Published on *University of Colorado* (https://www.cu.edu)



# Remote Work FAQ [1]

With many CU System Administration staff working remotely, the following resources will keep you connected, more secure and aid in making your work more productive.

## Coronavirus-themed scams

### What are some of the channels being used to deliver fraudulent messages?

- **Electronic channels** being used to deliver fraudulent messages are prevalent - email, text, websites, social media, phone and robocalls
- Messages appear to come from **trustworthy organizations**:
  - Centers for Disease Control and Prevention CDC)
  - World Health Organization (WHO)
  - Internal Revenue Service (IRS)
  - Social Security Administration
  - Federal Trade Commission (FTC)
- Messages claim to be from **businesses with which we have relationships**:
  - financial services
  - insurance companies
  - health care providers
  - videoconferencing services
- Fraudsters are choosing from an **ample list of subjects** when crafting their fake messages:
  - Offers for cures, vaccines, test kits, sanitizers, protective wear (**face masks top the list**)
  - Assistance with economic relief and recovery
  - Tech / helpdesk support
  - Online pet adoption or rescue

### Can I see some examples of recent phishing scams?

There is no shortage of the approaches scammers are utilizing. Here are some of the most common phishing scams:

- As reported by CNN [2], scammers are sending text messages informing recipients they have **come in contact with someone who tested positive** or has tested positive or is showing symptoms

- The Better Business Bureau (BBB) reports [3] a text message that claims to come from the Department of Health and Human Services. Recipients are directed to click on a link and complete a **“mandatory online COVID-19 test.”**
- The Federal Trade Commission (FTC) reported on seven scams targeting businesses [4], including an email message that **appears to come from the recipients’ IT helpdesk**. The message tells recipients, “The meeting has been shifted to our new teleconferencing platform. Here’s the link.” Clicking on the link permits malicious software to be downloaded.
- The Federal Communications Commission reports [5] robocalls in which recipients are told to call the listed phone number to learn about new measures that include waiving interest on **federal student loans** or the **availability of free testing kits**:
    - *“Hello this is Brad ... with an important message regarding the effects of the coronavirus outbreak on your student loans. As you may have already heard, President Trump invoked his power as commander-in-chief by declaring a national emergency due to the widespread impact of COVID-19. New measures will include waiving interest on your federal student loans until further notice…For more information on how these new measures will impact your future payment obligations, call us back today at…”*
    - *“...[The Coronavirus] Response Act has made coronavirus testing more accessible immediately. If you want to receive a free testing kit delivered overnight to your home, press 1. If you do not want your free testing, press 2.”*

## What resources does OIS recommend for up-to-date awareness?

Regularly check these sites for updates on coronavirus-themed phishing scams:

- Better Business Bureau - Coronavirus [6] or BBB Scam Tracker [7]
- Federal Communications Commission – COVID-19 Scams [5]
- Federal Trade Commission – Coronavirus Scams [8]

Stay Safe Online offers a COVID-19 Security Resource Library [9] that offers press releases, tip sheets and videos for publication. Two examples include:

- Press Release-National Cyber Security Alliance Encourages Vigilance Against Coronavirus Scams, Best Cybersecurity Practices for Remote Workers [10]
- Tip Sheet-Security Tips for Remote Workers [11]

This poster and video, provided by Proofpoint - OIS' simulation phishing vendor:

- Video: Attack Spotlight: COVID-19 Phishing Emails [12]
- Poster: COVID-19 Phishing Scams [13]

## How can I avoid phishing scams?

Always be mindful. Fraudsters go to all of this effort to trick people because it is financially profitable. The coronavirus-themed subject line may be different, but it is still the same

phishing scam.

The FBI Cyber Division [14] provides these tips to avoid phishing scams:

- Be wary of unsolicited attachments, even from people you know. Cyber actors can "spoof" the return address, making it look like the message came from a trusted associate.
- Keep software up to date. Install software patches so that attackers can't take advantage of known problems or vulnerabilities.
- If an email or email attachment seems suspicious, don't open it, even if your antivirus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the antivirus software might not have the signature.
- Save and scan any attachments before opening them.
- Turn off the option to automatically download attachments. To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and disable it.

