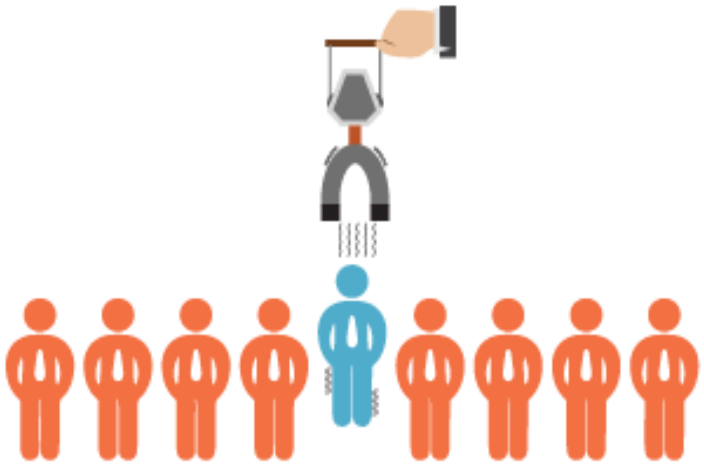


الدليل

للهندسة الإجتماعية

The Guide to Social Engineering

المحتويات:

yahia2mee@yahoo.com

تعريف:

ما هي الهندسة الإجتماعية؟

الهندسة الاجتماعية هي فن الوصول إلى المباني ، الأنظمة أو البيانات عن طريق استغلال علم النفس البشري ، بدلا من استخدام تقنيات القرصنة التقنية. على سبيل المثال ، بدلاً من محاولة البحث عن ثغرة برامج ، مهندس اجتماعي يمكن أن يتصل بالموظف ويعرض نفسه كشخص يدعم تكنولوجيا المعلومات ، ويحاول خداع الموظف في ليكشف كلمة المرور الخاصة به. الهدف هو دائما الحصول على ثقة واحد أو أكثر من موظفيك.

ساعد المخترق الشهير كيفين ميتنيك في تعميم مصطلح "الهندسة الاجتماعية" في التسعينات ، لكن الفكرة البسيطة نفسها (خداع شخص ما للقيام بشيء ما أو الكشف عن المعلومات الحساسة) كانت موجودة منذ عصور كثيرة.

ما الذي يريده المهندسون الإجتماعيون؟

الهدف للكثير من المهندسين الاجتماعيين هو الحصول على المعلومات الشخصية التي يمكن أن تقودهم مباشرة إلى المعلومات المالية أو سرقة الهوية أو إعداد معلومات ل هجوم أكبر على مؤسسة ما. كما أنهم يبحثون عن طرق لتثبيت البرامج الضارة التي تخول لهم الوصول بشكل أفضل إلى البيانات الشخصية أو أنظمة الكمبيوتر أو الحسابات ، المهندسين الاجتماعيين دائمي البحث عن المعلومات التي تؤدي إلى هدفهم. العناصر والمعلومات التي يجدها المحتالون قيّمة تشمل ما يلي:

- كلمات المرور
- المفاتيح السرية
- أي معلومات شخصية (تاريخ الميلاد – عدد الابناء واسمائهم .... الخ)
- أرقام الحسابات
- بطاقات الوصول وشارات الهوية
- قوائم الهاتف
- تفاصيل نظام الكمبيوتر الخاص بك
- اسم شخص لديه امتيازات الوصول

كيف تعمل الهندسة الإجتماعية؟

هناك عدد لا حصر له من مآثر الهندسة الاجتماعية .قد يخدعك المخادع في ترك الباب مفتوحًا أمامه ، أو يزور صفحة ويب مزيفة أو ينزِّل مستندًا برمز خبيث ، أو قد يدرج USB في جهاز الكمبيوتر الخاص بك مما يتيح له الوصول إلى شبكة الشركة الخاصة بك .تتضمن الطرق النموذجية ما يلي:

سرقة كلمات المرور: في هذه الطريقة العامة ، يستخدم الهاكر المعلومات من ملف تعريف الشبكات الاجتماعية لتخمين سؤال تذكير كلمة المرور للضحية .تم استخدام هذه التقنية لاختراق تويتر واقتحام البريد الإلكتروني.

الصداقة : في هذا السيناريو ، يكتسب الهاكر ثقة الفرد أو المجموعة ثم يحصل عليها للنقر على روابط أو مرفقات تحتوي على برامج ضارة تقدم تهديدًا ، مثل القدرة على استغلال نقطة ضعف في نظام الشركة .على سبيل المثال ، إنه قد يجري معك محادثة عبر الإنترنت حول الصيد ثم يرسل صورة لمركب يفكر في شرائه تكون مرفقة ببرنامج ضار لتضغط عليه.

انتحال الهوية / انتحال شخصية الشبكة الاجتماعية: في هذه الحالة ، يقوم المخترق بالتواصل معك أو أصدقائك أو الاتصال بك عبر الإنترنت باستخدام اسم شخص تعرفه .ثم يطلب منك أن تفعل له معروفا ، مثل إرساله جدول بيانات أو إعطائه بيانات من "المكتب". "كل ما تراه على نظام الكمبيوتر يمكن أن يتم الخداع أو التلاعب به من قبل الهاكر ،".

