Chapter 5: Social Engineering

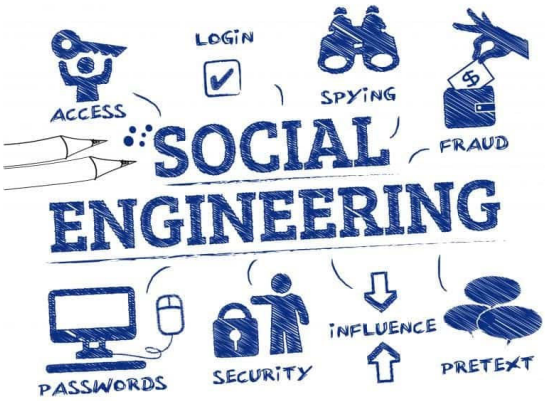
- Introduction
- Why is social engineering important?
- Types of social engineering
- How to protect yourself from social engineering
- Conclusion

62

62

What is social engineering?

- Social engineering is a type of hacking that relies on **human** interaction to gain **access** to information or systems.
- Attackers use social engineering to **trick** victims into giving up their **personal** information, clicking on malicious **links**, or installing **malware**.



ماهي الهندسة الاجتماعية؟

- الهندسةالاجتماعية هي نوع من القرصنة التيتعتمد عليها**بشر**التفاعل لكسب **وصول**للمعلومات أو الأنظمة.
- يستخدمالمهاجمون الهندسة الاجتماعية **حيلة**الضحايا للتخلي عن **شخصي** المعلومات ،والنقر على الخبيثة**الروابط**أو التثبيت**البرمجيات الخبيثة**.

63

63

Why is social engineering important?

- Social engineering is a **growing** threat, and it is often the **first** step in a successful **cyberattack**.
- By understanding social engineering, you can **protect** yourself and your **organization** from attack.

لماذاتعتبر الهندسة الاجتماعية مهمة؟

- الهندسةالاجتماعية هي **أينمو**التهديد ، وغالبأما يكون**أولاً**خطوة ناجحة**هجوم الانترنت**.
- من**خلال** فهم الهندسة الاجتماعية ، يمكنك**ذلك** **يحمي** نفسك ولك **منظمة** من**الهجوم**.

64

Types of social engineering

- Common types of social engineering attacks, including:
  - Phishing
  - Pretexting
  - Baiting
  - Tailgating
  - Impersonation
  - Spear phishing

أنواعالهندسة الاجتماعية

- الأنواعالشائعة لهجمات الهندسة الاجتماعية ،بما في ذلك:
  - التصيد
  - ذريعة
  - اصطياد
  - ذيل
  - التمثيل
  - التصيدبالرمح

65

Phishing Attacks

- Phishing is a type of social engineering where attackers **send emails** or text messages that appear to be from a **legitimate** source, such as a **bank** or credit card company.
- The emails or text messages will often contain a **link** that, when clicked, will take the victim to a **fake** website that looks like the real website.
- Once the victim enters their personal information on the fake website, the attacker can **steal** it.

هجمات التصيد

- التصيد هو نوع من الهندسة الاجتماعية حيث يقوم المهاجمون **إرسال رسائل البريد الإلكتروني** أو الرسائل النصية التي تبدو وكأنها من **شرعي** المصدر ، مثل **أبنك** أو شركة بطاقات الائتمان.
- غالبًا ما تحتوي رسائل البريد الإلكتروني أو الرسائل النصية على ملف **وصلة** هذا ، عند النقر فوقه ، سينقل الضحية إلى ملف **مزيف** موقع الويب الذي يشبه موقع الويب الحقيقي.
- بمجرد قيام الضحية بإدخال معلوماتها الشخصية على موقع الويب المزيف ، يمكن للمهاجم ذلك **يسرق** هو - هي.

66

Pretexting

- Pretexting is a type of social engineering where attackers **pose** as someone else in order to gain the **trust** of their victim.
- Once they have **gained** the victim's trust, they will then ask for personal information, such as a Social Security number or bank account number.

ذريعة

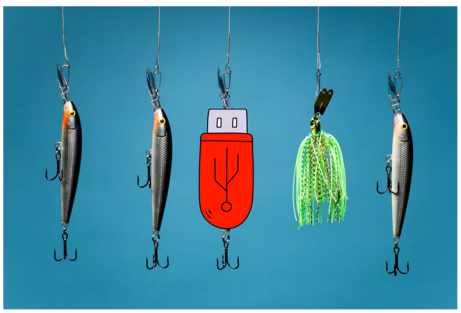
- هونوع من الهندسة الاجتماعية حيث المهاجمون Pretexting **أثار** كشخص آخر من أجل الحصول على **يثق** ضحيتهم.
- بمجرد أن يكون لديهم **المكتسبة** ثقة الضحية ، سيطلبون بعد ذلك معلومات شخصية ، مثل رقم الضمان الاجتماعي أو رقم الحساب المصرفي.

67

67

Baiting

- Baiting attacks involve the social engineer **leaving** a malicious file or device in a public place, such as a **USB** drive or a CD.
- When someone plugs the device into their computer, the **malware** on the device can be installed on the computer.