The Better Business Bureau [3] provides these tips to spot a COVID-19 text message scam:

- Government agencies do not typically communicate through text messages.
- Ignore instructions to text "STOP" or "NO" to prevent future texts. This is a common ploy by scammers to confirm they have a real, active phone number.
- If you think your text message is real, be sure it's directing to a web address like "agency.gov" or “agency.ca,” not "agency.otherwebsite.com."
- Check for look-alikes. Be sure to do your research and see if a government agency or organization actually exists. Find contact info on your own and call them to be sure the person you’ve heard from is legitimate.

More tips from the Office of Information Security [15]:

- Do not provide your username, password or any personal information requested by unsolicited email.
- Do not click links or attachments unless you are positive the content is safe.
- Ignore tactics aimed to scare you into taking urgent action, including: threats of a lawsuit, a computer full of viruses, locked accounts or opportunities to earn or save money now.
- Legitimate companies and service providers will provide a way for you to contact them directly. If you’re uncertain, you can learn more by researching them online.
- Verify the legitimacy of charities and crowdfunding sites before making donations. Do not provide donations in cash, gift cards or money wires.
- Be on alert for these and other similar phishing emails and recognize the red flags:
    - Messages of fear and urgency: Legitimate messages will not instill fear or demand that you take urgent action.
    - Requests for personal or financial information: No public health or government agency will send you an email message (or call) asking for personal or financial information.
    - Links and attachments: Cybercriminals can use links and attachments to deliver malware to your computer and gain access to sensitive work or personal information. They may also lock your computer for ransom until a payment is

received.

### How do I report a suspected phishing scam?

If you receive a phishing message that appears to come from CU or mentions CU, report it to your campus technology or information security staff.

If you suspect that your university-provided computer may be compromised or if you inadvertently disclosed sensitive university information to unauthorized individuals, it is important to report it immediately.

Visit the Office of Information Security [16] website for more Information on how to report potential incidents.

## Technology purchases

### I need to purchase equipment. What are the steps I need to take?

CU System employees have realized they need additional equipment or software to effectively work remotely.

Here are a few reminders on our purchasing processes and policies:

- **Getting started:** The UIS Service Desk is available to assist with purchasing IT-related equipment, but departments are responsible for funding these purchases. To initiate the process, please email the UIS Service Desk [17], making sure to include manager approval and Speedtype on all purchasing requests.

- **Purchase and delivery:** Technology purchases using CU funds, including those made with a department's Procurement Card, must be properly imaged, installed and asset tagged. This ensures the item is secure, inventoried and that you can access the CU-specific applications you need. Therefore, all IT purchases must be shipped to the System Office:
  Your Name
  Attn: UIS Service Desk
  1800 Grant Street STE 200
  Denver, CO  80203

- **Set an appointment:** The Service Desk is also practicing social distancing as much as possible but will be available in-person on select days from 10 a.m. - 2 p.m., **by appointment only**. The Service Desk will contact you when your order is delivered. For software purchases, they can install remotely. For physical equipment, they can either schedule an appointment time when you can come and pick it up or leave your

equipment at your desk (or other secure location) once it has been properly imaged and asset tagged.

- **Special requests:** In special situations (higher risk individuals, those with immunocompromised persons in their home, anyone out of the state, etc.), the Service Desk may be able to ship your equipment to you after it has been properly imaged and asset tagged. Please contact them *before completing the purchase* to understand the options available.

### I've already ordered an item. Is there anything else I need to do?

If you have already made an IT equipment purchase and had it delivered to your home address, reach out to the UIS Service Desk [18] immediately to determine what additional steps must be taken.

## Connecting to work files

### What do I do if my machine is sluggish in connecting to CU applications?

Before contacting the Service Desk, check your internet plan and run a remote internet connection using a broadband speed test like Speedtest [19] or Fast [20]. If the results are not around what you are paying for or you are unsure of your internet plan, contact your internet provider.