التظاهر من الداخل (من الشركة): في كثير من الحالات ، يطرح المخادع نفسه كعامل في مكتب مساعدة تكنولوجيا المعلومات أو مقاول لاستخراج معلومات من العملاء مثل " كلمة المرور " وما يقرب من ٩٠ ٪ من الأشخاص الذين استفدت منهم بنجاح خلال [تقييمات قابلية التأثر للعملاء] وثقوا بي لأنهم ظنوا أنني عملت لصالح نفس الشركة" ، وكمثال في إحدى الحالات ، تم الاحتيال بالتظاهر كعامل متعاقد ، وتمت مصادقة مجموعة من العمال ونم وإعداد مخطط التصيد الاحتيالي الناجح الذي من خلاله تم الحصول على أوراق اعتماد موظف ، وفي النهاية تم الحصول على دخول إلى البنية التحتية الكاملة للشركة.

yahia2mee@yahoo.com

هجمات الهندسة الاجتماعية واسعة النطاق ، وتكلف المنظمات الآلاف من الدولارات سنويا ، وفقا لبحث من شركة الأمن .Check Point Software Technologies وقد وجد مسحها لـ ٨٥٠ من المتخصصين في تكنولوجيا المعلومات والأمن في الولايات المتحدة وكندا والمملكة المتحدة وألمانيا وأستراليا ونيوزيلندا أن نصفهم تقريباً (٤٨٪) كانوا ضحايا للهندسة الاجتماعية وشهدوا ٢٥ هجومًا أو أكثر في العامين الماضيين تقريباً تكلف هجمات الهندسة الاجتماعية الضحايا ما بين ٢٥،٠٠٠ دولار إلى ١٠٠٠٠٠ دولار أميركي لكل حادث أمني ، حسب التقرير.

وبحسب بيان صادر في الاستطلاع ، فإن "الهجمات المهندسة اجتماعياً تستهدف الناس تقليدياً بمعرفة ضمنية أو الوصول إلى معلومات حساسة" ."يستغل المتسللون اليوم مجموعة متنوعة من التقنيات وتطبيقات الشبكات الاجتماعية لجمع معلومات شخصية ومهنية عن كل فرد من أجل العثور على الحلقة الأضعف في المنظمة."

ومن بين الذين شملهم الاستطلاع ، فإن ٨٦٪ يعترفون بالهندسة الاجتماعية باعتبارها مصدر قلق متنامٍ ، حيث ذكر غالبية المستجيبين (٥١٪) أن المكسب المالي هو الدافع الأساسي للهجمات ، تليها الميزة التنافسية والثأر .كانت أكثر هجمات الهجوم الشائعة للهجمات على الهندسة الاجتماعية هي رسائل البريد الإلكتروني التصيدية ، والتي شكلت ٤٧٪ من الحوادث ، تليها مواقع الشبكات الاجتماعية بنسبة ٣٩٪.

الموظفون الجدد هم الأكثر عرضة للهندسة الاجتماعية ، وفقا للتقرير ، يليهم المقاولون (٤٤ ٪) ، والمساعدين التنفيذيين (٣٨ ٪) ، والموارد البشرية (٣٣ ٪) ، وقادة الأعمال (٣٢ ٪) وموظفي تكنولوجيا المعلومات (٢٣ ٪).

ومع ذلك ، قال ما يقرب من ثلث المنظمات أنها لا تملك برنامجًا للوقاية والتوعية في مجال الهندسة الاجتماعية .من بين الذين شملهم الاستطلاع ، ٣٤٪ ليس لديهم أي تدريب على الموظفين أو سياسات أمنية مطبقة لمنع تقنيات الهندسة الاجتماعية ، على الرغم من أن ١٩٪ لديهم خطط.

القواعد الاساسية:

هناك أربعة قواعد نفسية أساسية يستخدمها المهندسون الاجتماعيون لكسب الثقة والحصول على ما يريدونه.

إن معرفة هذه القواعد الأساسية للهندسة الاجتماعية سوف تمكن الموظفين من التعرف بسهولة أكبر عندما يتم استهدافهم من قبل المخادع (المهندس الاجتماعي).

القاعدة الأولى: نقل الثقة والسيطرة.

إن واحدة من الخطوات الأولى هو العمل على ثقة .على سبيل المثال ، يمكن لشخص ما يحاول الدخول إلى مبنى أمن إنشاء شارة (بطاقة) أو التظاهر بأنه من شركة خدمات .إن المفتاح إلى الدخول بدون رفض هو ببساطة التصرف وكأنك تنتمي إلى هناك وأنك ليس لديك ما تخفيه .نقل الثقة مع وضع الجسم يضع الآخرين في بسهولة تحت السيطرة.

"لا يعمل الأشخاص الذين يديرون الحفلات الموسيقية في كثير من الأحيان على البحث عن الشارات (البطاقات) انهم يبحثون عن الموقف (الحدث) ويمكنهم دائمًا أن يعرفوا من هو أحد المعجبين الذين يحاولون التسلل وإلقاء نظرة على النجم ومن يقوم بهذا الحدث وهم يبدون وكأنهم ينتمون لمن يدير الحفلات الموسيقية ليقع ذلك المعجب تحت سيطرتهم".

طريقة أخرى للحصول على اليد العليا (السيطرة) وهي في عرفهم أن الشخص الذي يسأل الأسئلة يسيطر على المحادثة" ، فعندما يطرح عليك أحدهم سؤالًا ، يضعك على الفور في الدفاع . وتشعر بضغوط لتقديم رد صحيح أو مناسب."

ننصح الموظفين بعدم الارتياح أو السماح للغرباء بالدخول إلى المبنى .يجب أن يكون لدى الزائرين (ومقدمي الخدمات) بيانات اعتماد محددة بدقة – حتى لو كانت وجوهًا مألوفة.

yahia2mee@yahoo.com

القاعدة الثانية: الهدايا والهدايا المجانية

التبادل هو الدافع البشري الآخر الذي يستخدمه المهندسون الاجتماعيون فعندما يُعطى الناس شيئًا ، مثل خدمة أو هدية ، حتى إذا كانوا يكرهون فعلًا الشخص الذي قام بذلك ، فإنهم يشعرون بالحاجة إلى المعاملة بالمثل"

إن التأخير الزمني بين إعطاء الهدية وطلب الحصول على خدمة هو أمر مهم فإذا أعطيت هدية ثم طلبت خدمة على الفور ، فإن الاحتمالات هي أن شخصًا ما قد يعتبرها رشوة وإن إعتبرها رشوة ، فإنه سيتصرف بشكل غير مريح. "بدلاً من ذلك ، قد أعطي شيئًا لموظف البوابة في وقت مبكر من اليوم ثم أعود لاحقًا ، مدعياً النسيان ، مثل أوراق تركتها بعد اجتماع .

