

Noah Burkhardt, Maya Chudamani, Theodore Gwo, Cole Schneider, Ryan Sutton  
Group 0201-B Biometrics Revised Video Script  
Video: <https://youtu.be/ywxTLV2Jshc>

Narrator: Every time you enter the dining hall, you are risking your identity being stolen. How?  
BIOMETRICS

Theodore: What are Biometrics?!?!??

Narrator: Biometrics are technologies that we can use to determine a person's identity based on physical characteristics, such as fingerprints, iris scans, HAND SWIPES, and facial recognition.

Maya: So where are biometrics used?

Narrator: Biometrics are used in wide variety of places. As a student at the University of Maryland, you probably use biometrics everyday to gain access to the dining halls. In addition to the dining halls, you might have a smartphone or laptop that enables you to use biometrics to securely log in. A recent study showed that over 500 million biometric scanners are projected to be in use by the year 2019, so you are likely to be impacted by biometrics at some point in the future.

Theo: What are the risks to using biometrics?

Narrator: One of the biggest risks to using biometrics is its immutability. If your fingerprints were stolen, you would never be able to change it like a password. Also, biometric security has the risk of being faked. While not a common problem, a determined hacker could replicate your fingerprint and access your phone.

Maya: But if biometrics are so bad, why are they everywhere?

Narrator: They can make tasks more efficient and effective. Airport security time may be cut down drastically in the future thanks to biometrics. The TSA and several airlines have been testing out iris and fingerprint scans to replace lengthy identification processes. Since every person has unique characteristics, the data is harder to replicate. Convenience is essential in our fast-paced world and biometrics are doing their part to help.

Theo: What can I do to stay safe?

Narrator: Rest assured, your data is safe with UMD's Dining Services. When sharing or using biometric information, it's important to handle the information properly. Make sure you know where your biometric information is going and where it is stored. You can usually find this out on an organization's website or by contacting the organization yourself. You should also only use this information with organizations you trust and don't be completely reliant on biometrics as the only method used to identify yourself to organizations you work with.

## Group 0201-B Biometrics Initial Script

Ryan: Every time you enter the dining hall, you are risking your identity being stolen. How?

BIOMETRICS

Theo: What are Biometrics?!?!??

Ryan: Biometrics are technologies that we can use to determine a person's identity based on physical characteristics, such as fingerprints, iris scans, HAND SWIPES, and facial recognition.

Maya: So where are biometrics used?

Ryan: Biometrics are used in wide variety of places. As a student at the University of Maryland you probably use biometrics everyday to gain access to the dining halls on campus. In addition to the dining halls, you might have a smartphone or laptop that enables you to use biometrics in order to securely log in. Besides these uses of biometrics that are most commonly seen by students, the technologies also appear at the airport in TSA checks and other various locations. The use of biometric technologies continues to spread to a wider variety of locations as time goes along.

Theo: So what if I do not have a dining plan and do not have a smartphone that uses biometrics?

Ryan: Just because you are currently not affected by biometrics does not imply that you will not be affected in the future. A recent study showed that over 500 million biometric scanners are projected to be in use by the year 2019, which means you are more likely than not to be impacted by biometrics at some point throughout your life. As biometric security becomes more popular, it becomes more and more important that everyone understands all of the benefits and risks associated with the technologies.

Maya: Are there any risks to using biometrics?

Ryan: There definitely are. One of the biggest risks to using biometrics is its immutability. If your biometric information were somehow compromised, such as your fingerprint information, you would never be able to change it like you could change your password. In addition to this, biometric security has the risk of being faked. While it is not a prevalent problem, a determined hacker could replicate your fingerprint, for example, and gain access to your phone.

Theo: But if biometrics are so bad, why are they everywhere?

Ryan: They can make tasks more efficient and more effective. For example, airport security time may be cut down drastically in the future thanks to biometric technology. The Transportation Security Administration (TSA) and several airline companies have been testing out iris and fingerprint scans as a replacement for the lengthy identification processes that currently can take hours at airports. Since every person has characteristics unique to them, the data is harder to replicate. Convenience is essential in our fast-paced world and biometrics are doing their part to help with that.

Maya: What can I do to stay safe from the risks of Biometrics?

Ryan: When sharing or using biometric information, it's important to handle the information properly. Make sure you know where your biometric information is going and where your biometric information is stored. You can usually find this out on an organization's website or by contacting the organization by phone or email. You should also only use this information with organizations you trust and don't be completely reliant on biometrics as the only method used to identify yourself to organizations you work with.