About Multifactor Authentication

Multifactor authentication (MFA) is an overly technical sounding term for a very simple solution. Think of MFA as a brand-new deadbolt lock for your account. The most common layer of security we are all familiar with is a password. But what happens when someone steals your password? Anyone can have access to your accounts!

Because MFA requires something only you have, if your password gets stolen, it will be much more difficult for someone to access your accounts and subsequently compromise university data.

You Are a Target Too!

As cybersecurity tools become more sophisticated, it is becoming more practical for hackers to target users, not computers. With today's detection technology, one mistake can sound the alarm to security professionals. Because of that, many would-be hackers are choosing to target the people who use computers. If a hacker can discover an authorized user's account credentials, they're far less likely to sound the alarms that will get them caught. MFA is an efficient and effective way for the University of South Carolina to help reduce the risk of account takeover.

Getting Started with Duo Security

First time users should:

1. Install the Duo Mobile app on your smartphone

2. Log in to myaccount.sc.edu and select Update Account Settings. Log in using your Network Username and password, answer your security question, and then select the Multifactor tab

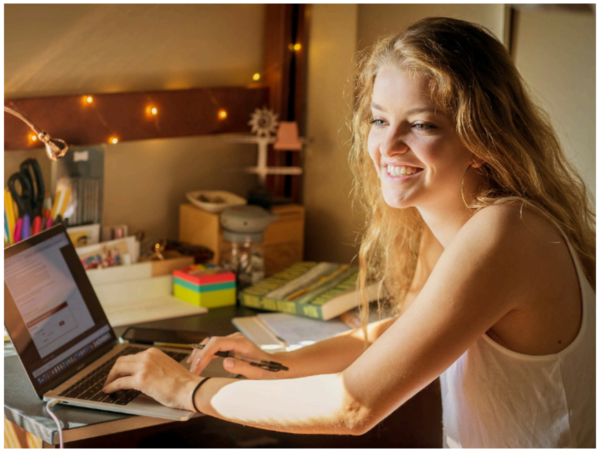
3. Enter your mobile phone number, select mobile, choose your platform, then press submit

4. Select Activate beside your mobile phone number. A QR code will be displayed. (You will scan this code in a later step.)

5. Open the Duo Mobile app on your smartphone

6. On the app, press + at the top of the screen

7. Scan the QR code displayed on your computer



DIVISION OF INFORMATION TECHNOLOGY

DUO SECURITY

A guide to configuring, managing, and using Duo Security

UofSC South Carolina

Authenticating with Duo "Push"

Duo "Push" is the recommended way to authenticate using Duo Security. Once your device has been configured to work with Duo, the Duo "Push" technique is mostly hand's off. When you attempt to access a service that is protected by Duo Security, you will enter your Network Username and password. Within seconds, you will receive a notification on your mobile phone that someone is attempting to access your account. Simply approve the log in from your phone to verify your identity.

Enter your Network Username and password

Use your phone to verify your identity

Securely logged in

Authenticating with a Voice Call

While using the Duo Security Mobile App in conjunction with "Duo Push" is the recommended authentication method, it is also possible to authenticate using a voice call. When prompted to enter the phone number, provide the phone number for the device you wish to receive Duo calls. It may be a mobile phone, or your office landline.

When you are ready to test your configuration, select "Test Authentication," then enter your Network Username and password. Choose your desired device from the dropdown menu, then select the bubble beside "Phone call." Within moments, you should receive a voice call from Duo. Simply press 1 on the telephone keypad to verify your identity.

Authenticating with an SMS Text Message

Duo Security also allows users to authenticate via text message. If your mobile device has not been previously configured to work with Duo, you will need to complete the steps from the "Getting Started" column.

When you are ready to test your configuration, select "Test Authentication," then enter your Network Username and password. On the next page, select the appropriate device from the dropdown menu, select the bubble for "Passcode," then click "Send SMS passcodes." That link will change to text and read "Next SMS passcode starts with 1." You should have received an SMS message to your phone. Locate the passcode in the message that begins with 1 (or the appropriate number). Enter that passcode in the Duo passcode field and your authentication is complete.

Hardware Tokens and Key Fobs

Duo Security supports hardware tokens and key fobs .The implementation of this technology will require a procurement and incur additional cost to the department.

While more costly than other authentication methods, hardware tokens and key fobs can be a trustworthy way for users to present their second authentication factor. These devices may be useful for those who travel internationally or work remotely. To learn more about hardware tokens, including information on supported devices, place a service ticket with the DoIT Service Desk by calling (803)-777-1800.

What if I Forget My Phone?

Sooner or later, most of us will forget our mobile phone. Don't worry, Duo Security provides ways for you to access the accounts you need, even without your mobile phone.

You can also visit the Duo self-service portal at https://my.sc.edu/multifactor. From this portal, you can generate a one-time passcode that will allow access the appropriate system. If your device was lost or stolen, this portal will also allow you to delete the device from your Duo account, insuring no one can use it to access accounts in your name.