مفهوم الهندسة الإجتماعية (أمن المعلومات)

الهندسة الاجتماعية (فن اختراق العقول) :

هي عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفضون بمعلومات سرية , تـُستخدم الهندسة الاجتماعية أحياناً ضمن احتيال الإنترنت لتحقيق الغرض المنشود من الضحية ، حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة بسيطة أو تافهة (عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذي سلطة أو ذات عمل يسمح له بطرح هكذا أسئلة دون إثارة الشبهات).

الأساليب المتبعة في الهندسة الاجتماعية

من أشهر الأساليب المتبعة في مثل هذا النوع من الاختراق :

1. **الهاتف .** فأكثر هجمات الهندسة الاجتماعية تقع عن طريق الهاتف . يتصل المهاجم مدعياً أنه شخص ذو منصب له صلاحيات و يقوم تدريجياً بسحب المعلومات من الضحية.
2. **البحث في المهملات** . حيث يوجد الكثير من المعلومات الهامة عن المنظمة يمكن الحصول عليها من سلة مهملات الشخص أو الضحية.
3. **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.

أشهر المهندسين الاجتماعيين :

من بين المهندسين الإجتماعيين المشهورين أيضاً: فرانك أباغنال (Frank Abagnale) من مواليد 27 أبريل 1948 ، دايفيد بانون (David Bannon) من مواليد 1963 , ستيفن جاي راسل (Steven Jay Russell) من مواليد 14 سبتمبر 1957 ، بن ميلة اكرم (Benmila Akram) من مواليد 06 ديسمبر 1992, خالد الفيومي (Khaled Alfaiomi) من مواليد 11 أبريل 1978 كبار مستشاري امن المعلومات في شركة مايكروسوفت ، وديفيد كينيدي (David Kennedy) من مواليد 15 يونيو 1955 وهو من أنشأ ما يعرف Social-Engineer Toolkit .

الهندسة الاجتماعية - تقنيات وشروط :

وتستند جميع تقنيات الهندسة الاجتماعية على سمات معينة من الإنسان صنع القرار المعروفة باسم التحيزات المعرفية , هذه التحيزات وتسمى أحيانا "الخلل في الأجهزة البشرية" يتم استغلالهم في توليفات مختلفة لخلق تقنيات هجوم ، والمعروف أيضا في المملكة المتحدة و blagging أو bohoing، هو عمل من أعمال إنشاء واستخدام سيناريو اخترع (و ذريعة) لإشراك الضحية المستهدفة على نحو يزيد من فرصة الضحية سوف الكشف عن معلومات أو تنفيذ إجراءات من شأنها أن تكون غير المحتمل في الظروف العادية. محكم كذبة، فإنه غالبا ما ينطوي على بعض البحوث السابقة أو إعداد واستخدام هذه المعلومات لالانتحال (على سبيل المثال، تاريخ الميلاد، رقم الضمان الاجتماعي، مشاركة قيمة الفاتورة) ل إنشاء الشرعية في ذهن من الهدفويمكن استخدام هذه التقنية لخداع رجال الأعمال بغرض كشف معلومات العملاء فضلا عن المحققين خاصة في الحصول على سجلات هاتفية وسجلات المرافق، والسجلات المصرفية وغيرها من المعلومات مباشرة من ممثلي خدمة الشركة. ويمكن بعد ذلك أن تستخدم المعلومات لإنشاء شرعية أكبر حتى في ظل أصعب الأسئلة مع مدير، على سبيل المثال، لإجراء تغييرات حساب، والحصول على أرصدة محددة، الخ. ويمكن أيضا أن تستخدم لبالتستر انتحال زملاء العمل، والشرطة، والبنوك، سلطات الضرائب، ورجال الدين، والمحققين التأمين - أو أي فرد آخر الذي يمكن أن ينظر إليها السلطة أو في ذهن الضحية المستهدفة الحق في المعرفة. يجب أن pretexter إعداد ببساطة أجوبة على الأسئلة التي قد يطلب من الضحية. في بعض الحالات كل ما هو مطلوب هو الصوت الذي يبدو موثوقة، لهجة جادة، والقدرة على التفكير على قدم واحدة. سرقة تحويل سرقة تحويل، والمعروف أيضا باسم "لعبة ركن" أو "جولة في لعبة ركن"، نشأت في الطرف الشرقي من لندن. وباختصار، هو تحويل سرقة "يخدع" التي يمارسها اللصوص المحترفين، عادة ضد شركة النقل أو البريد السريع. والهدف من ذلك هو إقناع الأشخاص المسؤولين عن تسليم المشروعة التي يتم طلب الشحنة في مكان آخر - ومن هنا، "على مرمى حجر". مع حمولة / شحنة إعادة توجيه، واللصوص إقناع السائق لتفريغ الشحنة بالقرب من، أو بعيدا عن وعنوان المرسل إليه، في التظاهر بأنها "الخروج مباشرة" أو "مطلوب على وجه السرعة إلى مكان آخر". و"يخدع" أو الخداع جوانب عديدة ومختلفة، والتي تشمل تقنيات الهندسة الاجتماعية المشروعة لإقناع الموظفين الإداريين أو المرور من شركة النقل أو البريد السريع إلى إصدار تعليمات للسائق لإعادة توجيه أو تحميل شحنة. اختلاف آخر من السرقة والتسريب تمركز سيارة الأمن خارج مصرف في ليلة الجمعة. حراس يرتدون ملابس أنيقة استخدام خط "آمنة ليلة خارج الترتيب، سيدي". باستخدام هذا الأسلوب، يتم gulled أصحاب المتاجر وغيرها في الاستيلاء على إيداع في الشاحنة. انهم بالطبع الحصول على إيصال، ولكن في وقت لاحق هذا تبين أن لا قيمة لها. تم استخدام تقنية

