Exercise Using Quotations and MLA Documentation

Below you have two excerpts from real sources. Your task is to read the articles and write a brief paragraph using at least one quote from each source correctly, and then create a Works Cited page.

Task #1: Use Quotes Correctly ("Sandwich" them)

1. Set up the quote correctly: include the CONTEXT (who said it when from where) and some PREPARATION for what the quote will say, represent, or mean. Use proper MLA in-text citation format.
2. Put a sentence after the quote that clarifies the significance of the quote in terms of making your overall point. CONNECT this evidence to the claim or point.

Task #2: Document These Sources Using MLA Documentation

3. Use in-text citation
4. Create a properly formatted Works Cited page. (Use citation generator to help you.)

Make the topic sentence of the paragraph this statement (use it word for word):

Biometric authentication is the wave of the future.

First article:
Source: American Banker **Date:** June 9, 2017
Title: "The future of authentication is biometrics. No other model competes"
BYLINE (author): Isabelle Moeller **SECTION:** Vol. 182 No. 110

Biometric authentication has become something of a go-to metaphor for bleeding edge, bulletproof security thanks in no small part to the whims of Hollywood. Iris scanners, after all, make for great movies.

Sadly, reality is always different from the big screen. The last five years have lifted biometrics out of "Mission Impossible" and dropped the authentication method into the lives of everyday consumers. From consumers logging into their telephone banking via their voices or signing into their smart phones via their fingerprints, biometrics is fast assuming a central role in digital identity management. But security breaches, while unfortunate, have underlined that biometrics is far from infallible and, most certainly, is not an overnight solution to the world's digital ID problems.

Neither is biometric authentication toothless, however. Biometrics could give real punch to banks' security mix and address an urgent need in authenticating users digitally. Indeed, the recent proliferation of digital services and cloud-based platforms - each requiring independent user verification - is making mincemeat of the username and password model. Ubiquity compels even a diligent person to reuse at least some login credentials, which dramatically increases the security implications of a hack. […] The days of usernames and passwords are numbered.

Two-factor or multifactor authentication solutions are far less penetrable than a single username and password. However, adoption rates remain comparatively low. That is because the multifactor approach fails to deliver a smooth and convenient user experience. Physical authentication tokens, often used in online banking, are easily lost or stolen. But more importantly, the authentication process itself is laborious. […] Replacing all usernames and passwords with this multi-step model is no solution at all; today, we log in to so many different platforms that interruption and end-user frustration would dominate the digital experience.

Enter biometrics. There is little doubt that the future of digital identity lies in using multiple factors to verify a user's authenticity. Banks will also deliver one or more of those factors biometrically to simplify the authentication process for their customers. Apple's Touch ID is an excellent example of how a biometric can make an authentication process fast and convenient as well as secure. Indeed, with biometrics in play, a digital world in which the authentication process disappears entirely from the user's experience could be right around the corner.

URL: http://www.americanbanker.com/opinion/the-future-of-authentication-is-biometrics-no-other-model-competes

Second Article

Source: PaymentsSource
Date: January 25, 2017 Wednesday
TITLE: 'Lazy' passwords must give way to flexible biometrics
BYLINE(AUTHOR): George Avetisov
SECTION: Vol. 1 No. 1

With more than 3 billion credentials reported stolen worldwide in 2016, and 51 companies admitting a breach, we are clearly all in need of a resolution to fix the password problem.

Lazy passwords have failed us, and it's time we work harder to overcome this roadblock along the path to a secure online experience. Attacks on retailers and large service providers likeLinkedInare avoidable. What's needed to get us in shape are solutions that achieve two objectives.

First, service providers must replace the archaic centralized username and password login scheme with decentralized biometric authentication. Enterprises that store sensitive user data, be they secrets like passwords or biometric templates, are targets for hackers who know that a successful breach through phishing or credential stuffing yields a treasure trove of sellable data.

We must abandon the concept that enterprises should centralize the storage of passwords and PII. This shift will disrupt career hackers' business model of hitting one target to obtain a payload as large as and marketable as bulk user data. Going from device to device in the hopes of possibly stealing a person's credentials will send a message to hackers that this practice is neither scalable nor efficient.

Forget what you know about biometrics as they're implemented in the public and legacy commercial spheres, where an entity holds a biometrics database and each time the user authenticates hers or his biometric is matched. The sophistication of today's mobile devices enables encrypted biometrics to be verified against themselves and safely stored on-device. Users after all are the appropriate carriers of their biometrics if, as it should be, privacy is a consideration.

Second, let's break a stubborn rule that says added security reduces usability, and vice versa. Today's mobile devices make possible a fully biometric experience, one that is multimodal so that touch, face, voice, eye, palm, and behavioral recognition offer choice and their combinations, even higher levels of assurance. The ubiquity of online shopping and the rise of mobile-that latter of which conflicts with directives to use 40-character strong passwords-makes clear that we should marry security and usability.

Decentralization and committing to offer the best experience are two 2017 goals that are attainable. 2017 can be the year of breaking old habits like the use of passwords, but only if we as providers, enterprises, and consumers align our willingness to put the worst of yesterday behind us.
URL: http://www.paymentssource.com/opinion/lazy-passwords-must-give-way-to-flexible-biometrics

****

What you will turn in	**Resources to help you do this task:**
Page 1—a paragraph that starts with the line “Biometric authentication is the wave of the future” followed by two quotes from the readings (one from each) that support this claim. Each quote should be properly “sandwiched” and “documented.” Page 2—a Works Cited page properly documenting the two sources you have used	Using Quotes Guide The Sandwich Principle More On Integrating Quotes MLA Guide (in-text and Works Cited) Citation Machine MLA (tool for formatting Works Cited entries)