الفرص هي ، هذه الطريقة تسمح لك عن طريق المعاملة بالمثل لكيفية معاملتك لهم في وقت سابق وتحصل على الخدمة التي تريدها والمعلومات التي تطلبها.

يجب تقديم المشورة للموظفين ليكونوا متشككين في كل من يحاول تقديم شيء لهم .واعتمادًا على حجم المخاطر ، قد يقضي المجرم المتمرس أسبوعًا في وضع الأساس لتشكيل علاقة متبادلة مع الموظفين والتي قد تؤدي إلى الوصول إلى مناطق حساسة أو آمنة.

القاعدة الثالثة: استخدام الفكاهة

يستمتع الناس عمومًا بأولئك الذين يتمتعون بروح الدعابة .يعرف المهندس الاجتماعي ذلك بشكل جيد ويستخدمه للحصول على معلومات ، أو تجاوز حارس البوابة أو حتى الخروج من المتاعب .

في سيناريو إجرامي ، قد يحاول المهندس الاجتماعي الدردشة مع أحد الموظفين للحصول على معلومات منه .أحد الأمثلة الجيدة على ذلك هو اتصال مساعد تكنولوجيا المعلومات المزيف ، حيث يطلب المتصل كلمة مرور الموظف .من المرجح أن يتم إعطاء المعلومات الحساسة إذا كانت المحادثة ممتعة ، وتضع الموظف في وضع مريح.

القاعدة الرابعة: ذكر السبب دائماً

استلهمت مؤخراً مؤسسة "Brushwood" نتائج دراسة Harvard التي وجدت أن الأشخاص دائماً يتنازلوا إذا استخدمت كلمة "لأن" عند السؤال .نظرت الدراسة إلى مجموعات من الأشخاص الذين

ينتظرون استخدام آلة نسخ في المكتبة وكيف استجابوا عندما اقترب أحدهم وطلب منهم نسخ ورقة ذاكراً سبب استعجاله.

في المجموعة الأولى ، سيقول الشخص: "إسمح لي ، لدي خمس صفحات .هل يمكنني استخدام آلة النسخ لأنني في عجلة من أمري؟ "في تلك المجموعة ، سمح ٩٤٪ للشخص بالتخطي في الطابور .في مجموعة أخرى ، سأل صاحب المكتبة مباشرة: "عفواً ، لدي خمس صفحات .هل يمكنني استخدام آلة النسخ؟ "فقط ٦٠٪ قالوا نعم لهذا الشخص .في مجموعة ثالثة ، كان السؤال ، "عفواً ، لدي خمس صفحات .هل يمكنني استخدام آلة النسخ لأنني بحاجة إلى نسخ؟ "على الرغم من أن السبب كان سخيفًا على ما يبدو ، إلا أن ٩٣٪ ما زالوا يقولون نعم.

تبين ، أن الكلمة السحرية هي ، "لأن" تمامًا كما لو كنت ترى شخصًا يسير حول المكان وكأنه يمتلك المكان ، فمن الآمن أن نفترض أنه ينتمي إلى هناك .وبالمثل ، إذا قال أحدهم "لأن" ، يفترض الناس أن لديهم سببًا مشروعًا."

أن الحصول على تعاون الناس يتطلب مجرد إدراك سبب ، حتى لو كان السبب هراء

من المهم إبطاء النظر والاستماع إلى ما يحدث وما يقال في بيئة العمل .خلال اليوم ، قد يبدو من السهل توجيه شخص ما لكن الوعي ووجود العقل لهما أهمية قصوى لمنع المجرم من الاستفادة منك.

الوقاية:

لا توجد منظمة محصنة ضد تهديد الهندسة الاجتماعية .ففي مسابقة عقدت في مؤتمر DefCon للأمن ، حيث تم الطلب من المتسابقين الحصول على معلومات حول شركات مستهدفة للحصول على معلومات يمكن استخدامها لمنظمات المجتمع المدني وهذا هجوم افتراضي ولكن من بين ١٤٠ مكالمة هاتفية تم إجراؤها للموظفين في الشركات المستهدفة ، تم الحصول على جميع المعلومات التي تم طلبها تقريبًا . خمسة موظفين فقط لم يدلوا بمعلومات وكذلك فتح ٩٠٪ من الموظفين المستهدفين عنوان URL تم إرساله إليهم بواسطة المتسابقين – على الرغم من أنهم لم يعرفوا بالفعل الشخص الذي أرسله وهنا تكشف الأرقام عن نطاق واسع ومشكلة الهندسة الاجتماعية لجميع المنظمات.

مع أخذ ما سبق في الاعتبار ، إليك بعض الطرق لتقليل مخاطر مؤسستك.

توعية الموظفين:

من المتفق عليه على نطاق واسع أن الطريقة الوحيدة الأكثر فعالية لمحاربة المهندسين الاجتماعيين هي وعي الموظفين .إن ثقافة الوعي الأمني ممكنة في أي منظمة طالما أنها هي المعيار الذي يعمل من خلاله كل شخص ، ويتم تعزيز المفاهيم باستمرار .فيما يلي أفكار تساعدك على زيادة وعي الموظفين بمخاطر الهندسة الاجتماعية.

أمان الحياة الشخصية اجعل الموظفين يهتمون بالأمان من خلال تسليحهم بتقنيات لتأمين معلوماتهم الشخصية .حيث يمكن للموظفين الحصول على نصائح حول ما يحتاج إلى أمن معلوماته وكيفية إدارة كلمات المرور الشخصية ، وكيفية تأمين الشبكات اللاسلكية المنزلية ، إلخ.

