Application Security and Privacy

NaNLabs is developing a rework of Central de Ofertas’ start up application for Argentinean, small business owners, which allows them to make group, bulk purchases for a better deal. This will be an Android application, which will provide an interface for the community, linking them through sales and social media. We’re working with NaNLabs to develop a new, safe version of this app including implementing some new features. Our focus is prioritizing security and privacy, without limiting the applications accessibilities.

Keeping a user’s information secret is not only for safety, but important to most people. When using a website or a phone application, a person has rights to expect a certain amount secrecy with their information. Practices such as data collection and sharing of a user’s data, can be helpful in with certain applications, yet can be harmful if used maliciously. (Wilber) It is important, whilst adding new features, to make sure this new technology is safe for users and their data privacy. Mobile technology is a rapidly growing platform, so it has become a target for hackers to try and breach. This is why we must make sure all this application is secure for the users on the platform and network end. (Behani) We need to make sure we write secure code with secure API’s and be careful what we are trusting or giving permissions to. We also need to make sure we have encrypted data, use authorization/anti-tampering techniques and have proper session management. (Behani)

Sensitive data storage is a very important first step in making an app secure. “A 2011 viaForensics study found 83% of popular apps sampled store data insecurely.” (NowSecure) People have to give apps certain amounts of personal information to even use them often. This data includes names, emails, security questions and even Social Security Numbers or credit cards. The users handing over this information are putting trust in the developers, so it is the developers’ responsibility to make sure this data isn’t mishandled. Apps that are transmitting data with little to no encryption or mishandling sensitive information are vulnerable to attack. (NowSecure)

A simple and sure way to avoid data compromise is to simply not store/cache data whenever possible. The way I would handle this would be only keeping data in RAM storage, so it gets cleared when the app is closed. (NowSecure) Limiting the amount of access to sensitive data in the company is also a simple step to keep data private. Only people who need access to this data should have it, and these people should be few and responsible. (Nerdery) Another step towards securing private data is good password protection. I want us to implement a password requirement that needs capitol letter, lowercase letter, a number, a symbol and 8 characters min. (NetID) Although users don’t generally like strict password requirements, it’s for their data’s protection, which we’re not willing to risk. To store passwords, we need to implement hashing the passwords. This is a form of one-way encryption, that will ensure nobody but the user has access to or knows their passwords, and they aren’t directly stored anywhere. (Nerdery) This only affects usability by causing the user to reset their password whenever they forget it, which is a good thing to do regularly anyway and also will be a streamlined process. Finally, any data needs to be encrypted. I would also use the standard crypto library from Android to add a layer of encryption to data that must be stored. (NowSecure) The app will need credit card information and various other sensitive personal information that will need to be stored for a group purchase, because users don’t want to type their card number in every time they make a purchase with it. I believe that should these methods be implemented into our design, it will properly secure all sensitive data to keep the user’s information private.

Social Media sharing is a feature of this is application, which is going to share deals to both help user’s get a better price whilst having them promote the app. Social Media is essentially a platform for sensitive data, so we need to be cautious when we’re are working with it. Social Media platforms have not only been hacked through 3rd party apps that share permissions, which presumably brings big lawsuits, but they have also been known to mishandle information themselves. (Newberry) This means first, we need to look out for and make sure we don’t have any weak point. Also, giving personal information to a platform known for mishandling information, is inadvertently mishandling the information. The only information that needs to be given to the Social Media outlets is the information about the purchases being made, and a link to the app. This will limit the potential room for error or malicious activities.

Data collection can be a useful tool when used correctly, especially as it pertains to marketing. There are two types of data collection research, quantitative and qualitative. Qualitative research pertains to a consumer’s feelings and outlook of a product. When that product is an app, qualitative research allows app designers to improve features such as the user-friendliness of the interface, the usability and also can get direct ideas from the people using the app. This data can be collected in focus groups, interviews or received from comment/complaint submissions. (Juneja) We can collect this qualitative data with a feature that allows users to anonymously report bugs and give any feedback they have. This will allow future improvements to be implemented as the application popularity grows. Quantitative research deals with raw numbers to try and recognize patterns in consumers interests and behaviors. These statistics aren’t subjective, and draw their conclusions directly from whatever data sample is being analyzed. (Juneja) We can use these numbers to figure out what people want and are commonly buying. I think if these numbers are stored anonymously also, with no connection to more specific and sensitive data, then it can be used without compromising any integrity. This information can be obtained using Google Analytics, and be used to give businesses in the area an idea of what could be stocked.

Lastly, as we proceed with this, we need to remember to write secure code. We can’t make mistakes like hardcoding credentials or leaving room for cookie manipulation. To help solve cookie manipulation, we can reassign unique cookies after login, making it harder for a person to assume the identity of another using cookies. (Anand) We can also implement methods of compromising a brute force attack. For example, we need to limit the amount of times a login can be attempted incorrectly, before locking it down and sending an email to the user. Also, we can use text conformation for login attempts on new devices. (Anand) The Google maps widget being used will be a trusted source, we just need to make sure that we are implementing it properly.

I believe if we implement all the above methods, we will have sufficient security for our users’ privacy, without compromising much of the usability. Techniques will be used to store user’s private data securely, and we will guard from compromise from within. We will have connections with social media, but make sure that we do not allow them access to any sensitive data. We can collect data anonymously, and use it for the growth and benefit of our company. We will do all this with securely written code and most importantly, we can do all this safely and securely.