The solution that I presented to fixing a buffer overflow attack is fairly simple. In the code, the input value can only accept 20 characters, given that the array is only 20 large in size. What I did to prevent a buffer overflow is to make the cin function only take in the first 20 characters entered. Thus, it will never be possible for the buffer to overflow since the cin function is not able to accept enough characters to overflow the buffer.

```
Buffer Overflow Example
Enter a value: 12345678910111213141516171819 20
You entered: 1234567891011121314
Account Number = CharlieBrown42

C:\Users\Ayden\source\repos\Module 2 Overflow\x64\Debug\Module 2 Overflow.exe (process 30908) exited with code 0.
Press any key to close this window . . .
```