* **Explain what the following statement means as a best practice in secure coding: “Don’t leave security to the end.”**

The statement means do not wait until the end of the development process to incorporate security. Any defect in coding can introduce glitches, or security breaches. With the number of security related incidents rising, it is paramount to detect vulnerabilities and protect against attacks as early in the development process as possible.

* **Describe the steps you can take to prevent threats.**

In order to understand the steps a developer must take to prevent threats they must first understand common security risks faced by software developers. Things like not maintaining software, poorly written code, vulnerabilities in web services, or insecure data storage can introduce threats to any software. Many software developers skip security preparations which can be associated with various reasons, the most common reason is time, resource constraints, and a lack of knowledge about potential threats. Below are some steps that can prevent threats.

* + - * Don’t Trust the User – End users have power over software and if given too much power some will see if they can break the software.
      * Keep It Secure and Simple (KISS) – An easy software design is much simpler to secure than a complex design.
      * Automation is Your Friend – Automation reduces human error by eliminating the human variable. Software does the same thing every time, making sure all coding standards and guidelines are followed, automation will prevent threats.
      * Threat Model Your Software – This step is essential in preventing threats, if developers can locate areas in code where attackers could compromise the system can prevent attacks.
      * Get Your Cryptography Right – Making sure data is secured correctly by following industry standards and guidelines. Things like don’t store keys in the same place data is stored, don’t hard code keys, don’t use vaults to store keys, don’t create your own algorithms, use algorithms provided by frameworks, and encrypt data at rest and in transit.
* **Provide one example that you can include in your Project Two presentation of how you plan to ensure that security is addressed intrinsically and not left until an issue is discovered—for instance, the use of unit testing.**

In project two I will provide unit testing to ensure security is addressed. I have taken several courses in which I have performed unit testing and including a course on software testing which focused on Junit testing. Using static analysis tools such as ReSharper, CppCheck or Klocwork can find errors or vulnerabilities in code and then using unit testing can ensure the code has the desire outcome.