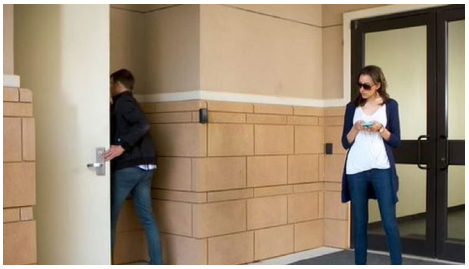
اصطياد

- هجماتالاصطياد تشمل المهندس الاجتماعي **مغادرة**ملف أو جهاز ضار في مكان عام ، مثل ملف **USB**محرك الأقراص أو قرص مضغوط.
- عندمايقوم شخص ما بتوصيل الجهاز بجهاز الكمبيوتر الخاص‌به ، فإن ملف**البرمجيات الخبيثة**على الجهاز يمكن‌تثبيته على الكمبيوتر.

68

Tailgating

- Tailgating attacks involve the social engineer **following** someone through a **secured door** without being authorized to enter.
- Tailgating attacks can be prevented by using **physical** security measures, such as locked doors and security **guards**.



ذيل

- تشمل‌هجمات Tailgating المهندس الاجتماعي**التالي**شخص من خلال أ **باب مؤمن** دون‌أن يؤذن بالدخول.
- يمكن‌منع هجمات Tailgating باستخدام **بدني**التدابير الأمنية ، مثل الأبواب المغلقة والأمن**حراس**.

69

Impersonation

- Impersonation attacks are a type of social engineering attack in which the attacker **pretends** to be someone they are **not**.
- This can be done in **person**, over the **phone**, or **online**.
- Attackers use a **fake** name, title, or affiliation in order to gain the victim's trust in impersonation attacks.

التمثيل

- هجماتانتحال الهوية هي نوع من هجمات الهندسةالاجتماعية التي يستخدمها المهاجم**يتظاهر**ليكونوا شخص ما هم عليه **لا**.
- يمكنالقيام بذلك في**شخص**، على مدار **هاتف**، أو**متصل**.
- يستخدمالمهاجمون أ**مزيف**الاسم أو اللقبأو الانتماء من أجل كسب ثقة الضحيةفي هجمات انتحال الهوية.

70

Spear Phishing Attacks

- Spear phishing attacks are a type of **targeted** social engineering attack in which the attacker sends an email or text message to a **specific** individual or group of individuals.
- The email or text message will often be **tailored** to the victim's interests or concerns in order to increase the **chances** that the victim will click on the link or reveal their personal information.

هجماتالتصيد بالرمح

- تعتبرهجمات التصيد بالرمح نوعاً من **المستهدفة**هجوم الهندسة الاجتماعية الذي يرسلفيه المهاجم بريداً إلكترونياً أو رسالة نصيةإلى**محدد**فرد أو مجموعة من الأفراد.
- غالباًما يكون البريد الإلكتروني أو الرسالة النصية **تناسب**لمصالح الضحية أو مخاوف منأجل زيادة **الفرص**أن الضحية سوف تنقر علىالرابط أو تكشف عن معلوماتها الشخصية.

71

Social Engineering Defense Strategies

- Raising awareness and providing training is the most important thing that individuals and organizations can do to defend against social engineering attacks.
- Strong authentication measures, such as multi-factor authentication, can make it more difficult for attackers to gain access to accounts and systems.
- Individuals and organizations should verify the identities of anyone they interact with, both online and offline.
- Security policies should be regularly updated to reflect the latest threats and vulnerabilities.

72

استراتيجياتالدفاع عن الهندسة الاجتماعية

- يعدنشر الوعي وتوفير التدريب من أهم الأشياء التي يمكن للأفراد والمنظماتالقيام بها للدفاع ضد هجمات الهندسة الاجتماعية.
- يمكنأن تجعل إجراءات المصادقة القوية ، مثل المصادقة متعددة العوامل ، منالصعب على المهاجمين الوصول إلى الحسابات والأنظمة.
- يجبعلى الأفراد والمؤسسات التحقق من هويات أي شخص يتفاعلون معه ، سواءعبر الإنترنت أو في وضع عدم الاتصال.
- يجبتحديث السياسات الأمنية بانتظام لتعكس أحدث التهديدات ونقاطالضعف.

Real-World Case Studies

- The Target data breach, which was caused by a phishing attack, resulted in the loss of over 40 million customer records.
- The Home Depot data breach, which was also caused by a phishing attack, resulted in the loss of over 56 million customer records.
- The Sony Pictures data breach, which was caused by a spear phishing attack, resulted in the loss of confidential data, including employee salaries and Social Security numbers.

73

دراساتحالة في العالم الحقيقي

- أدىخرق البيانات الهدف ، الذي نتج عن هجوم التصيد الاحتيالي ، إلى فقدانأكثر من 40 مليون سجل عميل.
- أدىخرق بيانات Home Depot ، الذي نتج أيضاً عن هجوم تصيد احتيالي ،إلى فقدان أكثر من 56 مليون سجل عميل.
- أدىخرق بيانات Sony Pictures ، الذي نتج عن هجوم تصيد احتيالي ، إلى فقدانالبيانات السرية ، بما في ذلك رواتب الموظفين وأرقام الضمان الاجتماعي.

73

Conclusion

- By raising awareness, providing training, implementing strong authentication measures, verifying identities and information, and regularly updating security policies, individuals and organizations can reduce their risk of being targeted by social engineering attacks.

- من خلال زيادة الوعي ، وتوفير التدريب ، وتنفيذ تدابير المصادقة القوية ، والتحقق من الهويات والمعلومات ، وتحديث سياسات الأمان بانتظام ، يمكن للأفراد والمنظمات تقليل مخاطر تعرضهم لهجمات الهندسة الاجتماعية.

74

74

Resources

';--have i been pwned?

Check if your email or phone is in a data breach

https://youtu.be/lc7scxvKQOo

75

75