Select **one** of the topics below. Then, answer the “what,” “how,” and “why” questions below about your selected topic. Provide a simple code or code snippet example to further illustrate your thoughts.

* Use CSRF (Cross-Site Request Forgery) tokens
* Implement CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

**“What,” “How,” and “Why” Questions**

* **What:** What are you writing about? Give the audience a brief overview of the topic by providing them with foundational information (history, background information, etc.).
* **How:** How is the information relevant? Apply personal knowledge (this can be through research or actual practiced knowledge) to build trust with the audience.
* **Why:** Justify your position and/or course of action. The audience needs proof the information you are presenting is creditable and actionable.

For this discussion, I will be covering Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA). It is safe to assume that you have likely encountered CAPTCHA if you are an internet or application user. CAPTCHA helps verify that a user is a human, not a bot or machine (IBM, 2022). It does this by challenging the user in a way that is complex for a machine to achieve (IBM, 2022). CAPTCHA dates back to the late 1990s and early 2000s to defend against malicious actors and bots (IBM, 2022). Sanctum IT made the first CAPTCHA before it was known under that term (IBM, 2022). There is CAPTCHA, reCAPTCHA v1, Google reCAPTCHA v2, and reCAPTCHA v3.

Understanding the background of CAPTCHA and how it works is very relevant. There is so much spam activity online, and bots are sent to websites to flood them or hack accounts. Having safeguards against these protects developers, users, and other stockholders. CAPTCHA can be implemented and used to "prevent fake registrations, guard against suspicious transactions, protect online poll integrity, stop comment and product review spam, and defend against brute-force and dictionary attacks" (IBM, 2022). Some negatives of CAPTCHA are that bad actors can learn to trick these verification processes, it can be annoying or inconvenient for users, and it is less accessible to users with disabilities (IBM, 2022).

This information comes from the official IBM website, which provides reliable information. Using this information is a great jump start for learning how to incorporate CAPTCHA or other versions into your code to improve security.

Here is a code example of how reCAPTCHA can be implemented (GeeksforGeeks, 2020):

<html>  
<head>  
<title>reCAPTCHA demo: Simple page</title>  
<script src="https://www.google.com/reCAPTCHA/api.js" async defer></script>  
</head>  
<body>  
<form action="?" method="POST">  
<div class="g-reCAPTCHA" data-sitekey="your\_site\_key"></div>  
<br/>  
<input type="submit" value="Submit">  
</form>  
</body>  
</html>

**References**

GeeksforGeeks. (2020, August 11). *What is CAPTCHA code*. GeeksforGeeks. https://www.geeksforgeeks.org/what-is-captcha-code/

IBM. (2022, November 10). *CAPTCHA*. Ibm.com. https://www.ibm.com/think/topics/captcha

**Assignment Requirements and Grading:**

* An initial post of approximately 250 words is due by **Thursday, 11:59 p.m., CST**.
* Submit your post by clicking on the assignment link above, then Create Thread. You must create a thread in order to view your peers' posts. Tip: Create your post in a Word document and then copy and paste your work into the thread.
* A minimum of three (3) responses, to the original threads of other students, of 100-200 words each are due by **Sunday, 11:59 p.m., CST**.
* This discussion board is worth **25 Points**.

To view the rubric grading criteria, click on the following link: [Discussion Board Grading Rubric.](https://content.bellevue.edu/cst/csd/rubricdbv3.pdf)

Hey, Joe! I think you did a thorough job of covering the what, how, and why behind CAPTCHA. As much as I can feel annoyed by CAPTCHA as a user, diving deeper into it this week gave me a newfound appreciation for it. Next time I encounter one, I will feel less annoyed with it. It is a small touch, but I like how you titled your discussion CAPTCHA Crash Course. I like the code snippet you included; I also included the same one in my post. CAPTCHA increases privacy because it limits spam. I definitely foresee this being handy to implement when deploying applications or websites.

Hey, Truman! I think you did an excellent job of explaining the ins and outs of CAPTCHA and how to implement it. I completely agree that it is important to reduce the number of bots allowed on websites. Bots hack into a system, exposing valuable customer and stakeholder information. When a bot is successful and a security breach occurs, it can dishearten the users and lead them to find another application or website instead. As CAPTCHA has become more common, techniques for bots to beat it can be created. That is part of why new versions of CAPTCHA have been released.

Hello there, Samir! I enjoyed reading your post for this week. You did a good job of explaining the what, the how, and the why behind cross-site request forgery. Hackers and bad actors can attack in various ways, so being prepared for what you can to help protect yourself and other users is vital. Even public Wi-Fi can endanger users, so adding extra safeguards is an excellent practice. To add security, I use VPNs to help keep me secure when unsure of the level of protection a site provides. However, this seems even more important when payment information, social security numbers, and addresses are included on an application.