Teleworking Security

University of Nairobi ToTs Training

3rd April 2020

Trainer: Janet Maranga

Training Objectives

The objectives include training on :

- Definition
- Tips to Work from Home Securely
- Basic Digital Security Hygiene

Teleworking

- Working away from the office, i.e., outside of the physical premises of the University
- Staff are using fixed or mobile devices (e.g., PCs, notebooks, tablets, smartphones, etc.).
- Staff are using public or private communication networks e.g., Internet
- It allows for Business Continuity in extraneous circumstances

Tips to Work from Home Securely

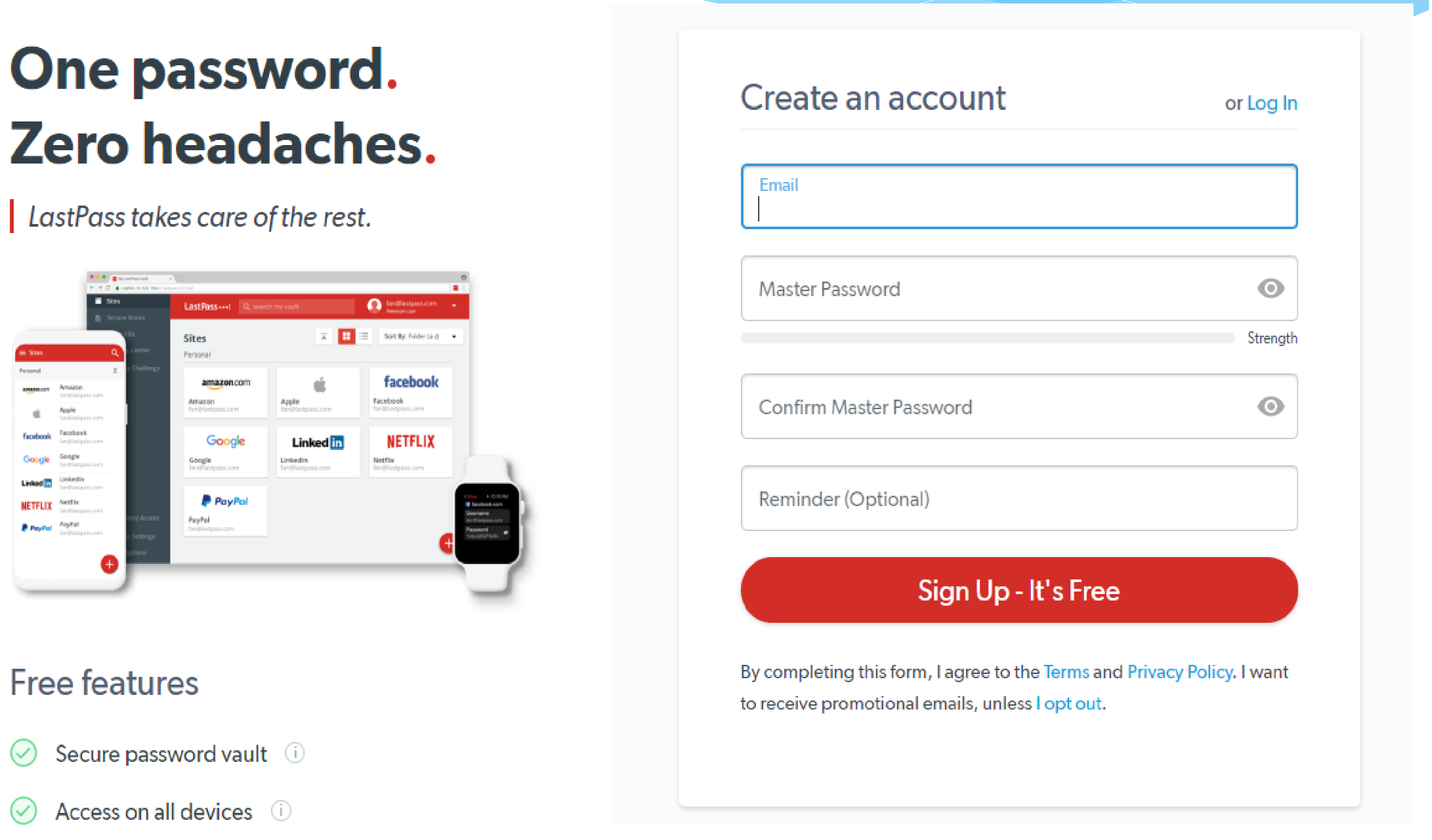
1. Authentication

- Use complex passwords, and never tell these passwords to anyone, note: ICT will **NEVER** ask you for your password to any system
- Use a password manager – This is an encrypted digital vault that stores the login information you use to access apps on mobile devices, websites and other services e.g.

