LEWIS & CLARK
COMMUNITY COLLEGE
—— DISCOVER ——

Guide to Duo Two-Factor Authentication

Why do we need two-factor authentication?

- Cybercrime is on the rise.
- Passwords can be stolen, hacked, or guessed.
- Alerts you when someone attempts to sign-in with your current password.

What are some different forms of two-factor authentication?

- **Duo Mobile App** or **Hardware Token**/security key
- Phone call or text message
- Biometrics (Touch ID or Face ID)
- Temporary bypass code
- iCloud Keychain

How does Duo work?

When you sign-in to a Duo protected system, you will type in your username and password, but after successfully authenticating you will receive a second prompt for authentication from Duo. The Duo prompt will guide you to act using your preferred method (Mobile App, Hardware Token, Call, or Text) to verify that this is your account.

Who do I contact if I have issues?

You can call the helpdesk during normal working hours for immediate assistance. You can also contact cybersecurity directly at cybersecurity@lc.edu for inquiries and questions.

Why am I not receiving a Duo Prompt?

There are many reasons you may not be receiving a Duo prompt on your device, so here are some questions to ask while troubleshooting your issue:

- If you open the Duo Mobile App, does the prompt now show up when authenticating?
- Does the device have a stable internet connection?
- Have you tried another connection type, like Wi-Fi vs. mobile data?
- Have you tried to restart the device(s) sending & receiving the prompt?
- Have you attempted to login too many times, and Duo states that you are locked out?

! I received an unexpected or suspicious Duo Prompt, what are my next steps?

If you receive an unexpected or suspicious Duo Prompt, click deny in Duo to mark the notification. Denying a Duo prompt will send a notification to IT for us to investigate. In the meantime, we recommend you change your password at selfservice.lc.edu.

⬤ How much does Duo 2FA help prevent unauthorized Logins to my account?

Below is a graph based on data from a Google Security Blog in 2019 about how effectively 2FA prevents email compromises via phishing attacks. 2FA like Duo Mobile will help prevent unauthorized logins to help protect your account and your personal information. Phishing is the most common tactic hackers use to attempt to gain access to emails.

Email Compromise Prevention Rate Using Different Security Measures

Source: Google Security Blog
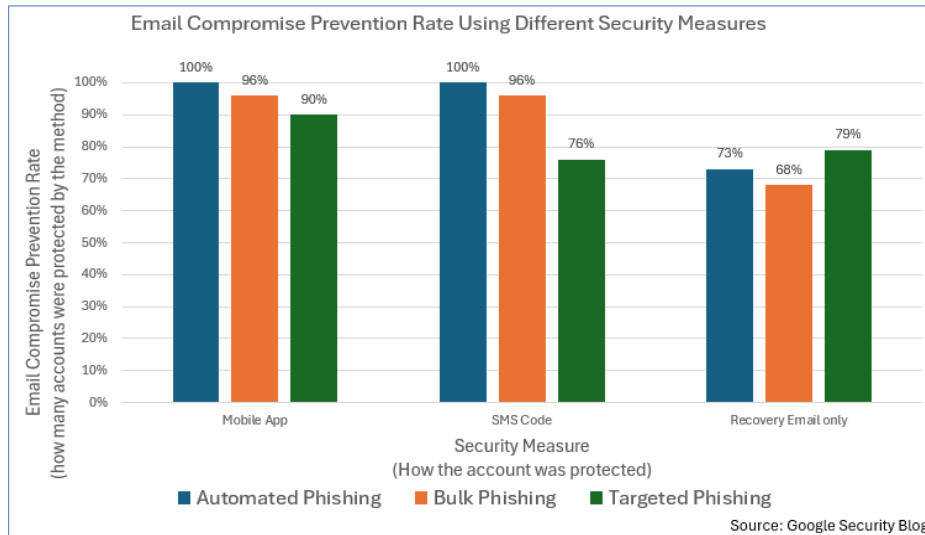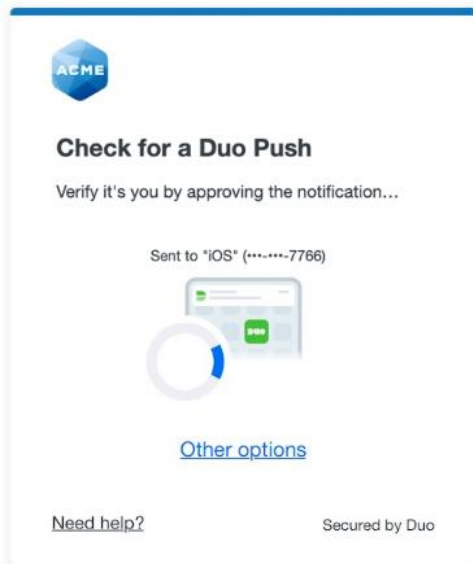
👥 I do not have a smartphone or any cell phone, how will I authenticate using Duo?

If you do not have a cell phone that uses mobile data, please contact us directly at cybersecurity@lc.edu to discuss alternative methods to authenticate with Duo 2FA

📄 What does Duo and the Duo Prompt look like?

Below are a couple examples of how the Duo prompt will look when you login. The ACME logo is a placeholder and is where you will see the Lewis & Clark logo when signing-in to our systems.

The Duo Universal Prompt

The Duo traditional Prompt

Source: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html