تقديم الشكر: احتفل بمناسبة عرضية حيث يشكر الأمن الموظفين لقيامهم بالدور الخاص بهم.

استخدم مكتبهم: إذا كان لديك سياسة مكتبية نظيفة ، قم بإجراء فحوصات مكتبية عشوائية بعد ساعات العمل و مكافأة الأشخاص الذين ليس لديهم مادة حساسة عن طريق ترك قطعة صغيرة من الحلوى أو قطعة من العلكة وعلامة "شكرًا لك على إنجاز دورك" أو إدخالها في رسم شهري للحصول على جائزة.

استخدام شاشة الكمبيوتر الخاصة بهم: إذا كان لديك نشرة إخبارية خاصة بالشركة ، قم بتضمين مقالة أمنية في كل طبعة ، وقدم معلومات عن آخر الحوادث ، لا سيما في مجال عملك . أكمل رسالتك الإخبارية برسالة بريد إلكتروني شهرية إلى جميع الموظفين ، مع رسالة قصيرة حول موضوع مناسب وفي الوقت المناسب وقم بتوفير صفحة أمان على إنترانت الموظف تسرد سياسات الأمان ومعلومات الاتصال المهمة والروابط وما إلى ذلك.

ضرورة التدريب: سوف تكون برامج التدريب أكثر فعالية إذا قمت بتضمين تمارين تفاعلية أو مسابقات أو ألعاب أو منح .حاول أن تبقي التدريب قصيرًا ، واختبر الفهم.

تذكر أن موظفيك يمكنهم عمل أو كسر برنامج الأمان الخاص بك ، كما يقول نعم لأحد المهندسين الاجتماعيين ، لذا اجعلهم يشاركون في العملية من خلال التماس التعليقات والاقتراحات.

توقف ، فكر ، تواصل:

طوّر ائتلاف من الحكومة الامريكية والمنظمات غير الربحية حملة تهدف إلى جعل الناس يفكرون قبل أن ينخرطوا في أنشطة محفوفة بالمخاطر على الإنترنت .الرسالة – " توقف ، فكر ، تواصل " من المفترض أن تكون مفهومة وسهلة التنفيذ .

"إنها رسالة بسيطة وقابلة للتطبيق تنطبق على الجميع حيث أننا نصل إلى الإنترنت من خلال مجموعة من الأجهزة ، بما في ذلك أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر الشخصية والهواتف الذكية ووحدات تحكم الألعاب."

في كتابه "الهندسة الاجتماعية: فن القرصنة البشرية" ، يروي Chris Hadnagy ثلاث قصص لا تُنسى عن اختبارات تقييم القابلية التي أجراها من أجل الشركات ، لقياس مستوى تعرضها للخطر و تشير كل قصة إلى ما يمكن للمنظمات أن تتعلمه من هذه النتائج.

حالة الرئيس التنفيذي لشركة Overconfident

الدرس المستفاد ١: لا توجد أية معلومات ، بغض النظر عن طبيعتها الشخصية أو العاطفية ، غير مفيدة لمهندس اجتماعي يسعى إلى إلحاق الضرر.

الدرس المستفاد ٢: غالباً ما يكون الشخص الذي يعتقد أنه أكثر أماناً هو الذي يشكل أكبر نقطة ضعف .يعتقد بعض الخبراء أن المديرين التنفيذيين هم أسهل أهداف الهندسة الاجتماعية.

تم توظيف Hadnagy مرة واحدة كمدقق حسابات SE لمحاولة الوصول إلى خوادم شركة الطباعة التي كانت عملياتها والبائعين تهم المنافسينوقد قال الرئيس التنفيذي لـ Hadnagy أن اختراقه سيكون أقرب إلى المستحيل لأنه "حرس أسراره بحياته."

"كان هو الرجل الذي لن يسقط لهذا" ، يقول Hadnagy " .كان الرئيس التنفيذي يفكر في شخص ما على الأرجح يدعوه ويطلب كلمة المرور الخاصة به ، وكان مستعدًا لمثل هذا النهج."

بعد جمع بعض المعلومات ، وجد Hadnagy مواقع الخوادم وعناوين IP وعناوين البريد الإلكتروني وأرقام الهواتف والعناوين الفعلية وخوادم البريد وأسماء الموظفين والعناوين وأكثر من ذلك بكثير و من خلال الفيس بوك ، كان بإمكانه أيضًا الحصول على تفاصيل شخصية أخرى عن الرئيس التنفيذي ، مثل مطعمه المفضل وفريقه الرياضي. لكن الجائزة الحقيقية جاءت عندما علم Hadnagy أن الرئيس التنفيذي كان متورطًا في جمع التبرعات للسرطان ، بسبب معركة ناجحة مع أحد أفراد العائلة .

مسلحا بتلك المعلومات ، كان على استعداد للضرب و اتصل بالرئيس التنفيذي وتظاهر بأنه يتبع لحملة لجمع التبرعات من جمعية خيرية للسرطان تعاملت مع الرئيس التنفيذي في الماضي .أخبره بأنهم يقدمون جائزة في مقابل التبرعات – وشملت الجوائز تذاكر لعبة قام بها فريقه الرياضي المفضل ، بالإضافة إلى شهادات وهدايا للعديد من المطاعم ، بما في ذلك مطعمه المفضل.

وافق الرئيس التنفيذي ، فقال له Hadnagy اسمح لي بإرسال ملف pdf به مزيد من المعلومات حول حملة الصندوق وحتى يتمكن الرئيس التنفيذي من فتحه سأله أي إصدار من برنامج Adobe Reader الذي كان يعمل به و بعد فترة وجيزة من إرساله ملف PDF ، فتحه الرئيس التنفيذي ، حيث قام Hadnagy بتركيب shell سمحت ل Hadnagy بالوصول إلى جهاز المدير التنفيذي.

عندما ذكر Hadnagy للشركة عن نجاحهم في اختراق حاسوب المدير التنفيذي ، كان المدير التنفيذي غاضباً بشكل مفهوم.

