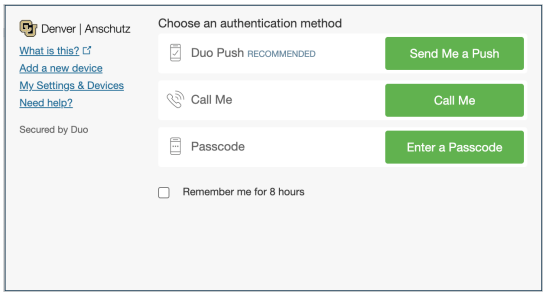
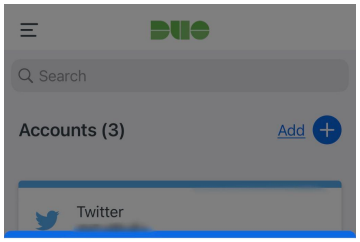
Laurel Schwaebe
LIS 4050-1
10/25/2022
Assignment 1: Tools and Utilities Report

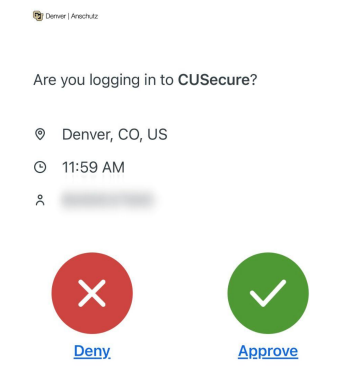
Overview of Multi-Factor Authentication (MFA)

Long gone are the days in which passwords were strong enough to protect user information. Information institutions, like the University of Colorado Denver, utilize multifactor authentication, along with other tools, to help protect user identity from hackers. Multi-factor authentication (MFA) requires two or more steps in authentication during user login, often in the form of time-based text codes, push notifications from apps, or unique time based application codes credential IDs. With two steps to authentication, this would be called two-factor authentication (2FA), but MFA can have any number of steps, within reason. In theory, the more steps, the more secure, but users will only be willing to accept so many steps to protect their own security.



How MFA Works





After logging in with their username and password, users will be directed to the secondary authentication page. This page may take form in a request page to send a code to a text message or app, a plugin page for a code sent to text or app without a command, or another form of secondary authentication. The University of Colorado Denver uses Duo as an additional layer of authentication in part of their login process. Duo sends users to a page that offers users a number of options for secondary authentication. Duo recommends users install its app, Duo Mobile, which allows Duo to send push authentication notifications for quick approval. Users can also approve logins through calls, which allow users to touch any key after accepting the call to approve the login, or to use the passcode option, which sends a text to either the phone number on file or to the Duo Mobile application. The idea behind this process is that the user needs to confirm their identity by taking ownership of a secondary deceive, namely a mobile phone, to prove that they are indeed the owner of the account they are attempting to log in to. Additionally authentication methods may include biometric authentication, which would prove ownership of the body associated with the account.

Duo's MFA

As mentioned above, Duo has a number of authentication methods that it uses for its MFA.

- Duo Push - part of the Duo Mobile application that can send push notifications for authorization on login
- Webauthn - a biometric authenticator that connects to built-in authenticators like TouchID on iOs
- Time-Based One-Time Passcodes - time-based one-time passcodes (TOTP) need to be manually entered within a set time frame in order to be valid; these are often seen as text codes sent to phones or applications
    - Bypass Codes - provides temporary access for contractors or vendors, or for individuals who do not have access their laptop or phone but still need to access

Where Duo Works

As the name suggests, Duo Mobile works on mobile devices. Duo's website notes that the app works for iOs and Android, as well as wearables like Apple Watch. The passcode option associated with Duo Mobile works with mobile devices, which means that it will work with any working phone number that can receive texts. Duo does not appear to be supported on other devices.

Problems

Naturally, the biggest concern with mutifactor-authentication relying on Duo is that not all students have mobile phones. The University of Colorado's Office of Information Technology FAQs offer no solutions for students who do not own mobile devices. While this is an increasingly rare proble, it is not one that has been completely eliminated. Presumably, texts can be sent to WhatsApp, which can then opened on a computer browser, so this may be somewhat bypassed, but it is nonetheless a frustrating issue.

Furthermore, the security offered in mutlifactor authentication is only strong as the individual factors. Even a fairly technologically unsaavy person can gain access to a person's texts, applications may be insecure, phone calls may be misdirected, or any number of other ways to gain access to Duo's notifications. Even layering these factors might not provide nearly as much protection as users might think.

Resources

Cisco. *Two-factor authentication & data protection*. Duo Security. Retrieved October 25, 2022, from https://duo.com/

Office of Information Technology. *Frequently Asked Questions*. University of Colorado Denver | Anschutz Medical Campus. Retrieved October 24, 2022, from https://www.ucdenver.edu/offices/office-of-information-technology/software/how-do-i-use/cu-secure-and-multi-factor-authentication/frequently-asked-questions

Office of Information Technology. *CU Secure and Multi-Factor Authentication (MFA)*. University of Colorado Denver | Anschutz Medical Campus. Retrieved October 24, 2022, from https://www.ucdenver.edu/offices/office-of-information-technology/software/how-do-i-use/cu-secure-and-multi-factor-authentication/