مماثلة قبل سنوات عديدة لسرقة ستاينواي بيانو ضخم من استديو إذاعي في لندن. "تعال جوف (يارجل) لإصلاح البيانو"، وكان خط الدردشة.
الخداع المقال الرئيسي: الخداع التصيد هو أسلوب الاحتيال للحصول على معلومات خاصة. عادة، ومخادع يرسل البريد الإلكتروني التي يبدو أن تأتي من الشركة، طلب بطاقة الأعمال المشروعة أحد البنوك، أو الائتمان "التحقق" من المعلومات والتحذير من بعض نتيجة وخيمة إذا لم يتم توفير ذلك. البريد الإلكتروني عادة ما تحتوي على وصلة لصفحة الويب الاحتيالية التي يبدو المشروعة، مع شعارات الشركة والمحتوى، ولها شكل طلب كل شيء من عنوان الصفحة الرئيسية ل بطاقة ATM ل PIN. على سبيل المثال، شهد عام 2003 انتشار عملية احتيال التصيد في أي من المستخدمين تلقت رسائل البريد الإلكتروني من المفترض من موقع ئي باي مدعيا أن حساب المستخدم على وشك أن يتم تعليق إلا إذا الرابط المقدم قد تم اختيار لتحديث بطاقة الائتمان (المعلومات التي يباي حقيقية بالفعل). لأنها بسيطة نسبيا لجعل موقع على شبكة الإنترنت تشبه موقع منظمة المشروعة من خلال محاكاة رمز HTML، يتم خداع واحتيال تحسب على الناس في التفكير ويجري الاتصال بهم من قبل موقع ئي باي وبعد ذلك، كانوا في طريقهم لموقع ئي باي لتحديث معلومات حساباتهم. بواسطة البريد الإلكتروني غير المرغوب مجموعات كبيرة من الناس، ويجري قراءة "مخادع" يعول على البريد الإلكتروني عن طريق نسبة مئوية من الأشخاص الذين سبق ذكره أرقام بطاقات الائتمان مع eBay مشروعة، الذين قد ترد. IVR أو الخداع الهاتف المقال الرئيسي: Vishing هذه التقنية يستخدم المارقة الاستجابة الصوتية التفاعلية (IVR) لإعادة نظام نسخة المشروعة السبر من أحد البنوك أو مؤسسة أخرى في نظام IVR. يتم مطالبة الضحية (عادة عن طريق البريد الإلكتروني التصيد) لاستدعاء لفي "البنك" من خلال عدد (رقم مثالي مجانا) قدمت من أجل "تحقق" من المعلومات. وهناك نظام نموذجي رفض دخول الإضافية باستمرار، وضمان الضحية يدخل دبابيس أو كلمات المرور عدة مرات، في كثير من الأحيان الكشف عن كلمات المرور مختلفة. نظم أكثر تقدما نقل الضحية إلى المهاجم تظاهر بأنه عامل خدمة العملاء لمزيد من الاستجواب. يمكن للمرء حتى سجل الأوامر نموذجي ("اضغط واحد لتغيير كلمة المرور الخاصة بك، اضغط مرتين إلى التحدث لخدمة العملاء"...) وتشغيل الاتجاه يدويا في الوقت الحقيقي، وإعطاء مظهر كونه IVR من دون حساب. كما دعا التصيد الهاتف vishing. الاصطياد الاصطياد هو مثل حصان طروادة في العالم الحقيقي الذي يستخدم وسائط مادية وتعتمد على الفضول أو جشع الضحية. في هذا الهجوم، المهاجم يترك البرمجيات الخبيثة المصابين الأقراص المرنة، CD ROM، أو محرك أقراص فلاش USB في موقع تأكد من أن العثور على (حمام، مصعد، مواقف الكثير الرصيف،)، يعطيها تسمية المشروعة والفضول يبحث الإزعاج، وينتظر لمجرد ضحية لاستخدام الجهاز. على سبيل المثال، قد مهاجم إنشاء قرص يضم شعار الشركة، متاحة بسهولة من موقع ويب الهدف، والكتابة "ملخص الرواتب التنفيذي 2012 Q2" على الجبهة. أن

