الهندسة الاجتماعية الإلكترونية

**تشير** الهندسة الاجتماعية، **في سياق أمن المعلومات، إلى التلاعب النفسي بالأشخاص لدفعهم إلى القيام بأعمال أو الكشف عن معلومات سرية. وتعتبر نوعا من الاحتيال بغرض جمع معلومات أو الغش أو النفاذ إلى نظام، وتختلف عن "الخدع" التقليدية من حيث أنها غالباً ما تكون إحدى الخطوات العديدة في مخطط أكثر تعقيدًا للاحتيال.**

فضلا عن ذلك، يرتبط مصطلح "الهندسة الاجتماعية" باعتباره فعلا للتلاعب النفسي بالبشر، بالعلوم الاجتماعية، ولكن استخدامه محصور بين محترفي الكمبيوتر وأمن المعلومات.

وتستند جميع تقنيات الهندسة الاجتماعية على صفات محددة لصنع القرار لدى الإنسان تدعى الانحيازات المعرفية. ويتم استغلال هذه الانحيازات، التي يطلق عليها أحيانًا "عِلل الأجهزة البشرية"، في مجموعات مختلفة لتطوير تقنيات هجومية، وبعضها مدرج في القائمة أدناه. ويمكن استخدام الهجمات المستخدمة في الهندسة الاجتماعية لسرقة المعلومات السرية للموظفين. ويحدث أكثر أنواع الهندسة الاجتماعية شيوعًا عبر الهاتف. ومن الأمثلة الأخرى لهجمات الهندسة الاجتماعية نذكر المجرمين الذين يتظاهرون بأنهم يعملون في شركات إبادة الحشرات، ورجال المطافئ، والتقنيين حتى لا يلاحظهم أحد عندما يقومون بسرقة أسرار الشركات.

ومن بين الأمثلة على الهندسة الاجتماعية، نشير إلى شخص يدخل إلى مبنى وينشر إعلانًا يبدو وكأنه نشرة رسمية للشركة يفيد أن رقم مكتب المساعدة قد تغير. لذلك، عندما يتصل الموظفون برقم المساعدة، يسألهم الشخص المجيب عن كلمات المرور وهوياتهم وبالتالي يحصل على القدرة على النفاذ إلى معلومات الشركة الخاصة.

وثمة مثال آخر للهندسة الاجتماعية يحدث عندما يقوم قرصان/هاكر بالاتصال بالشخص المستهدف على أحد مواقع التواصل الاجتماعي ويبدأ محادثة مع الهدف. تدريجيا، يكتسب الهاكر ثقة الهدف ثم يستخدم هذه الثقة للنفاذ إلى معلومات حساسة مثل كلمة المرور أو تفاصيل الحساب البنكي.

*المصدر:* [*https://en.wikipedia.org/wiki/Social\_engineering\_(security)*](https://en.wikipedia.org/wiki/Social_engineering_(security))