(FiCloud). IEEE, 2016, page 146.

5. http://dx.doi.org/10.19101/IJACR.2016.623006, [accessed September 12, 2017].

6. Ibid.

7. Michael Alexander, “Methods for Understanding and Reducing Social Engineering Attacks”,SANS Institute,April 30, 2016, page 11.

8. R. Dhull, Prof. Sugandha Singh Hooda, “Contrast Study of Social Engineering Techniques”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 4, (Jul.-Aug. 2016), Page 66.

9. Ibid.

10. Anshul Kumar, Nagresh Kumar, Social Engineering: Attack, Prevention and Framework, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 4, Issue II, February 2016 ، page 571.

11. R. Dhull, Prof. Sugandha Singh Hooda, “Contrast Study of Social Engineering Techniques”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 4, (Jul.-Aug. 2016), page 67.

12. Zrinka Lovrić Švehla, Ivan Sedinić and Luka Pauk, “Going White Hat: Security Check by Hacking Employees Using Social Engineering Techniques”, Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention, IEEE, 30 May-3 June 2016, page 1419.

13. Michael Alexander, “Methods for Understanding and Reducing Social Engineering Attacks”,SANS Institute,April 30, 2016, page 8.

14. Zrinka Lovrić Švehla, Ivan Sedinić and Luka Pauk, Op.Cit., page 1419.

15. S. Gastellier-Prevost, G. Gonzalez Granadillo and M. Laurent, “A Dual Approach to Detect Pharming Attacks at the Client-Side”, New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference, IEEE, 2011, page 2.

16. https://usa.kaspersky.com/resource-center/definitions/scareware, [accessed September 14, 2017].

17. Michael Alexander, Op.Cit., page 10.

18. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh, [accessed September 15, 2017].

19. Ibid.

20. Ibid.

21. https://www.agari.com, [accessed September 16, 2017].

22. https://www.isaca.org/pages/2016-cybersecurity-snapshot.aspx, [accessed September 16, 2017].

23. https://me.kaspersky.com/blog/mia-ash/4873, [accessed September 17, 2017].

24. A. Jain, H. Goswami, M. Singh Sankhla,R. Kumar, Social Engineering: Hacking a Human Being through Technology,2016, page 98.