يقول Hadnagy: "لقد شعرت أنه من الظلم استخدامنا شيئًا من هذا القبيل ، لكن هكذا يعمل العالم" المخترق الخبيث لا يفكر مرتين في استخدام تلك المعلومات ضدك".

تأمين الحلقة الأضعف: المستخدم النهائي

بما أن التكنولوجيا قد تغيرت ، فإن العامل الأكثر تأثيرا في الأمن هو: الموظف .وكما يقول وين شوارتو ، مؤسس شركة الوعي الأمني ، "إن الحلقة الأضعف في كل هذه الأشياء هي الشخص الموجود على لوحة المفاتيح". ونتيجة لذلك ، فإن مديري الأمن يواجهون مجموعة من الجهل واللامبالاة والغرور عندما يتعلق الأمر الوعي الفردي.

إن الهندسة الاجتماعية لديها مهندسون ونماذج جديدة ، لكن التقنيات الأساسية تظل هي نفسها في الغالب وهنا بعض النقاط للتأمين:

لا تقدم أبدًا معلومات شخصية – لأي شخص وأخبر أي شخص أو قسمب المؤسسة " أن القسم لن يطلب منك أبداً هذه الأنواع من التفاصيل كما إن الإجراء المناسب عند إطلاق نظام جديد هو إصدار بيانات اعتماد جديدة أنت لا تسأل عن بيانات الاعتماد الموجودة.

كمثال على ذلك: *أذكر أنه تم توظيفنا من قبل شركة خدمات مالية كبيرة للقيام بالتدريب على الوعي الأمني و أردنا إجراء تقييم لمستوى الوعي لديهم ، لذلك قمنا باختبار الهندسة الاجتماعية.*

لم نقم بـ "دعوة شخص ما على الهاتف التقليدي ومحاولة الهندسة الاجتماعية معه." لا بل أخذنا عناوينهم وكتبنا رسالة وأرسلناها عبر البريد العادي إلى حوالي ٣٠ ٪ من الموظفين ، وهو ما يقرب من ١٢٠٠ شخص .قالت الرسالة بشكل أساسي: "مرحبًا ، نحن من أمن معلومات الشركات .السبب في تلقيك لهذه الرسالة هو أننا نعرف أن الهندسة الاجتماعية تحدث في العمل ، وسنقوم بترقية أنظمتنا ". ثم انتقلنا إلى بعض المعلومات التقنية التفصيلية حول كيفية قيامنا بترحيل قاعدة البيانات وهكذا.

وحوت الرسالة كذلك : "نعلم أنك قلق بشأن الأمان ، وهذا هو السبب في هذه الرسالة .لا نريدك أن تنقل أيًا من المعلومات على أي شيء باستثناء البريد ، لأن هذه هي الطريقة الوحيدة الآمنة للقيام بالنقل و نحتاج إلى بياناتك الشخصية حول بعض الأمور حتى نتمكن من نقلها إلى النظام والتحقق منها للتأكد من دقتها نظرًا لأننا واجهنا مشكلة مع قواعد البيانات في النقل.

كما أخبرنا المستلمين: "يُرجى عدم إرسال هذه المعلومات عبر البريد الإلكتروني أو الفاكس فقط استخدم المغلف المختوم ، "وارسله إلى عنوان ***لم يكن عنوان الشركة*** *وأخبرناهم أننا فعلنا ذلك لأننا لم نكن نريد من أي شخص في العمل اعتراض ذلك في المكتب .أخبرناهم أيضًا بأننا قد أنشأنا صندوق البريد فقط لإدارة الأمن.*

كانت النتيجة كارثية ، تلقينا استجابة تبلغ ٢٨٪ .كان اختبارًا بسيطًا في الهندسة الاجتماعية ، وسقط أكثر من ربع الأشخاص المستهدفين.

بغض النظر عن عدد الاختبارات والتقييمات والتدابير الأخرى التي تضعها ، فلن تعمل ضد الطبيعة البشرية .يمكننا مضاعفة التدريب ، وقياس الزيادة التدريجية في الوعي ، لكنك لن تحقق نجاحًا بنسبة ١٠٠٪ أبدًا.

متى ما طلبت أوراق اعتماد ، فأغلب من يطلبونها ليسوا جديرين بالثقة

والشعب السوداني (ما شاء الله) يقوم بتصوير الرقم الوطني والجواز والبطاقة الشخصية متى ما طلب ذلك وفي أي وقت بدون أي قلق... وقد شهدت ذلك عند بائع الرصيد والشرائح.. يااااا أخي ان كانت الشرائح لا تباع الا بالاوراق الثبوتية

yahia2mee@yahoo.com

فلم لا تذهب الى الشركة لماذا تعطي كل اوراقك لشخص لا تعرفه ومن قال لك أنه لن يستخدم هذه المعلومات ضدك..
***كمثال** من قال لك أنه لن يقوم بتسجيل شرائح اخرى بأوراقك ثم يستخدمها لإجراء المكالمات المشبوهة ويتركك في مقدمة الإتـهام..*

"لا تثق أبدًا في أي شخص يأتي إليك يطلب أوراق اعتمادك."

المهندسون الاجتماعيون في العمل:

على الشبكات الاجتماعية

مواقع الشبكات الاجتماعية ، ومكاتب الشركات وأي مكان على شبكة الإنترنت كلها أماكن شائعة للمحتالين من أجل التجارة ، بقصد سرقة الهويات ، واختطاف الحسابات ، وتسلل أنظمة الشركات وجني الأموال .فيما يلي بعض أساليب الهندسة الاجتماعية الأكثر انتشارًا ، والتي تستهدف مستخدمي الشبكات الاجتماعية ، وموظفي المكاتب .

