INFORMATION

SECURITY

NAME : SOWNDARIYA G

ROLLNO : 22BCM051

DEPARTMENT: II BSC COMPUTER SCIENCE (A)

SOCIAL MEDIA AWARENESS

Social media platforms are ubiquitous, nowadays, and have connected us in ways, ten years ago, we could never have imagined. We share information and updates instantaneously with the networks of connections we have built, and are subsequently flooded with updates from those same networks. While sharing information in this manner is advantages for many reasons, it brings many risks along with it.

Oversharing information is arguably the biggest risk of using social media, and the ways in which it can be harmful are numerous. Potential burglars are watching for people on vacation hackers are looking for information they can use to break into your accounts, scammers are looking for vulnerable people to swindle, and identity thieves are searching for good targets. There are many other examples, but the root issue is the same - too much information is available to people who shouldn't necessarily have access.

Cyberbullying is another issue that has risen to the forefront due to the increased use of social media. The internet has proven itself to be a forum where people feel very comfortable saying things that they could likely never say in person.

It's important to be cognizant of your actions online, so that you don't contribute to such a problem, or become a victim.

Here are some tips to be more secure while using social media:

Change the privacy of your posts and profiles. it may take a bit of research, but there will be some level of configuration available that allows you to restriction visibility of your posts.

Be careful about what you make visible to your network, but especially what you make public. you shouldn't make the name of your high school, your birthdate, your address, your children's or pet's names, or other personal information public. Many times, this information is used by

Scammers to pretend to be someone you know, or by hackers trying to force password reseti on accounts. And, while it may be obvious, do not post social security numbers, credit card numbers, account numbers or other types of confidential / Financial information.

Turn off location services when you post to social media. you are announcing your location in real-time if you don't disable GPS / location services. Depending on the privacy controls of people you're connected to, people outside your network might be able to see information that you don't want them to.

Read the privacy policy and terms

of service for the social media site. you may be surprised at what the site is allowed to do with your information, pictures and other data. if you decide that giving up some control of your data is worth using the site, that is fine, but you may want to restrict your posts and activities ever further

Remember that you are building a brand with your posts. Social media is perfectly suited to expressing personal opinions, but you should use caution. A good rule of thumb for deciding what to post is to assume that at some point in the future, the post will become public and to choose your words, accordingly

Google yourself, and check out

your social media profiles while logget out. This is a good sanity check to ensure that you've configured the privacy settings the way you want. Also googling your own name can reveal fake accounts that have been opened by imposters.

Don't automatically trust that someone is who they purport to be - verify. Imposter profiles are a huge problem for social media platforms, related to identity theft and online harassment.

Use two-Factor authentication and strong passwords to secure your logins to social media. in particular, two factor authentication will make it much more difficult for hackers to take over your accounts, even if your Password is stolen. most of the larger, well-known sites offer this feature.