**Section 7 Review and Key Points**

Welcome to the section review.  Below are the key takeaways from this section

* Social engineering is the exploitation of human psychology to get people to reveal sensitive information like passwords and usernames
* The human element is always the weakest link in a security model or system
* Vishing is a form social engineering where the attackers makes a call to the victim pretending to be a reputable person
* Smishing involves the use of text messages sent to a target in order to lure them to click on the links contained in the text
* Social engineering hackers can also pretend to be potential sex partners or job recruiters as a means to scam targets.
* They can also apply for jobs in a target company or connect with an employee in order to gain inside access
* The process of collecting data of potential targets such as emails and phone numbers by hackers is known as reconnaissance or footprinting
* Vigilance and training are the two best ways to fight against social engineering tactics