أنا سافرت أى اي مكان وفقدت محفظتي .هل يمكن أن أحصل على بعض المال؟ ***شهامة السوداني تكسب.***

كيف يتم ذلك: يقوم المخادع بصفته "صديقًا" على Facebook أو موقعًا آخر للتواصل الاجتماعي ، يرسل رسالة تدعي أنه عالق في مدينة أجنبية أومحلية بدون مال (بسبب سرقة أو محفظة مفقودة أو مشكلة أخرى) ويطلب من المتلقي تحويل الأموال يجب على المستخدمين أن يكونوا حذرين لأن المجرمين يستطيعون اختراق الحسابات ووضعهم كأصدقاء ، فلا يمكنهم دائمًا أن يكونوا متأكدين بنسبة ١٠٠٪ من هويات الأشخاص الذين يتفاعلون معهم.

"**شخص ما لديه سر عليك !تنزيل هذا التطبيق للعثور على ذلك!**"

كيف يتم ذلك: لدى Facebook آلاف التطبيقات التي يمكن للمستخدمين تنزيلها ، ولكن ليس كلهم آمنون .قد يقوم البعض بتثبيت برامج الإعلانات المتسللة التي تطلق إعلانات منبثقة ، بينما يعرض البعض الآخر المعلومات الشخصية إلى أطراف ثالثة .يجب أن يكون المستخدمون حكيمون بشأن التطبيقات التي يستخدمونها.

كيف يتم اختراق الفيس بوك عن طريق الصحفات المزورة

اولا الصفحات المزورة من اكتر الطرق انتشارا والاسهل استخداما وغالبا ما يقع فيها الكثير ممن ليس لديهم خلفيه عن اختراق الفيس بوك والطريقة تكمن فى الاتى ان تقوم بعمل حساب مزيف

على الفيس بوك باسم يوحى بانهو تابع لموقع الفيس بوك وارسال الصفحة المزورة للضحية وهذة الطريقة تدفع الضحية للثقة للدخول والتسجيل فى الصفحة المزورة ومن ثم تقو بسرقة حسابة.

كيف تعمل الطريقة.. (أنا بريء ممن يستخدمها في غير محلها).. الطريقة بدائية جداً..

اولا قم بالذهاب لموقع الفيس بوك وقم بانشاء حساب جديد وبعد ذلك تقوم بارسال طلبات صداقة لجميع الاشخاص الذى تود اختراقهم وسوف يقوم بقبول الطلب من بعضهم كمثال وبعد ان تتم الموافقة من الضحية على طلب الصداقة قم بتغير اسم الايميل الى اى اسم يوحى بانه ينتمى للفيس بوك مثال (مبلغ الاخطاء – امان حساب – تاكيد حسابك .....الخ) وبعد تغيير الاسم تقوم بتغير الصورة الشخصية لصور الفيس بوك وبعد ذلك تقوم بجلب الصفحة المزورة من اى موقع صفحات مزورة (Z–shadow – Arab spam_الخ) وتقوم بكتابة رسالة مخادعة مثال (قام شخصا ما بالولوج الى حسابك مؤخر سوف نقوم بتعطيل حسابك ان لم تكن انت برجاء مراسلتنا عبر هذة الرابط وتقوم بوضع رابط الصحفة المزورة لكن قبل ذلك تاكد من اختصار الرابط على جوجل شورتن بامكان ان تعدل على محتوى الرسالة كما تحب وبعد ذلك تقوم بارسال الرسالة للشخص وعمل لة بلوك ؟! سوف تسالنى لماذا جعلتنى ارسل لة طلب صداقة ولماذا تخبرنى الان بان اعمل لة بلوك فى الاول تقوم بارسال طلب صداقة حتى لا تذهب رسالتك الى طلبات الرسائل وهى اخر ميزات فيس بوك.

وبهذا لن يشاهد الضحية الرسالة الا عن طريقة الصدفة لان اغلبنا لا ينظر لطلبات الرسائل انتهينا من هذة الان لنعرف لماذا تامرنى بان اقوم بعمل لة بلوك؟ تقوم بعمل حظر اولا حتى لا يمكنة التواصل معك وتجبرة على الدخول الى اللصحفة المزورة ثاينا والاهم أنه لا يدخل على حسابك فيجدة حساب شخص عادى لا يمت للفيس بوك بصلة وتفشل العملية برمتها وهكذا انتهى شرح الطريقة الان **كيفية الحماية** ان الصفحات المزورة تحمل دومين مختلف عن www.facebook.com سوف تجده مشابها للفيس بوك ولكن به تلاعب فى الاحرف او عمل دومين فرعى مثلا www.appfacebook.com حتى لا تلاحظة كل ما عليك هو النظر للدومين اذا وجدتة مختلف اغلق الصفحة على الفور او قوم بالتبلغ عن انها صفحة اسبام والاهم كيف يطلب منك الفيس بوك تسجيل الدخول وانت لم تسجل الخروج من المتصفح بالفعل فاذا طلب منك تسجل الدخول راجع الامور السابقة وتاكد منها.

yahia2mee@yahoo.com

ماذا أفعل عند الوقوع ضحية للهندسة الاجتماعية

عادة يترافق الهجوم بأساليب الهندسة الاجتماعية بهجوم آخر ببرمجيات خبيثة مثلا .لذلك عندما يقع المستخدم ضحية للهندسة الاجتماعية عليه أن يقوم بخطوات تختلف تبعا لنوع الهجوم .

لكن بشكل عام يمكن القيام بالخطوات التالية :

- إعلام الشخص المسؤول عن الأمن الرقمي في المؤسسة أو الزميل المختص بموضوع الأمن الرقمي
- تقييم الضرر والأشخاص المتأثرين
- إزالة آثار الهجوم
- إعلام الجهات (مؤسسات، زملاء، أصدقاء، معارف، أفراد عائلة) والتي من الممكن أن تكون قد تضررت أو تأثرت بسبب وضوع المستخدم ضحية للهجوم.