If your results are fine, but your connection still is not, check the UIS website [21] for known Service Alerts. Report any outages or issues not listed to the UIS Service Desk by calling 303-860-HELP (4357) or emailing help@cu.edu [18].

If you would like to receive communications regarding service interruptions, sign up to receive RAVE alerts [22].

### Why can’t I connect to a CU-specific application?

If you are having issues connecting to a CU-specific application, first make sure you are connected to the VPN, then log in using your normal process and credentials.

If you still cannot connect, contact the UIS Service Desk by calling 303-860-HELP (4357) or emailing help@cu.edu [18].

### What is VPN and why do I need it?

VPN is a Virtual Private Network that allows you to send and receive data on your own network as though you were directly connected to 1800 Grant's private network.

You must be connected to the VPN in order to connect to CU applications, access your personal P: drive and any shared drives, and to ensure you receive the regular (and often critical) updates pushed out to your machine by the UIS Service Desk.

For detailed instructions, please review the Service Desk's How-To Guides on VPN:

- Configure Cisco AnyConnect on Android [23]
- Configure Cisco AnyConnect VPN for iOS [24]
- Install and configure Cisco AnyConnect VPN for [25]Windows [25]

Still having issues? Contact the UIS Service desk by calling 303-860-HELP (4357) or emailing help@cu.edu [26].

## What is Remote Desktop and do I need it?

A Remote Desktop allows you to access and use your work computer from another device. This is beneficial to those who will be working remotely and have a desktop computer, as opposed to a laptop or were unable to take their laptop out of the office.

To connect to your work computer using Remote Desktop, you do need to know the computer name you are trying to remotely connect to. Those instructions are detailed in the How-To Guides below, but can also be obtained by a Service Desk technician during regular business hours.

Please review the Service Desk's How-To Guides on connecting to a remote computer:

- Connect to a remote computer in Windows [27]
- Connect to a remote computer in MacOS [28]

## How do I get to my network drive / P: drive?

To access your network drive / P: drive, you must first connect to the VPN. You can then open your File Explorer and access drives as usual.

Still having issues? Contact the UIS Service desk by calling 303-860-HELP (4357) or emailing help@cu.edu

[29].

# Collaboration tools

## What is Teams and why do I need it?

Microsoft Teams is a communication and collaboration platform that provides you ways to send instant messages, meet with others via phone or video, share screens, and collaborate on documents. Microsoft Teams will be essential in ensuring that you are able to effectively collaborate and stay connected to others, even while working remotely. It should already be installed on your computer.

You can use Teams for audio and video calls, so it is a great alternative for those without a Zoom license or if Zoom runs into connectivity issues.

Please review the Service Desk's How-To Guides on Microsoft Teams for more details:

- Microsoft Teams Quick Start Guide [30]
- How to Install Microsoft Teams on an Android Device [31]
- How to Install Microsoft Teams on Mac iOS [32]
- How to Install Microsoft Teams on Windows [33]

Still having issues? Contact the UIS Service desk by calling 303-860-HELP (4357) or emailing help@cu.edu [18].

## What is Zoom and how does it work?

Zoom is used for video conference, webinars and large meetings. You don't need a license to join a Zoom meeting, but you do need a license to setup and host meetings. CU System has ensured that it has enough licenses for all its employees.

Like with Microsoft Teams, Zoom will be an essential tool used to communicate and collaborate while many of us are working remote, so please send your request for a Zoom license to help@cu.edu [34].

### Need help getting started?

- Zoom has a number of useful, one-minute videos [35] to guide you.

- The UIS Service Desk also has a number of step-by-step guides [36] to assist you. *(CU login required.)*

## Can I add Zoom to Outlook or my desktop?

Yes. Use this step-by-step guide [37] for details on:

- How to install Zoom Plugin for Outlook 2016
- How to set up Calendar Integration

## Do you have tips for hosting a successful Zoom meeting?

This step-by-step guide [38] will provide tips and tricks to ensure your Zoom meetings are successful.