  Lastpass, Keepass, DashLane etc
- Use 2-factor authentication

Example of Setting Up a Password Manager

From a browser: Enter https://lastpass.com/



One password.
Zero headaches.

LastPass takes care of the rest.

Free features

- Secure password vault
- Access on all devices

Create an account

or Log In

Email

Master Password

Strength

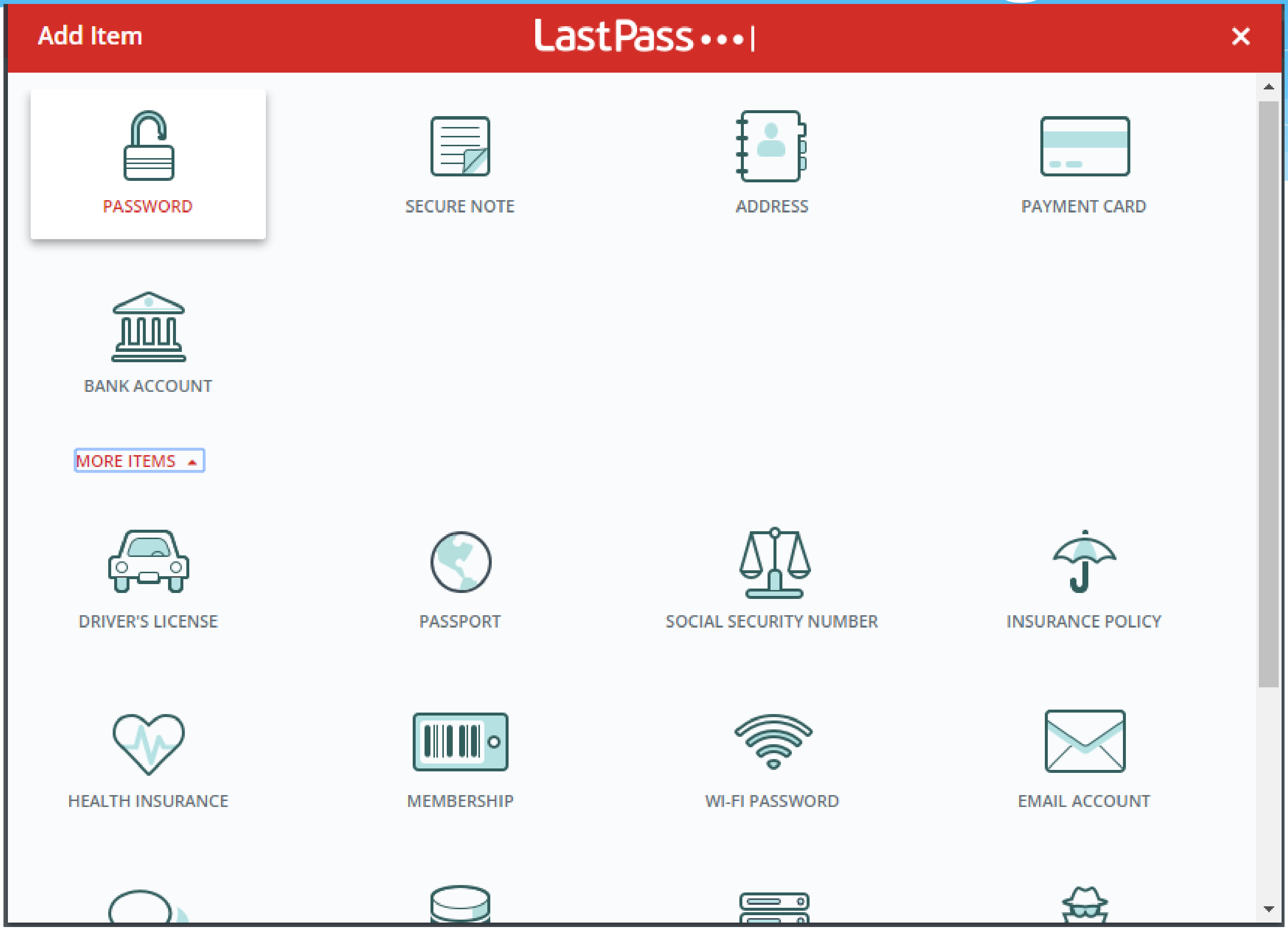
Confirm Master Password

Reminder (Optional)

Sign Up - It's Free

By completing this form, I agree to the Terms and Privacy Policy. I want to receive promotional emails, unless I opt out.

