<!DOCTYPE html>

<html>

<head>

<title>Cyber</title>

</head>

<body>

</body>

</html>

<h1 style="text-size:150%">Social Engineering</h1>

<img src="programming.gif" alt="Computer Man" style="width:100px;height:100px">

<h2 style="color:darkred; background-color:powderblue;"> Welcome to my website.</h2>

<img src="data:image/jpeg;base64," alt="alternatetext"style="width:500px;height:500;" >

<p1> Social engineering is used to trick authorized users into carrying out actions for unauthorized users. Social engineering is dangerous because it's hard to catch before any damage is done. This website will tell you the steps of social engingeering, what human tendencies are exploited in the process, and how you prevent it. Read more about the the prevalence of social engineering attacks <p1> <a href="https://www.splunk.com/en\_us/blog/learn/social-engineering-attacks.html#:~:text=98%25%20of%20cyberattacks%20rely%20on,access%20to%20sensitive%20business%20information." target="\_blank">here.</a>

<h3>Scroll down to learn everything you need to know about social engineering.</h3>

<h3 style="color:brown; background-color:darksalmon;">Social Engineering Process </h3>

<p style="font-family:brush script mt, cursive; font-size:165%;"> There are three steps in the social engineering process: </p>

<ol>

<li>Research</li>

<li>Development</li>

<li>Exploitation</li>

</ol>

<p> In the research phase, the attacker gathers information about the company or organization they're planning to attack. The more information the attacker can gather in this phase, the more successful they will be. Information can be gathered through physical reconnaissance or through technical sources such as <a href= "https://osintframework.com/" target="\_blank">Open Source Intelligence (OSINT).</a> </p>

<p> Next is the development phase, where the attacker seeks out individual targets and builds a relationship with them. By finding a common interest with the target, the attacker can get closer to them and it won't seem suspicious when they later ask something of them. </P>

<p> Finally, the attacker can use that relationship and exploit human tendencies such as reciprocation, social validation, or intimidation to gain information about the company. Some examples of these exploitations are quid pro quo, pretexting, baiting, and phshing. <a href="https://erau.instructure.com/courses/167175/assignments/3401785" target="\_blank">Click here</a> to learn more about phishing, vishing, and smishing. <p1>

<h3 style="color:darkblue; background-color:yellow; font-family:impact;"> Types of Attacks </h3>

<table>

<tr>

<th>Attack</th>

<th>Description</th>

</tr>

<tr>

<td>Baiting</td>

<td>Lures victim with flase promises that appeals to greed or curiosity</td>

</tr>

<tr>

<td>Tailgating</td>

<td>Unauthorized user follows someone with clearance into a secure area without being noticed</td>

<tr>

<td>Quid Pro Quo</td>

<td>Attacker offers or promises something in exchange for information</td>

<tr>

<td>Pretexting</td>

<td>Using a fabricated story to gain victim's trust and trick them into sharing sensitive information</td>

</tr>

</table>

<p style="background-color:powderblue;"> Understanding the most common type of social engineering attacks is important so you know what to look out for. Check out the videos below to learn more about the different types of attacks. </P>

<iframe width="700" height="500"

src="https://www.youtube.com/embed/Vo1urF6S4u0">

</iframe>

<iframe width="700" height="500"

src="https://www.youtube.com/embed/4SpvulRcVQ0">

</iframe>

<a href="https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks" target="\_blank"> Learn how to prevent falling victim to social engineering attacks here. </a>

<footer>

<p>Author: Gracie Bryner

</footer>