## I have Zoom installed, but I'm having issues connecting when I try calling into a meeting. What do I do?

Due to increased volume, many people are reporting issues with call-in numbers being overloaded, resulting in problems connecting or being dropped from calls.

To circumvent this issue:

- Please try joining the meeting using the Zoom meeting link and using Computer Audio, instead of via a phone call.
- If that doesn't work, you can also use Teams for audio and video calls and to share your screen, so it is a great alternative to Zoom when connecting to others.

Still having issues? Contact the UIS Service desk by calling 303-860-HELP (4357) or emailing help@cu.edu [18].

## How do I prevent Zoom bombing?

UIS adjusted CU System Administration's default Zoom settings on April 2, based on best practices to mitigate risk and ensure meeting security. While Zoom encrypts meetings by default to provide authentication, privacy and data integrity, these changes are intended to prevent "Zoom-bombing" – where uninvited guests intrude on Zoom meetings, often by simply typing in random Meeting IDs.

**System Administration settings changes**

- Meeting ID set to generate automatically
- Only the host can share their screen or transfer screen sharing control to others
- Host can start sharing when someone else is sharing

- Disable file transfer
- Disable remote control
- Disable desktop/screen share for users

Any meetings setup prior to these changes will not have the default best practices in place. You may need to make manual adjustments.

## Adjust your settings

You can control other settings by logging into CU System Administration's Zoom site [39], and selecting "Settings" from the left-hand menu.

**Assign a Co-host:** Adding alternative host or co-host can assist with the mitigation of a Zoom-bomber immediately. If you manage calendars and are setting up Zoom invites for others, you must set up the person who will lead the meeting as a co-host [40].

**Waiting Room:** This option is especially effective when running large, public meetings. When this option is selected, participants waiting to join the meeting will see a customizable Waiting Room screen and are unable to join the meeting until the host admits them.

**Allow Host to Put Attendee on Hold:** Turning on this setting, allows the meeting host to remove attendees by either moving them back to the waiting room or removing them from the meeting all together. When an attendee is removed completely from the meeting, they cannot rejoin the same meeting.

Other Zoom security features can be adjusted within the meeting itself.

**Screen Sharing:** The meeting host can control what is shown on the screen at any given time or allow participants to share their screens, as needed, through the Screen Share option during a meeting. This prevents accidental and intentional screen sharing.

**Lock the Meeting:** Once the meeting begins and you no longer wish to allow anyone else to join, you can lock the meeting so that no other participants can join, even if they have a password. This can be done from within the meeting itself by clicking "Manage Participants," going to the pop-up box, selecting "More" and "Lock Meeting."

Be mindful when sharing or discussing sensitive university information in virtual meetings. Only share such information with the people who need to know it for an authorized use. This includes verbal and written information.

Visit the UIS Zoom Sharepoint [41] to view Zoom guides and tutorials (*login required*).

If you need assistance using Zoom or adjusting your settings, contact the UIS Help Desk at 303-860-4357 (HELP) or email help@cu.edu [18].

# Phones

### How do I forward my phone calls?

Each CISCO phone has a way to forward your office phone calls to another number. Looking at your phone screen, select either the “CFwdALL” option, or a “Forward All” option. After you hear 2 short beeps, enter the phone number calls should be forwarded to (including +8 1). The phone will beep once and a message saying “Forwarded to 81##########” will appear on the phone screen. If you do not see this message on your screen, please hang up and try again.

At this time, there is no way for remote users to forward phone calls themselves, but the Service Desk Technicians can help you with this. Please submit a request to the UIS Service Desk by calling 303-860-4357 (HELP) or emailing help@cu.edu [42].

## Support

### What do I do if my CU machine crashes while I’m working remotely?

The UIS Service Desk will still be available for any equipment issues you run into, with technicians available onsite select days from 10 a.m. - 2 p.m. **by appointment only**. You’ll follow the same process as if you were in the office.

