إضاءات

نشرة توعوية يصدرها معهد الدراسات المصرفية

دولة الكويت - مارس 2019

السلسلة 11 العدد 4

الهندسة الاجتماعية

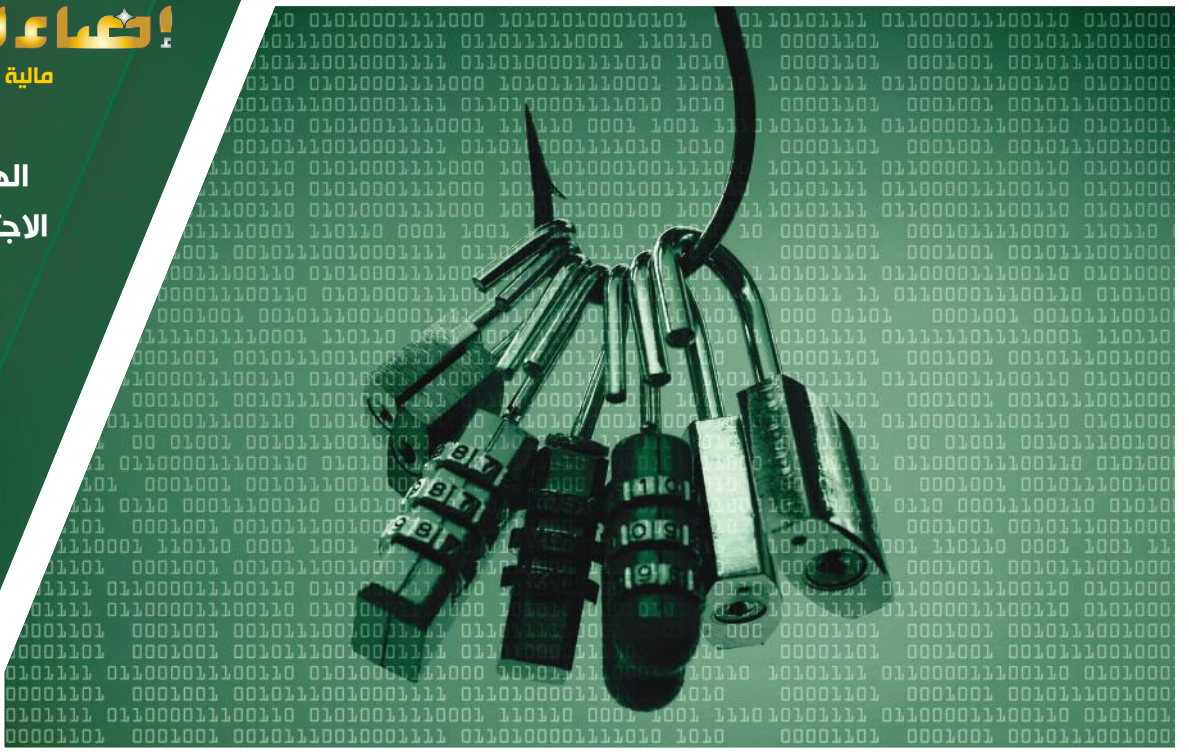
Social Engineering

الهندسة الاجتماعية هي فن اختراق عقول البشر وخداعهم بهدف الحصول على معلومات أو بيانات أو أموال كانت ستظل خاصة وآمنة ولا يمكن الوصول إليها. ولقد أصبحت الهندسة الاجتماعية، ذات شعبية كبيرة في السنوات الأخيرة نظراً للنمو الهائل والمتسارع لشبكات التواصل الاجتماعي والبريد الإلكتروني والأشكال الأخرى للاتصالات الإلكترونية. ولهذا، سوف نتطرق في هذا العدد إلى عرض أهم الأساليب والتقنيات المستخدمة والإرشادات الأمنية الواجب إتباعها.