Example of Setting Up a Password Manager



Important Principles for a Password Manager

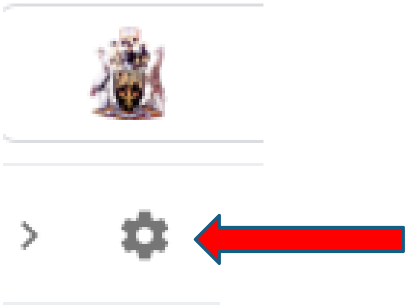
(1) **The master password has to be unique and very secure.** It's like a combination to the safe that holds all your money and everything dear to you. If someone can guess your master password, all your secrets are exposed.

(2) **You must never forget the master password.** The safe cannot be opened without the combination. LastPass customer support cannot look up your password. They can't help you change it.

(3) ***You must never forget the master password*** – Repeat for emphasis

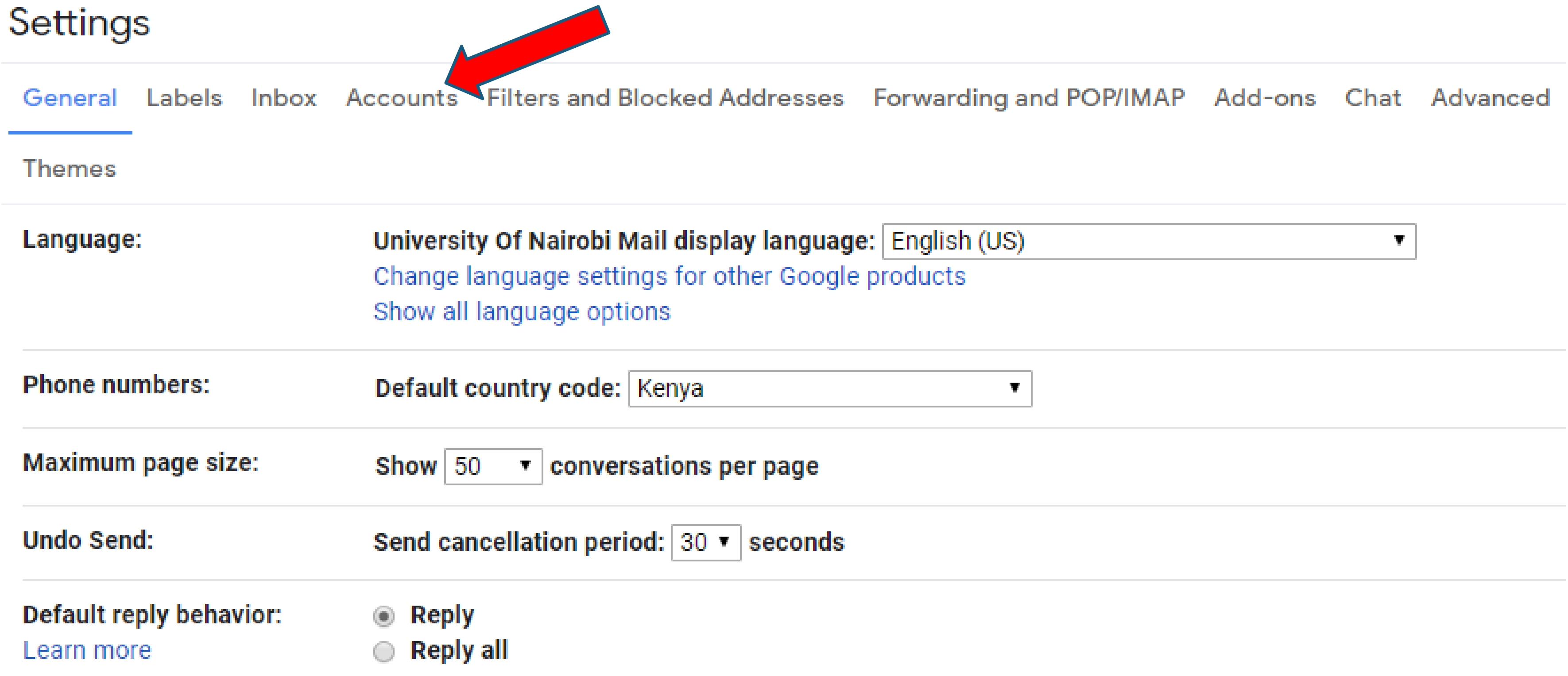
2 Factor Authentication Example

- From your University Google Account, on the top right corner, click the Gear icon