يقوم المهاجم بعد ذلك يخرج القرص على أرضية مصعد أو في مكان ما في بهو الشركة المستهدفة. موظف غير عارف قد تجد أنه من وضعه لاحقا القرص في جهاز كمبيوتر لإشباع فضولهم، أو السامري الصالح قد تجد أنه وتحويلها إلى شركة. في كلتا الحالتين نتيجة لإدراج القرص في مجرد جهاز كمبيوتر لمشاهدة محتويات، فإن المستخدم تثبيت تدري البرمجيات الخبيثة على ذلك، من المرجح إعطاء وصول المهاجم غير المقيد إلى PC الضحية وربما، فإن الشركة تستهدف الداخلية شبكة الكمبيوتر. ما لم ضوابط منع العدوى الكمبيوتر، أجهزة الكمبيوتر المدرجة لتعيين "التشغيل التلقائي" قد يؤثر سلبا وسائل الإعلام بمجرد إدراج قرص المارقة. أكثر جاذبية من الذاكرة، ويمكن أيضا أن تستخدم أجهزة معادية. على سبيل المثال، يتم إرسال "الفائز" حرة لاعب السمعية الرقمية التي يقوض في الواقع أي جهاز كمبيوتر موصول بها. شركة أمن تكنولوجيا HBGary باعت هذه الأجهزة لحكومة الولايات المتحدة. تقابل تقابل يعني شيئا لشيء : مهاجم يدعو أرقام عشوائية في شركة تدعي أنها تدعو مرة أخرى من الدعم التقني. في نهاية المطاف سوف تصل إلى شخص مع مشكلة المشروعة، بالامتنان أن شخصا ما يدعو إلى مساعدتهم.
سوف المهاجم "مساعدة" في حل المشكلة ويكون في عملية الأوامر نوع المستخدم التي تعطي وصول المهاجم أو إطلاق البرمجيات الخبيثة. في عام 2003 في المعلومات الأمنية المسح، 90٪ من العاملين في المكتب أعطى الباحثون ما زعموا كان لهم كلمة في الإجابة على سؤال الاستطلاع في مقابل رخيصة القلم الحصول على الدراسات الاستقصائية مشابهة في سنوات لاحقة نتائج مماثلة باستخدام الشوكولاتة وغيرها من السحر رخيصة، على الرغم من أنها قدمت أي محاولة للتحقق من صحة كلمات السر. ذيل المقال الرئيسي: حمل مركبة (الأمن) مهاجم، الذين يحاولون الدخول إلى منطقة محظورة مضمونة غير المراقب، والإلكترونية التحكم في الوصول، على سبيل المثال عن طريق RFID بطاقة، يمشي وراء ببساطة في الشخص الذي لديه حق الوصول المشروعة. بعد مجاملة المشتركة، فإن الشخص عادة المشروعة عقد الباب مفتوحا أمام المهاجم. يجوز للشخص أن تفشل المشروعة لطلب تحديد هوية أي من عدة أسباب، أو أن تقبل وتأكيد علي أن المهاجم قد نسي أو فقدت رمز الهوية المناسبة. قد مهاجم وهمية أيضا عمل عرض رمز الهوية. أنواع أخرى المشترك المحتالون الثقة أو المحتالين يمكن أيضا اعتبارها "المهندسين الاجتماعية" في أوسع معانيها، لأنها تعمد خداع الناس والتلاعب واستغلال نقاط الضعف البشرية للحصول على منافع شخصية. ويجوز لهم، على سبيل المثال، استخدام تقنيات الهندسة الاجتماعية كجزء من الاحتيال IT. وهناك نوع حديث جدا من تقنية الهندسة الاجتماعية تتضمن خداع أو معرفات تكسير أشخاص لديهم شعبية البريد الإلكتروني معرفات مثل ياهو، بريد جوجل، هوتميل، وما بين دوافع كثيرة لخداع و:
التصيد أرقام الحسابات بطاقات الائتمان وكلمات السر الخاصة بهم.
تكسير خاصة رسائل البريد الإلكتروني والدردشة وتاريخها، والتلاعب بها باستخدام تقنيات التحرير المشترك قبل استخدامها لابتزاز الأموال وخلق