محاور العدد:

- **مفهوم الهندسة الاجتماعية**
- **أدوات التحايل وعلامات الهجوم**
- **أسباب انتشار الهندسة الاجتماعية**
- **وسائل الهندسة الاجتماعية**
- **دور العنصر البشري في تسريب كلمة المرور**
- **أهم السلوكيات الخاطئة الواجب تجنبها**
- **كلمة أخيرة**

الهندسة الاجتماعية



مفهوم الهندسة الاجتماعية

مع انتشار الشبكات الاجتماعية واختلاف أنماطها من محادثات كتابية إلى صوتية وفيديو وبث مباشر وغيرها الكثير، والتي تهدف إلى اقتحام الخصوصية وسحب أكبر قدر من المعلومات، والتي قد يعتبرها البعض أمراً غير مهم، ظهر علم جديد من الاختراق يعرف بالهندسة الاجتماعية والتي لا تعتمد على دراسة أو أساسيات برمجية أو أكاديمية لمفاهيم الاختراق الإلكتروني، لكنها تحتاج إلى مهارة وفن وتقنيات لاختراق عقول البشر وجمع أكبر قدر من المعلومات عن الضحايا من أجل أغراض لا أخلاقية مثل: السرقة أو التشهير أو نشر الرذائل. والركيزة التي انطلقت منها هي اختراق الحلقة الأضعف في سلسلة أمن المعلومات، ألا وهي العنصر البشري، ولإتمام عملية البرمجة الذهنية اعتمدت الهندسة الاجتماعية على التعامل مع الغرائز البشرية التي تعتبر ثغرات موجودة في الطبيعة الإنسانية مثل الخوف والثقة والطمع والفضول والرغبة في المساعدة والانجذاب للأشخاص المشابهين، وغيرها من خلال أساليب مختلفة أهمها الإنترنت، والمتمثل بالرسائل الإلكترونية والمواقع المزيفة والشبكات الاجتماعية.

أدوات التحايل وعلامات الهجوم

يستخدم المخترق المتحايل "المهندس الاجتماعي" مهاراته لاستهداف نقاط الضعف البشرية في محاولة للتحايل على الضوابط والإجراءات التي من شأنها أن تمنعه من الحصول على المعلومات التي يحتاجها. ويعتمد في هجومه على أساسين:

- أن الأفراد لا يدركون قيمة المعلومات التي يمتلكونها.
- التساهل من قبل الأفراد في حماية معلوماتهم أو الإهمال.

الفرق الرئيسي بين المهاجم الذي يستخدم تقنيات الهندسة الاجتماعية وما يعرف باسم الهاكر، أن الأخير يستخدم وسائل البرمجيات والتقنيات للوصول إلى مبنى أو نظام لسرقة المعلومات، في حين يستخدم الأول الأساليب الاجتماعية مثل: تكوين صداقات أو اللعب بالعواطف، أو الإكراه والابتزاز في بعض الأحيان.

