Matthew Trembley

12/18/2022

Southern New Hampshire University

CS-405

Reflection

I always knew there was some type of industry standard and reasonings for why you would choose certain data types of others, and why compiler warnings exist, but I never knew what was the practicality of them before this course. Security. In the name of protecting customers, their data, and their assets. With technology becoming more advanced, there are essentially new, never before seen threats that may arise and it is important to stay with current security trends to stay afloat. The adoption of a secure coding standard isn’t just for professionals and corporations, it is important for the hobbyist developer as well. Even as a hobby, if one were to create a program, being keen on standards may not just improve security, it may also improve performance to some degree. There is also a huge benefit to mitigate threats before they become overwhelming – which is mainly cost. It is incredibly more expensive to fix a security flaw later as opposed to earlier, tapping on the importance of security not being an afterthought. The risk of not taking security seriously and ignoring any mitigation strategy may not only be detrimental to a product, but also to reputations of companies that may possibly never be able to recover. This is why every developer and company needs to have zero trust in users. Any user can become malicious if pushed, unfortunately – and therefore users need to be kept under the Triple A framework to keep an understanding of their actions, authority, and accessibility to a software product. This can all fit under the belt of a security policy. A security policy within a corporation sends a uniform message to not only the developers, but even the rest of the company who may have any internal workings of the products being created. It says that this company cares about their users and plans on protecting their data, and genuinely want to uphold to industry standards.