2 Factor Authentication Example

- Click on Accounts



Language: University Of Nairobi Mail display language: English (US) ▾
Change language settings for other Google products
Show all language options

Phone numbers: Default country code: Kenya ▾

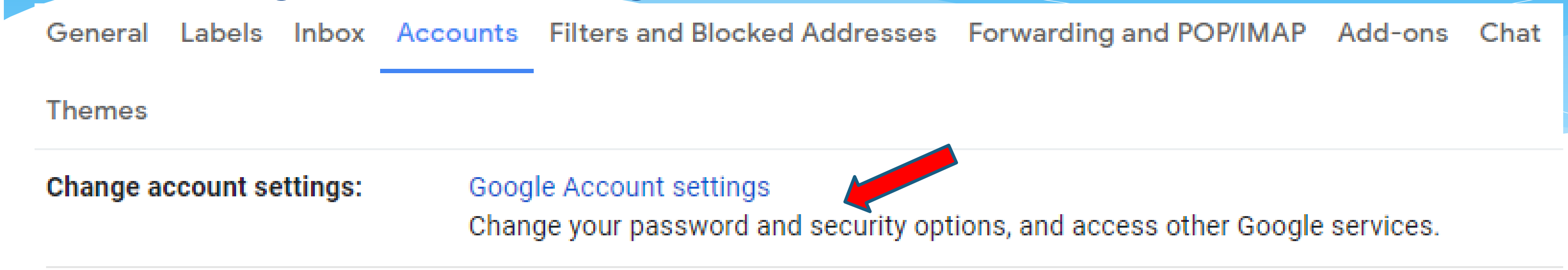
Maximum page size: Show 50 ▾ conversations per page

Undo Send: Send cancellation period: 30 ▾ seconds

Default reply behavior: Learn more
● Reply
○ Reply all

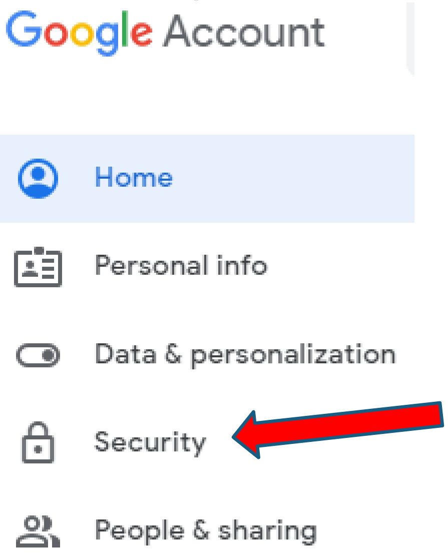
2 Factor Authentication Example

Click on Google Account Settings



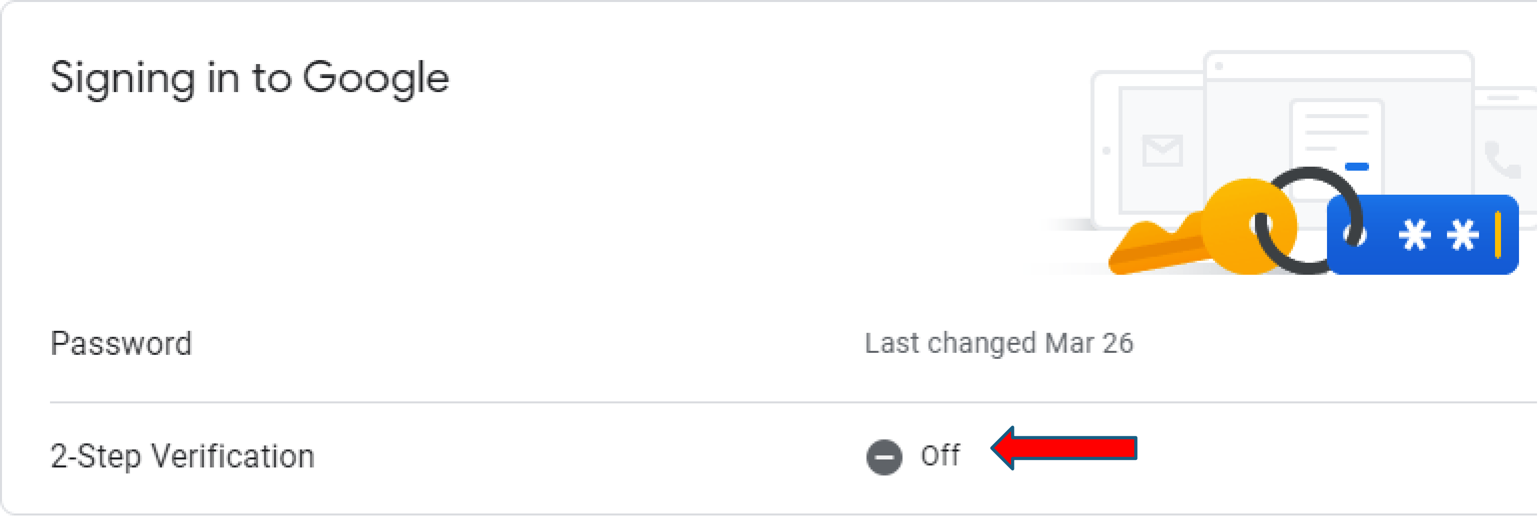
Change account settings: Google Account settings
Change your password and security options, and access other Google services.