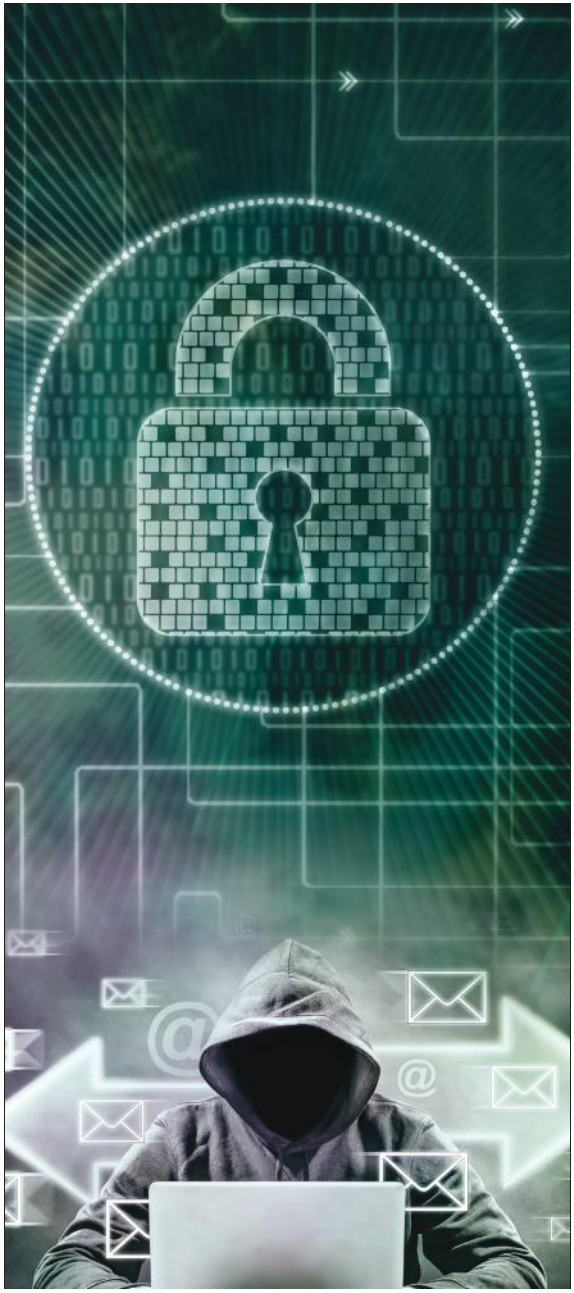
المهندس الاجتماعي له قدرة عالية على اصطياد الضحية من خلال دراسة شخصيته ومعرفة الحيل الممكن استخدامها معه، وقد ينتحل وظائف وشخصيات متعددة لكي يمارس القرصنة والوصول للهدف. وعادة ما يكون الأشخاص المستهدفون هم: العملاء والمستخدمين، الدعم الفني، موظفو الاستقبال ومكتب المساعدة، ومسؤولي النظام.

أهم علامات التحايل في الهندسة الاجتماعية هي:

- اظهار رقم لا يمكن إعادة الاتصال منه
- تقديم طلبات بطريقة غير رسمية
- طريقة الطلب يكون فيها تسرع وإسقاط اسم من غير قصد
- مجاملة بشكل غير عادي أو الثناء
- استخدام أسلوب التهديد إذ لم تتوفر المعلومات المطلوبة
- الانزعاج من أقل الأسئلة

أسباب انتشار الهندسة الاجتماعية

- الافتقار إلى وضع سياسات وقوانين تحمي النظام ومستخدمي النظام.
- سهولة الوصول لأية معلومة وخاصة مع انتشار الشبكات الاجتماعية ومحركات البحث.
- قلة التدريب في المجال الأمني للمعلومات.
- تقسيم المؤسسة أو الدولة إلى وحدات منفصلة.
- سهولتها مقارنة بالوسائل التقنية الأخرى، حيث يمكن تحقيقها بمجرد انتهاك العلاقات الإنسانية وقد لا تتطلب خبرة كبيرة من الناحية التقنية.
- المعدات الأمنية والتقنية لا تمنع من وقوعها لأنها ترتكز على الجانب الإنساني.
- المهاجم لا يحتاج معدات أو مهارات متخصصة، فهي أسلوب غير مكلف.
- كتمان الضحايا للأخطاء والسرقات التي تحدث لهم.
- عدم إدراك أهميتها ومدى خطورتها من قبل المتخصصين في مجال أمن المعلومات وكذلك مستخدمي الحاسوب.
- صعوبة الكشف عنها وتتبع أثرها.



