My.cu.edu security strengthened with authentication tool [1]

You need your password and a phone to access and update sensitive personal information in my.cu.edu.

The University of Colorado has implemented multifactor authentication to improve protection of personal employee information available in the portal [2]. It now takes two items—your password and your phone—to access sensitive information. This decreases the likelihood that others can access your data, even if they have your password.

How it works

Please watch this one-minute video to see how multifactor authentication works:

p;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;a

(Music: Can't Stop (Anotha C-Doc Instrumental) (Deadly Combo [3]) / CC BY-NC-ND 4.0 [4])

No time for a video? Here are the basics.

1. Log in to the portal [2], using your password.
2. When you try to access or update a protected page in the **CU Resources** area, you will be asked to authenticate your identity. You will have two options: Receive a phone call or receive a text with a passcode.
3. If you select "phone call," choose one of your phone numbers listed in the drop-down menu to receive the authentication call. You will get an automated call from the University of Colorado. Follow the instructions in the call, and you will be authenticated.
4. If you select "Text,"" you must choose a "CELL" or "MOBILE" device from the drop-down menu. Then, click on "Send SMS passcodes" to receive an SMS text message containing a passcode. Just enter that passcode into the portal's authentication screen, click "Log in" and you will be authenticated.

Only protected pages require authentication.

The University of Colorado understands the demands placed on its faculty and staff, so it implemented multifactor authentication to cause minimal disruption to your workday. You will be asked to authenticate your identity only when you try to access the following items in the **CU Resources** area of the portal [2]:

- direct deposit
- W-2
- W-4
- phone number (only when you push the “Change phone numbers” button in "Employee Profile")
- Employee Profile

- Benefits Summary

Example: If you view your phone number in the "Employee Profile" page, you won't be asked to authenticate. But when you click the "Change phone number" button, you'll be asked to authenticate your identity. After you authenticate once, you will be able to access all your information for the rest of your portal session. Your authentication will last up to eight hours as long as your session does not terminate.

Frequently Asked Questions

Whom do I contact for help if I have problems using the authentication system?

If you are having difficulty using the authentication system because you think your phone number may be incorrect or you need to add a different phone number, please contact your department's payroll liaison for assistance.
If you are a retiree or surviving spouse, please contact Employee Services at 303-860-4200, option 3, or EmployeeServices@cu.edu [5]for assistance.

For other issues, please email Employee Services at hcm_community@cu.edu [6]. Please include your name, employee ID, contact information and a description of the problem.

What is multifactor authentication?

Unfortunately, passwords aren't as secure as they used to be. If someone gets your password, they can access your account without any fuss.

multifactor authentication seeks to decrease the likelihood that others can access your data. It takes two items to access and update your information: “something you know” (like your password) and “something you have” (like your phone).

One simple example: Using an ATM machine. When you visit an ATM, one authentication factor is the ATM card you use to start the transaction. That's the “something you have.” Next, you enter a PIN number, which is the "something you know."" Without both of these factors, your authentication will fail.

Why did CU implement this multifactor authentication?

Increasingly, colleges and universities are a target for cyber criminals using fake ".edu" email addresses, according to the FBI and U.S. Department of Homeland Security. The enhanced security is CU's response to late 2013 phishing attacks that tricked several employees into giving their passwords to cyber criminals, who then altered their direct deposit information and stole their paychecks.

The university implemented authentication software from Duo Security, whose technology is used by the University of California Berkley, University of Michigan, Michigan State, University of Minnesota, University of Illinois and many major corporations.

How does the Duo Security software get my phone numbers?

The University feeds phone data (Home, Cellular, Campus 1, and Campus 2 phone types only) from HCM to Duo for CU employees and retirees. Updates are sent in real time to ensure the phone numbers you have in HCM are available for use in Duo. *Note: If you prefer to receive alerts from CU via text message, be sure that you have entered your cellphone number in the "cellular" phone field*.

Which HCM phone types are available for use in Duo?