يترافق الهجوم بأساليب الهندسة الاجتماعية بهجوم بروتكيت أو هجوم بحصان طروادة للتحكم عن بعد Remote Administration Trojan لذلك ننصح القرّاء بقراءة واستيعاب كل شيء عن حصان طروادة للتحكم عن بعد Remote Administration Trojan

لنعطي أمثلة واقعية عن الهندسة الإجتماعية ونتعرض له بشكل يومي وطرق الحماية منه:

المثال الأول: تصلنا رسائل على هواتفنا الذكية بربحنا الكثير من المال وأننا استطعنا الفوز في مسابقة ولا نعلم ماهي ، ويطلب منا الدخول الى رابط وتعبئة معلومات شخصية تخصنا كالاسم الكامل و رقم الهاتف والهوية الوطنية وغيره من المعلومات الشخصية.

طريقة الحماية: حذف الرسالة مباشرة وعدم النظر بها وفتح الرابط لانه قد يكون عبارة عن backdoor يتم تحميله تلقائي أو قد يكون الهدف منه جمع معلومات عنك.

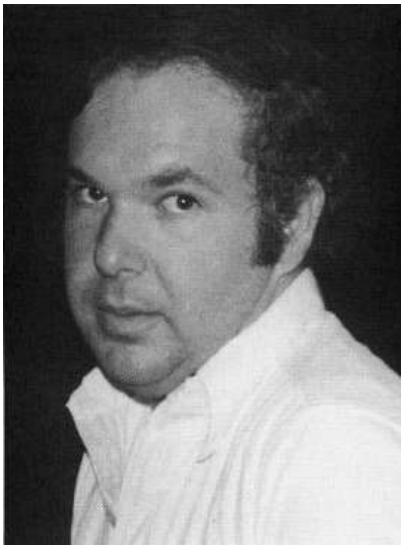
المثال الثاني: بعض المخترقين يستغلون الباحثين عن الوظائف ويقوم بإنشاء منشور يتضمن معلومات عن وظيفة وهمية براتب خيالي ويضع لك في الاخير رقم مزيف او ايميل شخصي وهمي ويخبرك بإرسال معلومات السيرة الذاتية عليه.

yahia2mee@yahoo.com

طريقة الحماية: عدم ارسال معلوماتك الشخصية لأي منشأة *لايحتوي البريد الخاص بها على اسم ونطاق الشركة* إلا في حال كان الإعلان موجود على صفحة الموقع الرئيسية.

قصص حقيقية تبين خطورة الهندسة الاجتماعية:

قصه حقيقه حدثت في عام ١٩٧٨ وتعتبر مثال كلاسيكي عن كيفية استخدام الهندسة الاجتماعية



الشخص الذي في الصورة هو Stanley Mark Rifkin كان يعمل في شركة تقوم بتطوير نظام نسخ احتياطي لبنك ,Security Pacific National Bank في عام ١٩٧٨ كان Rifkin يتجول داخل البنك واثناء تجولة كان يلاحظ طريقة العمل التي يتبعها الموظفين بدقه ويجمع المعلومات. استطاع ان يوصل لغرفه مهمه جدا في البنك والتي يتم فيها جميع التحويلات البنكية تسمى wire transfer room) في الاغلب قديما كانت تتم يدويا عن طريق الهاتف). من خلال ملاحظة ودراسة Rifkin لكيفة عمل البنك والسياسة الداخلية للبنك لاحظ ان الاشخاص المخول لهم بعمل التحويلات البنكية يتم اعطائهم اكواد بشكل يومي ليتم استخدامها اثناء الاتصال وطلب تحويل الاموال كنوع من انواع اثبات الشخصية وان الشخص مخول له بالتحويل. موظفين الـ wire transfer room كانوا يتلقون الاكواد بشكل يومي ويكتبوها على ورقه صغيرة ويلصقها امامه في المكتب لكي لا يتكلف عناء حفظ الكود كل يوم Rifkin .ذهب لغرفة التحويلات وقابل الموظفين لكي يسألهم بعض الاسئلة التي تخص تطوير النظام والتاكد بأن النظام يقوم بالعمل المطلوب اثناء التحدث مع الموظفين قام Rifkin بحفظ الكود وانهى الحديث معهم وشكرهم للتعاون معه وخرج من الغرفة. مباشرة توجة Rifkin الى اقرب

هاتف عمومي وقام بالاتصال بالبنك على انه احد موظفي قسم التحويلات الدولية. المكالمة كانت كالتالي:

Rifkin مرحبا, انا Mike Hansen من قسم التحويلات الدولية

موظفة البنك : ماهو رقم المكتب الخاص بك

Rifkin رقم المكتب الخاص بي هو ٢٨٦

موظفة البنك : اعطني الكود السري

Rifkin الرقم هو ٤٧٨٩ (هذا هو الرقم الذي عرفه اثناء زيارة غرفة التحويلات) ثم بدأ باعطاء التعليمات بتحويل عشرة مليون و مائتين الف دولار لحساب شركة Irving Trust في مدينة New Yorkوحساب البنك في Wozchod Handels bank في سويسرا.

موظفة البنك : الان اعطني ألـinteroffice settlement number

هذا لم يتوقعة Rifkin ولم يعرف ماهو هذا الرقم الذي فلت منه اثناء جمع المعلومات وعمل الدراسة للهجوم. ارتبك قليلا ولكن هذا لم يمنعه ان يواصل الهجوم , استعاد ثقته بسرعة ورد عليها : Rifkin دعيني انظر في هذا , سوف اتصل عليك بعد دقيقة.

قام Rifkin بالاتصال الى احد اقسام البنك مره اخرى وقام بالحصول على الكود المطلوب واعاد الاتصال مره اخرى واكمل عملية التحويل. بعد ايام سافر Rifkin الى سويسرا واخذ المبلغ كاش واشترى الالماس من منظمة روسية وعاد الى الولايات المتحدة.