وسائل الهندسة الاجتماعية

تنوعت الوسائل التقنية لتشمل ما يلي:

1- التصيد Phishing

هو محاولة الحصول على المعلومات الخاصة بمستخدمي الانترنت سواء أكانت معلومات شخصية أو مالية، عن طريق رسائل البريد الإلكترونية أو مواقع الانترنت التي تبدو وكأنها مبعوثة من شركات موثوقة أو مؤسسات مالية أو حكومية، من أجل توصيل رسالة التصيد التي ستقنع الضحية إما بالإفصاح المباشر عن المعلومات أو القيام بإجراء (مثل الدخول إلى موقع وهمي على شبكة الإنترنت أو النقر فوق رابط تحميل لأحد البرامج الخبيثة، .. الخ) يسمح للمهاجم - دون علم الضحية - بالاستمرار في خطته ذات النية السيئة.

يمكن الانتباه من التصيد من خلال الإرشادات التالية:

- حماية جهاز الحاسوب باستخدام برامج مضاد الفيروسات (anti-viruses)، وجدار النار(firewalls) كما يجب تحديثها باستمرار.
- التأكد من تحديث متصفح الإنترنت.
- تنزيل شريط أدوات لمتصفح الإنترنت للحماية من المواقع الإلكترونية المزيفة المعروفة.
- يجب عدم الوثوق بأي رابط وإن كان مرسلا من أحد أصدقائك.
- لا تدخل معلوماتك في أي موقع بشكل عشوائي ودون التأكد من اسم الموقع وصحته.
- التأكد من أن بداية عنوان الموقع في شريط العنوان للمتصفح هو: "https://" فوجود حرف «s» يعني موقع آمن من خلال استخدام تقنية التشفير، بالإضافة إلى أن الصفحة تتضمن توقيع رقمي (digital sign) وبغيرهما معاً يصعب التأكد والوثوق بالصفحة.
- تجنب تعبئة النماذج المتعلقة بالمعلومات المالية أو التي تطلب أية معلومة خاصة في الرسائل الإلكترونية.
- وضع الفأرة /الماوس على الرابط للتأكد أنه يطابق الرابط المكتوب قبل فتحه.
- التأكد من صحة العنوان URL (أخطاء غير ملحوظة) فالمهندسين الاجتماعيين يتعمدون وضع الأخطاء التي لا تلاحظ بسرعة مثل: facebook.co.com أو facceboook.com
- تأكد من عنوان البريد الإلكتروني، وإذا ساورك الشك حول أحد العناوين قم بعمل بحث سريع على جوجل عنه، حيث تقوم كل الشركات الكبرى بوضع قائمة بالعناوين التي ترسل منها الرسائل للمشتركين منعاً للاحتيال.

2- الشبكات الاجتماعية

- يجب معرفة أن معظم حسابات الشبكات الاجتماعية تكون مكشوفة للشركات المالكة له ولديها الحق في نقلها لطرف آخر أو نشرها.
- إن تطبيق الفيسبوك هو أكثر عرضة لهجمات الهندسة الاجتماعية وذلك لتوفر كم كبير من البيانات الشخصية، كما يعاني مستخدمي الفيسبوك غالبا من هجمات الفيروسات، حيث يعتبر وسيلة سهلة لنقل الفيروسات من خلال الصور وغيرها من عناصر متاحة.
- يكون الشخص معرض للاختراق من ناحيتين: الشركة التي تكون مطلعة على جميع بياناتك بالإضافة إلى الصلاحيات التي تسلبها منك، وكذلك اختراق الأفراد والتي قد يحدث بأكثر من طريقة.
- يقوم المهندس الاجتماعي باستغلال البيانات الموجودة في الشبكات الاجتماعية واستخدامها لاختراق الحساب المستهدف، لذلك يجب عدم وضع معلومات خاصة في الشبكات الاجتماعية مهما كانت بسيطة.
- يجب عدم الثقة بالمعلومات أو الأشخاص في الشبكات الاجتماعية، قد يكونوا الطعم لعملية احتيال جديدة.

