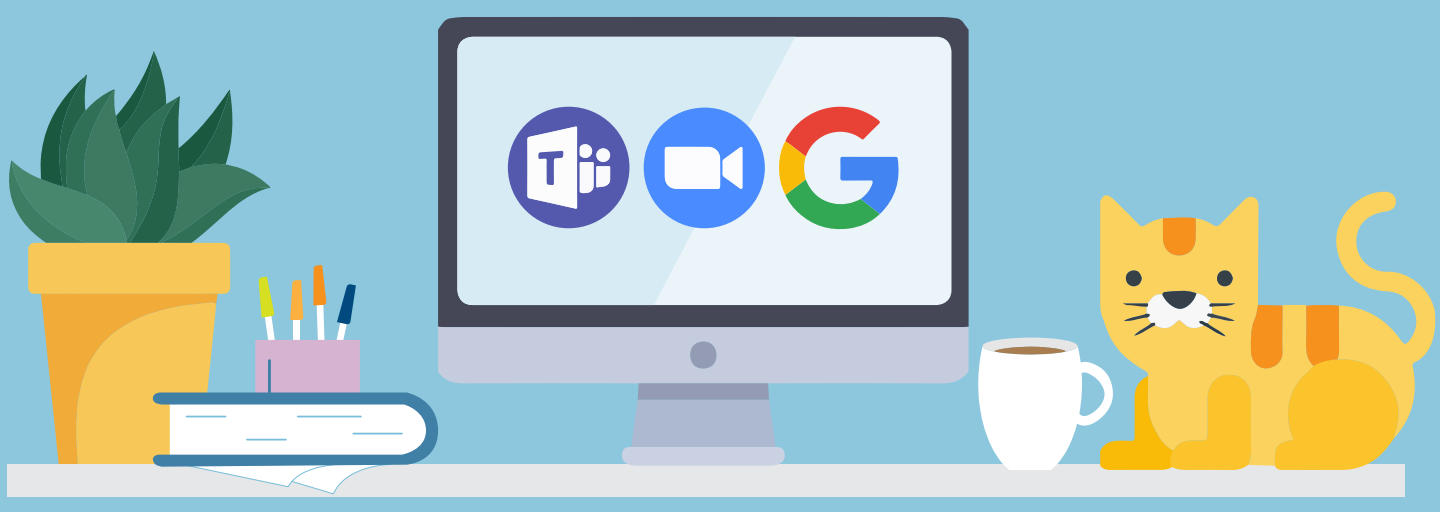
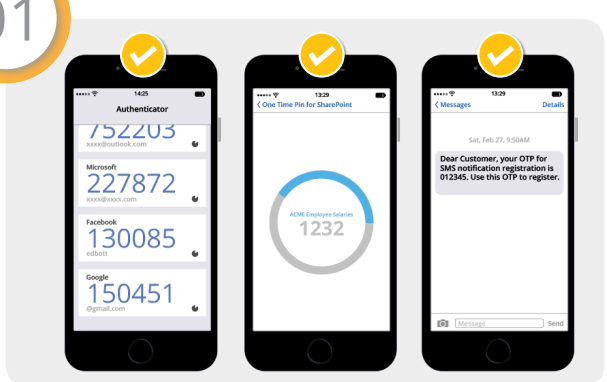


Collaborate Safely

Collaboration tools such as Microsoft Teams, Google, Zoom and others allow you to pull together as a virtual team and securely work while being stuck at home.

But all that sharing, and collaboration can come at a price – there are a few security risks you need to be aware of:

01



Your account passwords are the keys to the kingdom (and to all your data).
Make your passwords strong and unique. Use Multi-Factor Authentication. This is when you combine your username and password with something that you own, such as a One Time Password app on your phone.

02

BEWARE: scammers will try to steal your username and passwords.
COVID-19 has brought about an increase in cyber attacks targeting remote workers on all platforms. Don't click on links asking you to log into a site or update details and don't trust anyone asking you for your passwords over the phone or text.

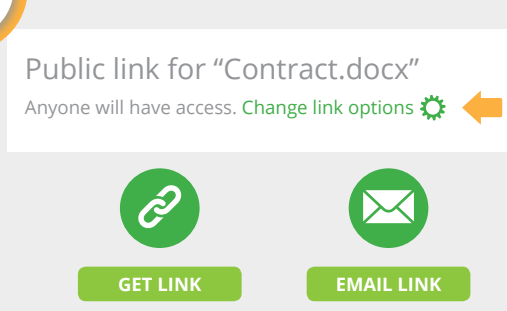
03

Who can do what with my documents?
You can give others permissions to co-author, edit or just view your files through group membership, or you by sending a link to the file. Think about the information and how sensitive it is before sharing it. Anything with personal information, financial data or intellectual property is usually classified.

04

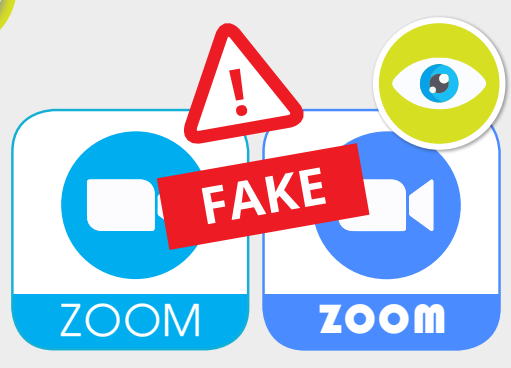
Don't download files to personal devices.
If you are working on a personal device, viewing documents in a browser is probably ok if you have the link and approval of the owner. Refrain from downloading it to your personal and non-managed devices.

05



Think twice before sharing files externally.
External file sharing allows you to share a file with a person that is not part of your company's network. Remember that you are opening a window to your file shares or potentially sending sensitive data outside of your network so be careful about who you share your files with externally.

06



Don't be doomed by fake Zoom.
Zoom has become hugely popular. Cybercriminals are taking advantage of this by registering many new and fake "zoom" domains with the objective of distributing malware.

- Only trust the legitimate zoom.us domain - watch out for lookalike domains
- Double check any Zoom links forwarded to you - verify with the sender
- Keep your Zoom app up to date

07

Prevent Zoom bombing.
Prevent trolls from crashing your Zoom meetings by enabling waiting rooms, not sharing your personal meeting ID in the public domain, controlling screen sharing and locking your meetings when everybody has arrived.

KnowBe4
Human error. Conquered.

Popcorn Training
a KnowBe4 company