The University feeds phone numbers for the following phone types to Duo: Home, Cellular, Campus 1, and Campus 2. *Note: If you prefer to receive alerts from CU via text message, be sure that you have entered your cell phone number in the “cellular” phone field*.

What should I do if I need to update my phone numbers in Duo?

You are required to authenticate yourself using the multifactor authentication process in order to update your information via self-service in the portal. If you are able to authenticate yourself using an existing phone number, you can update your phone data by going to "Employee Profile" in the My Info and Pay horizontal menu bar within the portal. Once there, click on the "Change phone numbers" button to update your information.
If you are not able to authenticate yourself in order to change your phone information via self-service, please contact your department's payroll liaison for assistance. Changes made by you via self-service and changes made directly in Human Capital Management (HCM), CU's HR tool, your HCM user will be sent in real time to Duo and be reflected in the Duo authentication page the next time you use it.

What if I can't update my phone information in the portal since multifactor authentication is required?

You will need to contact your department's HCM Community member (formerly known as a payroll liaison) for assistance with updating your phone information. If you are a retiree or surviving spouse, please contact Employee Services at 303-860-4200, or EmployeeServices@cu.edu [7].

What Phone types from HCM will have the SMS passcode option on the Duo authentication page?

The only phone type from HCM that will have the SMS passcode option in Duo is the CELL type.

How do I get the SMS passcode option?

You must select a CELL phone type on the Duo authentication page, in order to have the option to receive a SMS passcode.

Can the system handle international phone numbers?

Yes, Duo can handle international phone numbers. If entering an international phone number in self-service or HCM, you can leave a space between country code, city code, and the phone number.

How long will my authentication last?

Your authentication will last up to eight hours as long as your session stays active.

I've updated all of my phone data in HCM, but I still see another phone in the Duo page called MOBILE. Why?

The integration also pulls in MOBILE/CELL phone data from Campus Solutions. The MOBILE phone number can be updated in Campus Solutions, if need be.

I only own one phone number: a CELLPHONE. Should I populate that CELL number in both the CELL and HOME phone types?

No, use unique numbers in HCM; do not use the same number more than once. If you prefer to receive alerts from CU via text message, be sure that you have entered your cellphone number in the "cellular" phone field.

In Duo, a phone number can exist only once, unlike in HCM, where phone numbers do not have to be unique. Customers should only use cellphone numbers in the CELL phone type in HCM as that phone type is the only one that has SMS (text) abilities.

If the customer does not have a Home or Campus number they should just leave those phone types blank.

The system says 'enrollment is disabled. Access denied.' What should I do?

Most likely you are receiving this message because you do not have a phone number for one of the valid phone types (Home, Cellular, Campus 1, or Campus 2) in HCM. You may verify this by reviewing your phone information in the Employee Profile section under Personal Information in the CU Resources section of the portal. If that is the case, please contact your department's HCM Community member (formerly known as a payroll liaison) for assistance with updating your phone information. If you have a phone number for one of the valid phone types in the system, please contact hcm_community@cu.edu [8] for assistance.

Can I use Duo's additional authentication methods: Duo Push or passcodes generated via Duo Mobile, via a hardware token, or by an administrator?

The University of Colorado does not support these methods of obtaining passcodes at this time. Phone callback authentication and passcodes via SMS Text Message are the only available options at present.

Groups audience:
Employee Services
Right Sidebar:

ES: Multifactor Authentication

Source URL: https://www.cu.edu/employee-services/mycuedu-security-strengthened-new-authentication-tool

Links
[1] https://www.cu.edu/employee-services/mycuedu-security-strengthened-new-authentication-tool
[2] http://my.cu.edu
[3] https://blocsonic.com/releases/show/the-unattainable-re-mixx-instrumentals
[4] https://creativecommons.org/licenses/by-nc-nd/4.0/
[5] mailto:EmployeeServices@cu.edu ?subject=multifactor%20authentication
[6] mailto:hcm_community@cu.edu?subject=mutli-factor%20authentication
[7] mailto:EmployeeServices@cu.edu
[8] mailto:hcm_community@cu.edu