

HY455 Cyber Security
Assignment 1
Chris Papastamos (csd4569)

Question 1

For my target (Κωνσταντίνος Γκούμας 2746) I managed to gather the following information:

| Potential information | Value | Link used to find information |
|---|---|---|
| Name: First | Κωνσταντίνος | |
| Name : Last | Γκούμας | |
| Preferred name | Kostas Goumas | |
| Gender | Male | https://www.facebook.com/kostas.goumas.39 |
| Photo | https://scontent.fath3-4.fna.fbcdn.net/v/t39.30808-6/295832987_10221670307014672_1820409598550859438_n.jpg?nc_cat=100&ccb=1-7&nc_sid=09cbfe&nc_ohc=P-rwpRmp8v4AX_jI2v1&nc_ht=scontent.fath3-4.fna&oh=00_AfCRSNOu9qMYJY2q0wrB7PWVAcWCzCLj_JF_ea_lODsuCvw&oe=640DD62C | https://www.facebook.com/kostas.goumas.39 |
| Education: High school | 2o lykeio iliou{temponera} | https://www.facebook.com/kostas.goumas.39/about_work_and_education |
| Education: Undergraduate studies | Computer science στο CSD - UoC | https://www.facebook.com/kostas.goumas.39/about_work_and_education |
| Languages | English language, Greek | https://www.facebook.com/kostas.goumas.39/about_work_and_education |
| Favorites (music, movies, books, food, color, places, etc.) | Panathinaikos BC, Harry Potter, The Lord of the Rings Trilogy | https://www.facebook.com/kostas.goumas.39/about |

All information is from the target's facebook as that was the only source I could find for my target's information

Question 2

- a. In order for someone to remove his personal information from search machines like google.com you have to contact the website owner that holds the website showing your information (e.g. Facebook, Instagram, LinkedIn, etc). Most of the major websites allow you to remove your information, in most of them the process is fairly easy
- b. According to the Right to be forgotten every person has the right to have his information removed from search engines and other websites.

Question 3

The use of biometric data for user authentication can be very secure and easy to use for the average user.

The biggest argument for biometric data is that it is the most secure way to authenticate a user as it is not as easy to get someones bio data as it is to find their password (probably in an browser's autofill section). Also a big advantage is that a user cannot forget their fingerprint, voice or iris like they could forget their passwords or keys.

Although the upgraded security that bio data can provide it doesn't mean that it is hackproof. We have seen many fingerprint mimicking techniques, 3D printed plastic face replicas and voice recordings to mimic someones else voice.

The services that provide these sort of authentications have also to be careful on how they store their users data because a leak of user's DNA data can be devastating. That is because unlike a password or key, a user cannot change their fingerprint or iris.

Summing it all up, biometric authentication is a very secure way to know if users are who they say they are. But like any other advancement there are many things that can go wrong with this technology, so anyone who is implementing biometric authentication has to be extra cautious.