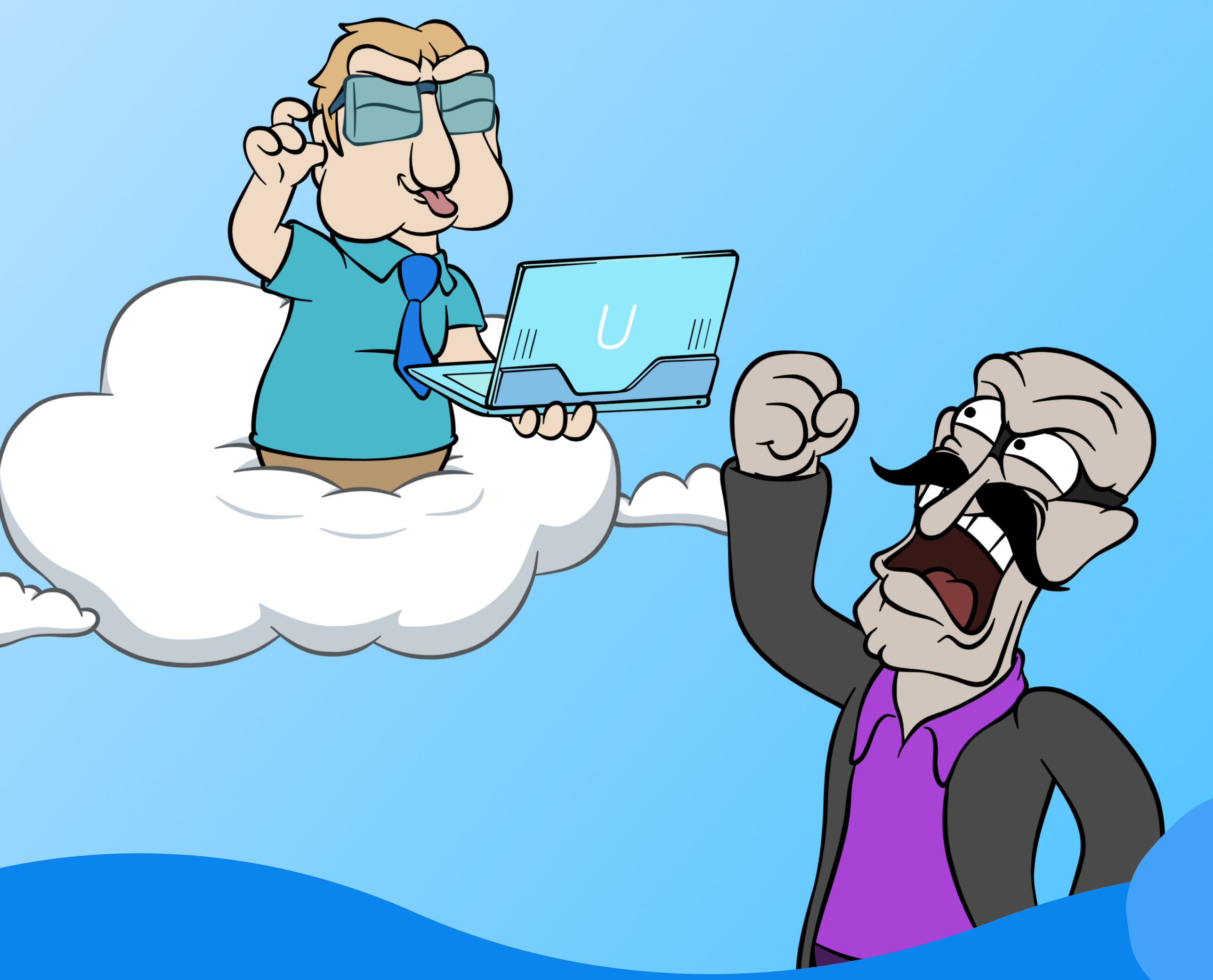

Stay secure in the cloud

Always protect your accounts with strong passwords and use a different one for every cloud service

#StopCyberto

Use the internet securely

Check that you're on the website you think you're on by inspecting the domain or using a search engine to find the legitimate version of the site

#StopCyberto

Keep your devices secure

Try not to leave mobile devices unattended in public and make sure operating systems have the latest updates installed

#StopCyberto

Don't take the phishing bait

Exercise caution when an email tries to create a sense of urgency, such as encouraging an immediate payment or downloading an attachment

#StopCyberto

Don't forget about physical security

Never leave sensitive documents unattended, such as in printer trays or left on your desk

#StopCyberto

Be cautious when using public Wi-Fi

Ensure you’re only connecting to legitimate networks by double-checking the network name

#StopCyberto

Keep your removable devices secure

Always keep your removable devices locked in a secure cabinet when not in use

#StopCyberto

Make sure your password is strong

Your passwords must be unique, private, and easy for you to remember without being easy for an attacker to guess

#StopCyberto

Stay security-savvy when WFH

Changing the default password on your home router and ensuring firmware is updated will help reduce the risk of being hacked

#StopCyberto

Look out for social engineering

Be suspicious if asked to do something you typically wouldn't do (e.g. send money, install something, share customer info, etc.)

#StopCyberto

Stay safe on social media

Restrict your privacy settings on social media and avoid sharing sensitive information that could be used by a cyber criminal

#StopCyberto