**3.3 I can set up and use access rights to enable others to access information**

A good policy when setting up accounts that involve the exchange of data is to use anonymous details, or to restrict who can access data to as few individuals as possible. Not doing this increases the risk of your information being used to spam you, or potentially steal your identity.

Being able to *tweet* about where you are and what you’re doing, or share your location, makes it potentially likely that those with nefarious intentions may take advantage.

For websites that I regularly use such as Amazon and Google Maps I take steps to lessen the risk, by using another name online, or logging where I’ve been some time after the event.

So that my work on this course can be checked I have had to create a Github account. In order to share repositories publicly I must grant others access to my files, but I have shared my online name only with those who need it. In addition no more personal information than my name I use on the course, and that of my cat, are anywhere in these files.