عدم الثقة بين الأفراد. تكسير مواقع الشركات أو المنظمات وتدمير سمعتها. الكمبيوتر الخدع فيروس المضادة يجب على المنظمات، على مستوى الأفراد الموظف /، ووضع أطر للثقة. (أي متى / أين / لماذا / كيف يجب أن يتم التعامل معها المعلومات الحساسة؟) يجب على المنظمات تحديد أي معلومات حساسة والسؤال سلامتها في جميع النماذج. (أي الهندسة الاجتماعية، وبناء الأمن، وأمن الحاسوب، الخ.) يجب على المنظمات وضع بروتوكولات الأمن للشعب الذين يتعاملون مع معلومات حساسة. (أي الورق مسارات لكشف المعلومات و/ أو الفتات الطب الشرعي) يجب تدريب العاملين في البروتوكولات الأمنية ذات الصلة لموقفهم. (على سبيل المثال، يجب على الموظفين تحديد الأشخاص الذين توجيه نحو المعلومات الحساسة.) (أيضا: في مثل هذه الحالات كما ذيل، إذا لا يمكن أن هوية الشخص يمكن التحقق، ثم يجب تدريب العاملين في رفض بأدب) يجب أن يتم اختبار إطار المنظمة بشكل دوري، ويجب أن تكون هذه الاختبارات لم يعلن عنها مسبقا. إدراج بعين ناقدة إلى أي من الخطوات أعلاه: لا يوجد حل مثالي لسلامة المعلومات. تقتصر القمامة الأمن باستخدام خدمة إدارة النفايات لديها مع تأمين حاويات عليها، مع مفاتيح لهم فقط على شركة لإدارة النفايات والموظفين التنظيف. أيضا التأكد من القمامة يقع في مكان ليس من الرأي، ومحاولة للوصول إلى أنها سوف تحمل خطرا على القبض أو ينظر أو خلف بوابة الجدار المغلقة أو التي يكون فيها الشخص يجب التعدي قبل أن يتمكنوا من محاولة الوصول القمامة.

طرق الحماية من الهندسة الاجتماعية:

- وضع قوانين للحماية الأمنية للمنظمة: تقوم المنظمة بالتوضيح للعاملين فيها قوانين الحماية الأمنية المتبعة والتي على العاملين تطبيقها.
- **على سبيل المثال**: يقدم الدعم الفني المساعدة ضمن أمور معرفة ومحددة مسبقاً.
- وضع حماية أمنية لمبنى المنظمة: يمنع دخول الأشخاص غير العاملين في المنظمة.
- و تحدد الزيارات في حدود الأعمال بمعرفة سابقة لحراس الأمن في المنظمة وتحت مراقبة منهم.
- **التحكم بالمكالمات الهاتفية**: وذلك بوضع نظام امني للمكالمات مع قدرة على التحكم في من يستطيع مكالمة من.
- منع المكالمات الخاصة وحضر المكالمات الدولية وبعيدة المدى إلا للضرورة وبإذن المسئول عن المكالمات.
- عدم إظهار مدخل للخط الهاتفي للمنظمة لتجنب استخدام الهاتف من قبل شخص خارج المنظمة.
- **التعليم والتدريب**: تثقيف الموظفين داخل المنظمة بمجال أمن المعلومات والاختراقات التي من الممكن حصولها.