3- الهواتف

تعد الهواتف أحد أساليب الهندسة الاجتماعية المستخدمة بكثرة في الوقت الحاضر، وتتضمن نوعين، هما:

- مكالمات صوتية وتسمى (Vishing): وهي أن تأتيك مكالمة صوتية تدعي أنك فائز بجائزة نقدية كبيرة مثلا أو أن يعرفك ليقوم بالاحتيال عليك.
- مكالمات نصية وتسمى (Smishing): وهي أن تصل إليك رسالة نصية تثير عندك الفضول أو الطمع ليجبرك أن تقوم بالضغط على رابط يؤدي إلى اختراق جهازك.

4- البرمجيات الخبيثة

- يمكن العثور على العديد من عينات البرامج الخبيثة المثيرة للاهتمام والتي تعتمد على الهندسة الاجتماعية من أجل توصيل هجومها إلى الضحية بشكل فعال، ومن أشهر الوسائل المستخدمة في عملية التوصيل هو ما يُسمى بالتحديثات الوهمية لبرنامج Flash Player، والملفات المدمجة في وثائق وورد، ونسخ المتصفحات المشروعة ذات الجودة المنخفضة مثل إنترنت إكسبلورر وغيرها.

الوسائل غير التقنية

تتضمن كل مما يلي:

- حيل العلاقات العاطفية (Sweetheart Scams)
- حيل الفرص الوظائفية (Online Job Scams)
- انتحال الشخصية: من أهم الشخصيات التي يتم انتحالها: طرف ثالث، دعم الفني، موظف من داخل المؤسسة، أو السلطة.
- تصفح الكتف (Eavesdropping and Shoulder Surfing)

هو محاولة الإطلاع على معلومات الغير والتطفل بقراءتها من دون علم صاحب الجهاز بذلك.

- الغوص في سلة المهملات (Dumpster Diving)

هذا الأسلوب يستخدم في الشركات وفي المنزل وفي مراكز الصراف الآلي وغيرها، إذ يحاول سارقوا الهوية البحث في النفايات لجمع معلومات عنك ثم استخدامها ضدك، حيث يمكن من خلالها الحصول على كمية هائلة من المعلومات المفيدة.

- الهندسة الاجتماعية العكسية (Reverse Social Engineering)

هو هجوم من شخص إلى شخص يقنع فيه المهاجم الهدف بأن لديه مشكلة أو قد يكون لديه مشكلة معينة في المستقبل وأنه هو، المهاجم، مستعد للمساعدة في حل المشكلة.

- حمل على الظهر (Piggybacking)

يشير إلى ملاحقة شخص لشخص آخر مرخص له بالدخول إلى منطقة محظورة، أو تمرير نقطة تفتيش معينة.

دور العنصر البشري في تسريب كلمة المرور

يعد تسريب كلمة المرور (Password) إحدى المخاطر الصادرة من العنصر البشري سواء بطريقة مقصودة أو غير مقصودة. ومن أهم طرق اختراق كلمة المرور:

1- التخمين

تعتبر من أسهل الطرق وأكثرها بدائية، أحيانا تنجح وأحيانا تفشل. قد تنجح في حال استخدام كلمات مرور ضعيفة أو قصيرة، مثل أرقام متسلسلة: 123456 أو أرقام مكررة مثل: 555، أو كلمات سهلة مثل: كلمة "Password"، وغيرها.

ومن أشهر الطرق:

Dictionary attacks
Brute force attacks

2- الخداع

تعتبر هذه الطريقة من أشهر طرق اختراق كلمة المرور، وهي أحد طرق الهندسة الاجتماعية، حيث يقوم من خلالها المهاجم بالحصول على معلومات سرية من المستخدم عن طريق الحيلة أو التصيد.