استطاع Rifkin ان ينفذ اكبر عملية سرقة بدون استخدام سلاح او خبرة تقنية فقط عن طريق جمع المعلومات والهاتف. هذه القصة كلاسيكية ومثال جيد جدا لتوضيح خطورة الهندسة الاجتماعية وعدم وضع سياسة صارمة وتدريب الموظفين .كما ان هناك اخطاء برمجية تسبب في اختراق المنظمات والمؤسسات هناك ايضا اخطاء وثغرات في سياسات الشركات والبروتوكول الاداري والذي يمكن التلاعب به بسهولة عن طريق الموظفين السذج او الغير مدربين لمثل هذا النوع من الهجمات.

yahia2mee@yahoo.com

قصة أخرى:

كان هناك شخص اسمه احمد .. تعرف علي عالم الانترنت ووصل الكثير من الدروس واصبح مهووس بعالم الانترنت ولكن اصبح ينسي بعض الشروحات من كثرة المعلومات التي في رأسه.. فأنشأ مدونة ليضع بها كل ماتعلمه كمخزن لمعلوماته واصبح كل يوم يضع مواضيع بنظام وترتيب وعندما ينسي اي شئ ببساطة يدخل علي مدونته ويأخذ الشرح الكامل.. اصبحت مواضيعه تتأرشف علي جوجل ولاحظ بتغير في زواره حيث اصبح زواره يفوقون ٢٠٠ زائر في اليوم واصبح لديه مثل مكتبة مليئة بالشروحات المختلفة فراسله بعض الناس ينتقدون القالب وايضا ليس لديه دومين فلم يرد ان يخبرهم انها في الاصل ليست مدونة للناس.. فاشتري دومين وايضا اشتري قالب واصبحت مكتبة جميلة مليئة بالشروحات والدروس اصبح يأتيه اكثر من ١٠٠٠ زائر كل يوم فدله بعض الاصدقاء علي عمل نظام الادسنس فوضعه فعلا وقبله جوجل ادسنس واصبحت لديه ارباح ٥ دولار في اليوم ومر اكثر من شهر ازداد الربح الى $١٠في اليوم واصبح كأنه عمل خاص به فشجعه الكثير من الناس ولكن للاسف انتبهوا لنجاحه الحاسدين وحاولوا احباطه ولكن لم يعطيهم اي اعتبار ولكن الخطر القادم هو من يستخدمون تقنيات الهندسة الاجتماعية .. خطط له شخص لاختراق مدونته واختراق حسابه في الادسنس وتاحصول علي المدونة والادسنس فكيف فعل ذلك .. تحدث مع احمد وجري حوار كالاتي:

الشخص الخبيث: سلام عليكم

احمد:وعليكم سلام

الشخص الخبيث: عندك مدونة

احمد:عندي اها

الشخص الخبيث: انا ايضا

احمد: رائع

الشخص الخبيث: اعطني الرابط

احمدhttp://www.example.com:

بعد ٥ دقائق!

الشخص الخبيث: مدونة جميلة جدا (اسلوب الاطراء)

احمد: شكرا لك جدا

الشخص الخبيث: والله انت مدون رائع

احمد: شكرا شكرا علي تقديرك

الشخص الخبيث: اراك غدا

بعد مرور يوم!

الشخص الخبيث:مرحبا

احمد : مرحبا

الشخص الخبيث: كيف حالك اليوم

احمد: الحمد لله

الشخص الخبيث: كم زائر في موقعك اليوم

احمد: كثير ولكن ليس مثل الاول

احمد: خايف بعد اسبوع يختفوا جميع زوار

الشخص الخبيث: عندي لك حل

احمد: كيف

الشخص الخبيث: لدي برنامج لجلب الزوار من اي دولة تريدها

احمد: لالا هؤلاء زوار وهمين

الشخص الخبيث:لقد جربته سوف اريك صورة من زوار مدونتي (صورة مزيفة)

احمد:حسنا ارسل لي برنامج (متحمس لرؤية البرنامج)

قام الشخص الخبيث بدمج برنامج keylogger داخل برنامج الزوار keylogger وهو برنامج لتسجيل اي كلمة تكتبها في المتصفح او اي كلمة مرور واسم مستخدم تضعه ... ارسل الشخص الخبيث الي احمد البرنامج .. احمد جرب البرنامج ولم يحدث شئ .. احمد تحدث مع الشخص الخبيث وقال له برنامجك لا يعمل فأجابه انه لايعمل علي النظام خاص بك.. ماحدث فعلا ان برنامج keylogger الان يعمل في نظام احمد وكل مايكتبه يظهر حتي محادثته علي فيسبوك والشخص الخبيث اغلق

المحادثة .. في اليوم الثاني نهض احمد من نومه مثل كل يوم يريد ان يتفقد مدونته ويريد وضع مواضع جديدة وضع كلمة سر واسم مرور وطبعا كل مايكتبه يظهر للشخص الخبيث.
فماذا فعل الشخص الخبيث .. انتظر احمد الي ان يغلق المدونة ودخل وكتب اسم المستخدم وكلمة المرور و فعلا سرق حساب الادسنس والمدونة وغير كلمة السر .. احمد دخل للمدونة فأستغرب ان للمدونة لاتفتح وهكذا تمت سرقة حساب الادسنس والمدونة بهندسة الاجتماعية.

هذه القصة حقيقة ١٠٠% فقط تم تغير الاسماء..

ملاحظة:

نحن لانشجع علي الاختراق عن طريقة الهندسة الاجتماعية

ولكن فقط لنحمي الناس من هولاء النصابين.

وفي الختام أحب أن اقول إن أصبت فمن الله ،، وإن أخطأت فمن نفسي والشيطان

للحديث بقية

أشكر لكم الاطلاع

ولا اطلب سوى دعوة ثادقة من القلب

لي ولوالدي ووالدتي

لمراسلتي

yahia2mee@yahoo.com

yahia2mee@yahoo.com