- تدريب الموظفين في مركز الدعم الفني وتثقيفهم على مستوى جيد من الناحية الأمنية وتوضيح أساليب المهاجمين وتدريسها لهم.
- تدريبهم على عدم إعطاء معلومات ذات سرية عالية إلا بعد التأكد من هوية الشخص ووفقاً للحد المسموح بيه.
- تدريبهم على كيفية رفض إعطاء المعلومات عند عدم الإمكانية بأسلوب لبق.
- إستراتيجية التصرف في المواقف الحرجة: بأن يكون هناك إستراتيجية محددة تضعها المنظمة تمكن الموظف من التصرف إذا طلب منه معلومات سرية تحت ضغط ما.
- إتلاف المستندات والأجهزة غير المستخدمة: وضع أجهزة لإتلاف الورق داخل المنظمة كي لا يمكن استخدام المعلومات التي تحويها سواء كانت معلومات حساسة أو كلمات سر للدخول للنظام ونحو ذلك.
- إتلاف أجهزة الكمبيوتر القديمة كي لا تستعمل باستخراج معلومات سرية منها.

ابرز مهندسي الاجتماعية

ولاية كاليفورنيا إدارات الشرطة التحقيق في الانتهاكات الضوء الأحمر أكثر من 30 ولاية كاليفورنيا الإلكتروني من إدارات الشرطة وهمية الضوء الأحمر كاميرا "تذاكر"، وتسمى أيضا "تذاكر واش،" في محاولة لأصحاب المسجلين خدعة في الكشف عن هوية الشخص الذي كان يقود السيارة في وقت الانتهاك المزعوم. لأنه لم تكن هذه "التذاكر" قدمت في المحكمة، وأنها تحمل أي وزن قانوني و(في الولايات المتحدة) المالك المسجل لديه الحق في التزام الصمت وليس عليها أي التزام للرد على أي نحو. في ولاية كاليفورنيا، وتذكرة حقيقية تحمل اسم وعنوان الفرع المحلي للمحكمة العليا وتوجيه المتلقي للاتصال تلك المحكمة، في حين أن وهمية "تذكرة" ولدت من قبل الشرطة لن تفعل ذلك. كيفن ميتنيك إصلاح الكمبيوتر مستشار الأمن الجنائي في وقت لاحق وكيفن ميتنيك يشير إلى أنه من الأسهل بكثير لخداع شخص ما في إعطاء كلمة السر لنظام من الجهد لقضاء للقضاء في النظام. بدر اخوان الاخوة رامي، مزهر، وShadde بدير-جميعهم من المكفوفين تمكنت من الولادة إلى إنشاء الهاتف والكمبيوتر واسعة النطاق في مخطط الاحتيال إسرائيل في 1990s باستخدام الهندسة الاجتماعية، التمثيل الصوتي، وأجهزة الكمبيوتر، عرض برايل. رئيس الملائكة و قبعة بيضاء القراصنة، مستشارا أمنيا الكمبيوتر، والكاتب لمجلة Phrack، رئيس الملائكة وقد أظهرت تقنيات الهندسة الاجتماعية للحصول على كل شيء من البيتزا لكلمات المرور لسيارات لتذاكر الطيران. ستيف Stasiukonis مستشار الأمن لتقنيات الشبكة الآمنة. مخترع محرك الأقراص USB الإبهام اختبار USB العصي حيث يستغل الواردة لمعرفة ما إذا الموظفين وتشغيلها من داخل بيئات العمل الخاصة بهم. هذا الهجوم هو الآن واحدة من تقنيات الهندسة

الاجتماعية الأكثر شعبية في وجود ويستخدم لاختبار العنصر البشري من الأمن في جميع أنحاء العالم . مايك Ridpath مستشار الأمن لل IOActive، نشر المؤلف، والمتكلم. تؤكد تقنيات وتكتيكات الهندسة الاجتماعية ل يدعو الباردة. أصبح ملحوظا بعد محادثاته حيث سيلعب المكالمات المسجلة وشرح له عملية التفكير في ما كان يقوم به للحصول على كلمات المرور من خلال الهاتف. أخرى المهندسين الاجتماعية الأخرى تشمل فرانك Abagnale، بانون ديفيد، بيتر فوستر، وستيفن راسل جاي قانون

