الهندسة الاجتماعية

هي التقنيات والأساليب التي يستخدمها الهاكرز للتحايل على مستخدمي تكنولوجيا المعلومات وجعلهم يفضون بشكل ارادي لمعلومات سرية تعطيهم الفرصة لاختراق الانظمة الالكترونية.

الأساليب المستخدمة:

- **توجيه أسئلة عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذات سلطة أو نفوذ.**
- **انتحال شخصية مقربة أو معروفة لدى المستخدم.**
- **استغلال السمعة الجيدة لتطبيقات معينة.**

طرق الحماية من الهندسة الاجتماعية:

- **تجنب مشاركة أي معلومات أو بيانات شخصية مع أي جهة كانت، وعلى الرغم من سهولة القيام بهذا الأمر فإن الكثير من المستخدمين يغفلون عن هذه النصيحة.**
- **تحقق دائما من الأشخاص الذين تتحدث إليهم سواء عبر الهاتف أو البريد الإلكتروني أو خدمات التواصل الفوري وغيرها، مثلا لو كان المتصل من شركة رسمية فلا تجد حرجا أن تطلب منه معلوماته الكاملة وأن يقوم بالاتصال من رقم هاتف رسمي يمكن التحقق منه.**
- **لا تفتح مرفقات البريد الإلكتروني من أشخاص غير معروفين، فلغاية الآن يتم استخدام هذه الطريقة على نطاق واسع لنشر البرمجيات الخبيثة والحصول على المعلومات الشخصية، وذلك من خلال انتحال هوية شركات كبرى وإرفاق بعض الملفات في البريد**

- اعمل على تأمين هاتفك الذكي أو حاسوبك المحمول، يمكن أن تعتمد على فلترة البريد المزعج بالاعتماد على أدوات خاصة، كذلك اعتمد على برامج قوية لمكافحة الفيروسات تتضمن أدوات لمكافحة رسائل وصفحات التصيد.

ما يجب فعله عند الوقوع ضحية الهندسة 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.