3- الاختراق

يعتبر الاختراق (Password Cracking) من أكثر الطرق خطورة، وتتم من خلال البرامج الخبيثة مثل Keylogger, Rainbow tables وكذلك Password sniffing

لذلك تجنب عمل ما يلي:

- استناد كلمة السر إلى معلومات شخصية يمكن تخمينها.
- استخدام كلمات ومفردات في القاموس.
- استخدام الأسماء الدارجة.
- كتابة كلمة السر في ورقة.
- ادخال كلمة السر أمام الآخرين.
- مشاركة كلمة السر مع الآخرين.
- استخدام كلمة سر واحدة لأكثر من حساب.
- تخزين كلمة السر في برامج مجهولة المصدر.

وفقا للموقع الالكتروني لصحيفة «ديلي ميل» فقد نصح الخبراء بإضافة حرف إلى الأرقام السرية لزيادة قوتها والتقليل من احتمالية تنبؤها واختراقها، وكذلك استخدام كلمات سر يصعب تخمينها ولتكن مزيج من الحروف الصغيرة والكبيرة، والأرقام، والعلامات التي لا تجدها في القاموس، والتأكد من أنها لا تقل عن ثمانية أحرف.

أهم السلوكيات الخاطئة الواجب تجنبها

- استقبال رسائل من جهات مجهولة وتحميل المرفقات دون الكشف عليها.
- التساهل بوضع الرقم السري واستخدام نفس الرقم لأكثر من نظام.
- الإهمال في تحديث البرامج.
- تحميل البرامج من مواقع عامة وليس من مصادرها الأساسية.
- الاتصال بالشبكات العامة دون الاكتراث بمدى أمنها.
- عدم تغيير الإعدادات للأجهزة والبرامج والإبقاء على الإعدادات الأولية.
- عدم الخروج بالصورة الصحيحة (logout) من الحسابات الخاصة سواء البنكية أو البريدية.
- استخدام الفلاشات في أجهزة عامة وغير آمنة.
- التكاسل عن عمل نسخ احتياطية من الملفات الهامة للمستخدم.
- وضع البيانات الشخصية في حسابات الشبكات الاجتماعية.
- تفعيل خاصية مشاركة الموقع في مختلف الحسابات والبرامج.
- مشاركة الملفات والبيانات الشخصية مع الآخرين.
- غلق نوافذ الملاحظات التي قد تظهر دون قراءتها.
- التكاسل في الإبلاغ عن الأنشطة المشبوهة وعمليات السرقات التي قد تحدث.

كلمة أخيرة

يعد تثبيت مجموعة الأمن الكاملة أمراً إلزاميا وإجباريا في هذه الأيام وذلك إذا كنت تقوم بأي نوع من النشاطات على شبكة الإنترنت، وبالإضافة إلى ذلك، من المهم أن تحدث معلوماتك حول آخر التهديدات وحيل وخدع الهندسة الاجتماعية لأن ذلك يعطيك أفضلية تحتاج إليها لتجنب الوقوع كضحية لهذا النوع من الهجمات (على الإنترنت أو دون ذلك). تذكر أن جميع الأدوات التكنولوجية وآليات الدفاع تعني لا شيء تقريبا إذا كنت لا تعرف كيفية استخدامها ومعرفة ما يمكن للمخترقين الوصول إليه في الوقت الحالي. احرص على خصوصيتك وعدم نشر معلومات شخصية عن نفسك لأن المهاجم قد يستخدمها لانتحال شخصيتك ومهاجمة صديق لك أو قد يستخدم المعلومات ليصيغ الهجوم عليك بشكل مقنع أكثر.

المصادر:

- مقالات الدكتورة/ صفاء زمان - جامعة الكويت
- البوابة العربية للأخبار التقنية

معهد الدراسات المصرفية
INSTITUTE OF BANKING STUDIES

ص.ب: 1080 الصفاة - 13011 الكويت
P.O.Box 1080 Safat 13011 Kuwait
تلفون: 22901100 965+ - فاكس: 22466430 965+
البريد الإلكتروني: cs@kibs.edu.kw - www.kibs.edu.kw

ibs_kuwait IBSKuwait