في القانون العام، بالتستر هو غزو الضرر خصوصية الاعتمادات بالتستر من السجلات الهاتفية في ديسمبر 2006، الولايات المتحدة الأمريكية الكونجرس على مشروع قانون مجلس الشيوخ برعاية جعل من الهاتف بالتستر يسجل الاتحادية جناية مع فرض غرامات تصل إلى 250،000 دولار وعشر سنوات في السجن لأفراد (أو غرامات تصل إلى 500،000 دولار لشركات). شارك في التوقيع عليها رئيس الأمريكي جورج بوش في 12 يناير 2007م التشريعات الاتحادية لعام 1999 "GLBA" هو الفيدرالي في الولايات المتحدة على وجه التحديد أن القانون بالتستر عناوين السجلات المصرفية حيث عمل غير قانوني يعاقب عليها بموجب القوانين الاتحادية. عندما كيان تجاري مثل محقق خاص، SIU محقق التأمين، أو الضابط وتجري أي نوع من الخداع، فإنه يقع تحت سلطة لجنة التجارة الاتحادية (FTC). هذه الوكالة الاتحادية لديه التزام والسلطة لضمان عدم تعرض المستهلكين إلى أي الممارسات التجارية غير العادلة أو خادعة. لجنة التجارة الفيدرالية الأمريكية القانون، المادة 5 من الدول FTCA، في جزء منه: "كلما لجنة يكون سبب للاعتقاد بأن أي شخص من هذا القبيل، شراكة، أو شركة كان أو باستخدام أي أسلوب غير عادلة من المنافسة غير العادلة أو فعل أو خادعة أو الممارسة أو تؤثر في التجارة، وإذا كان يجب أن يظهر للجنة أن دعوى به في هذا الشأن سيكون لمصلحة الجمهور، كان عليها أن تصدر وخدمة على ذلك الشخص أو شراكة أو شركة شكوى تفيد التهم في هذا الصدد. " النظام الأساسي تنص على أن فعندما يحصل أي الشخصية، المعلومات غير العامة من مؤسسة مالية أو المستهلك، والعمل على أن يخضع النظام الأساسي. يتصل علاقة المستهلك مع المؤسسة المالية. على سبيل المثال، باستخدام ادعاءات كاذبة pretexter إما للحصول على عنوان المستهلك من بنك المستهلك، أو للحصول على المستهلك الكشف عن اسم له أو لها البنك، وتكون مغطاة. مبدأ تحديد بالتستر هو أن يحدث فقط عندما يتم الحصول على المعلومات من خلال ادعاءات كاذبة. في حين اكتسب بيع الهاتف الخليوي سجلات هامة اهتمام وسائل الإعلام، والاتصالات السلكية واللاسلكية السجلات هي محور مشروعي القانون المعروض حاليا على مجلس الشيوخ في الولايات المتحدة، يتم شراء العديد من أنواع أخرى من السجلات الخاصة وبيعها في السوق العامة. يتم الإعلان جنبا إلى جنب مع العديد من الإعلانات لسجلات الهاتف الخليوي، والسجلات والمحاضر