- First, contact the UIS Service Desk by calling 303-860-4357 (HELP) or emailing help@cu.edu [18] for troubleshooting solutions.
- If those prove unsuccessful, it may be necessary for you to come into the office for service.

### Will UIS come to my house and support my technology?

No, the UIS Service Desk will not be available to physically come to offsite locations to support technology, but will be available at 1800 Grant on select days from 10 a.m. - 2 p.m. **by appointment only** and provide remote assistance to supported devices.

**Please note:** The Service Desk is able to offer best effort support and basic troubleshooting techniques for personal/non-standard equipment (ex: modems, personal printers, cell phones, etc.), but recommend reaching out directly to your provider for their expertise.

**Groups audience:**
UIS Service Desk
**Right Sidebar:**
UIS Service Desk: Contact

**Links**
[1] https://www.cu.edu/service-desk/how-guides/remote-work-faq
[2] https://www.cnn.com/2020/04/19/us/coronavirus-text-message-scam-trnd/index.html
[3] https://www.bbb.org/article/news-releases/21903-scam-alert-mandatory-covid-19-test-texts-are-a-scam
[4] https://www.ftc.gov/news-events/blogs/business-blog/2020/03/seven-coronavirus-scams-targeting-your-business
[5] https://www.fcc.gov/covid-scams
[6] https://www.bbb.org/council/coronavirus/
[7] https://www.bbb.org/scamtracker
[8] https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing
[9] https://staysafeonline.org/covid-19-security-resource-library/
[10] https://staysafeonline.org/press-release/ncsa-encourages-coronavirus-vigilance/
[11] https://staysafeonline.org/resource/security-tips-for-remote-workers/
[12] https://vimeo.com/400415172
[13] https://www.proofpoint.com/sites/default/files/2020-03/AttackSpotlight_coronavirus_Poster.pdf
[14] https://www.fbi.gov/investigate/cyber
[15] https://www.cu.edu/ois
[16] https://www.cu.edu/ois/report-incident
[17] mailto:help@cu.edu?subject=purchase
[18] mailto:help@cu.edu
[19] https://www.speedtest.net/
[20] https://fast.com/
[21] http://cu.edu/uis
[22] https://www.cu.edu/uis/forms/register-rave-alerts
[23] https://www.cu.edu/docs/how-guide-configuring-cisco-anyconnect-vpn-android
[24] https://www.cu.edu/docs/vpn-configuring-cisco-anyconnect-vpn-ios
[25] https://www.cu.edu/docs/vpn-install-and-configure-cisco-anyconnect-vpn
[26] mailto:help@cu.edu?subject=VPN
[27] https://www.cu.edu/docs/computer-help-connect-remote-computer
[28] https://www.cu.edu/docs/computer-help-connect-remote-computer-macos
[29] mailto:help@cu.edu?subject=%2FP%3A%20Drive
[30] https://www.cu.edu/docs/microsoft-teams-quick-start-guide
[31] https://www.cu.edu/docs/email-and-calendar-how-install-microsoft-teams-android-device
[32] https://www.cu.edu/docs/email-and-calendar-how-install-microsoft-teams-mac-ios
[33] https://www.cu.edu/docs/email-and-calendar-how-install-microsoft-teams-windows
[34] mailto:help@cu.edu?subject=Zoom%20license
[35] https://zoom.us/resources
[36] https://cu0.sharepoint.com/Pages/Zoom/Zoom.aspx
[37] https://www.cu.edu/docs/computer-help-integrate-zoom-outlook-calendar
[38] https://www.cu.edu/docs/how-guide-zoom-tips-and-tricks
[39] http://cusystem.zoom.us/
[40] http://support.zoom.us/hc/en-us/articles/201362603-Host-and-Co-Host-Controls-in-a-Meeting
[41] http://cu0.sharepoint.com/Pages/Zoom/Zoom.aspx
[42] mailto:help@cu.edu?subject=Phones