السلكية المرتبطة بطاقات الدعوة. كأفراد هواتف الاتصالات عبر بروتوكول الإنترنت لنقل، فمن الأسلم أن نفترض أن سيتم تقديم هذه السجلات للبيع أيضا. حاليا، يعتبر قانونيا لبيع تسجيلات هاتفية، ولكن غير المشروعة للحصول عليها. معلومات مصدر المتخصصين 1 النائب الأمريكي فريد أبتون (R- كالامازو أعرب، ميتشيغان)، رئيس اللجنة الفرعية للطاقة والتجارة في الاتصالات السلكية واللاسلكية والإنترنت، عن قلقه إزاء سهولة الوصول إلى الشخصية سجلات الهاتف المحمول على شبكة الإنترنت خلال E يوم الاربعاء & C جلسة استماع للجنة على سجلات الهاتف "لل بيع: لماذا لا سجلات الهاتف الآمن من بالتستر "؟ إلينوي أصبحت أول دولة رفع دعوى قضائية ضد وسيط السجلات عبر الإنترنت عند ليزا ماديجان المدعي العام دعوى قضائية ضد 1 المتخصصين معلومات مصدر، شركة، في 20 يناير، المتحدثة باسم مكتب ماديجان يقال. الشركة ومقرها فلوريدا تعمل العديد من المواقع على شبكة الإنترنت التي تبيع سجلات الهاتف النقال، وفقا لنسخة من الدعوى. وكلاء عام من ولاية فلوريدا وميسوري سرعان ما تبع الرصاص ماديجان، وتقديم الدعوى في 24 يناير و 30، على التوالي، ضد 1 المتخصصين معلومات مصدر و، في ميسوري الحال، وسيط سجلات أخرى - حلول فيرست داتا شركة، قدمت العديد من مقدمي الخدمات اللاسلكية، بما في ذلك تي موبايل، فيريزون، وقالت سينجيولار في وقت سابق دعاوى قضائية ضد الوسطاء السجلات، مع سينجيولار الفوز أمر زجري ضد حلول فيرست داتا و 1st المتخصصين معلومات مصدر في 13 يناير كانون الثاني. السناتور الأمريكي تشارلز شومر قدم (D-نيويورك) التشريع في فبراير 2006 بهدف الحد من هذه الممارسة. فإن قانون حماية المستهلك الوثائق هاتف لعام 2006 إنشاء جناية الجنائية عقوبات على سرقة وبيع سجلات الهاتف المحمول، والهاتف الثابت، والصوت عبر بروتوكول الإنترنت المشتركين (الصوت عبر بروتوكول الإنترنت). هيوليت باكارد باتريشيا دن ذكرت الرئيسة السابقة للشركة هيوليت باكارد، أن المجلس HP استأجرت الشركة تحقيق خاصة إلى الخوض في الذي كان مسؤولا عن تسرب داخل المجلس. واعترف دان أن الشركة تستخدم ممارسة بالتستر للحصول على المكالمات المسجلة من أعضاء المجلس والصحفيين. رئيس دن اعتذر في وقت لاحق عن هذا العمل، وعرضت على التنحي من المجلس إذا كان المطلوب من قبل أعضاء مجلس الإدارة. [31] على عكس القانون الاتحادي، كاليفورنيا يحظر القانون على وجه التحديد بالتستر من هذا القبيل. أسقطت الاتهامات جناية 4 الناجمة عن دن في الثقافة الشعبية

في فيلم قراصنة، وبطل الرواية تستخدم بالتستر عندما طلب أحد حراس الأمن لمعرفة رقم الهاتف إلى المودم محطة التلفزيون في حين تظاهر بأنه مسؤول تنفيذي الهامة. جيفري ديفر في كتابه في أي مكان والأزرق، والهندسة الاجتماعية للحصول على المعلومات السرية هي واحدة من الأساليب المستخدمة من قبل القاتل، Phate، للحصول على مقربة من

ضحاياه. في فيلم ليف فري أور داي هارد، جوستين لونج وينظر بالتستر أن والده يحتضر من نوبة قلبية لديهم وفي النجوم مساعدة ممثل بداية ما سيصبح سيارة مسروقة. في فيلم أحذية، واحدة من الشخصيات يشكل بأنه متفوق على مستوى منخفض الأمن الحارس من أجل إقناعه بأن خرق أمني هو مجرد إنذار كاذب. في الفيلم قضية توماس كراون، واحدة من الشخصيات يطرح عبر الهاتف بأنه متفوق حارس المتحف من أجل التحرك بعيدا عن الحارس منصبه. في جيمس بوند فيلم الماس للأبد هل، وينظر بوند كسب الدخول إلى المختبر وايت مع نظام آنذاك للدولة من بين الفن قفل بطاقة وصول " ذيل ". انه ينتظر فقط للموظف أن يأتي لفتح الباب، مما نفسه ثم الصاعد في المختبر، مزيفة إدخال بطاقة غير موجود بينما مقفلة الباب له من قبل الموظف. في برنامج تلفزيوني ملفات روكفورد، استخدام حرف جيم روكفورد بالتستر في كثير من الأحيان في عمله التحقيق الخاص. في TV شعبية مشاهدة The Mentalist في، بطل الرواية باتريك جين غالبا ما يستخدم لخداع المجرمين بالتستر على الاعتراف بالجرائم التي ارتكبوها.