On the left pane, click on Security



2 Factor Authentication Example

Click on the Off button to turn it to on



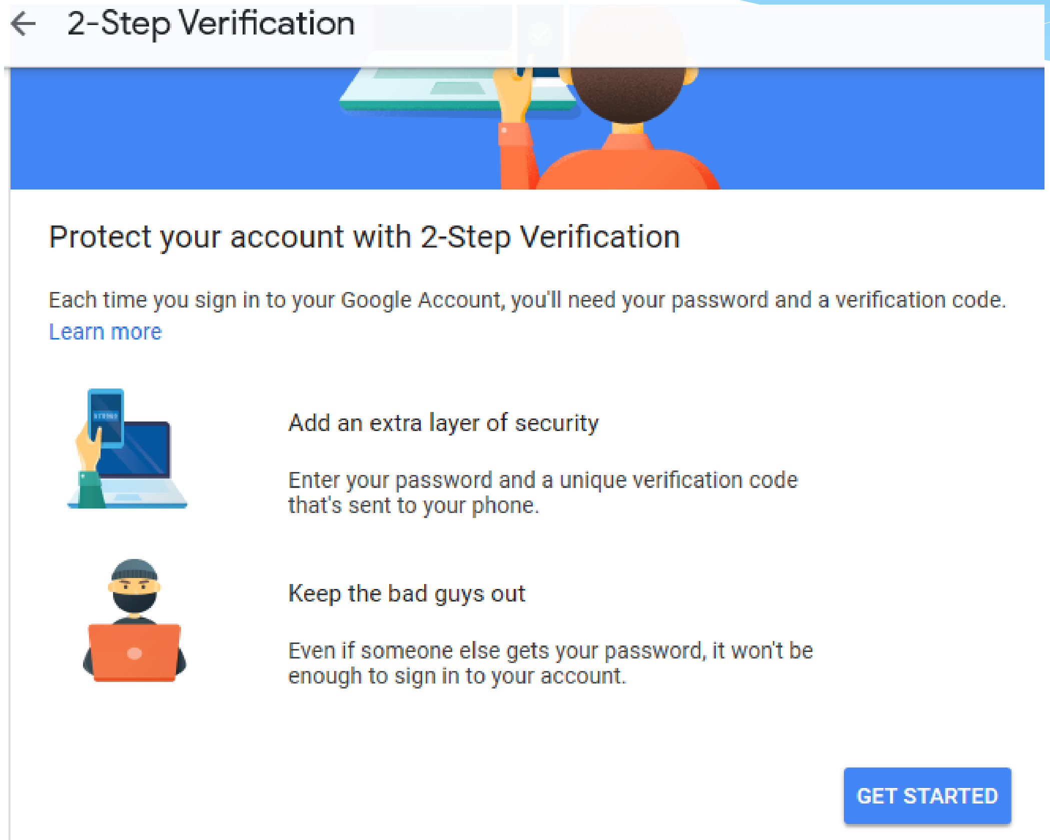
Signing in to Google

Password Last changed Mar 26

2-Step Verification ⊖ Off

2 Factor Authentication Example

Click on - Get Started



2-Step Verification

Protect your account with 2-Step Verification

Each time you sign in to your Google Account, you'll need your password and a verification code. Learn more

Add an extra layer of security

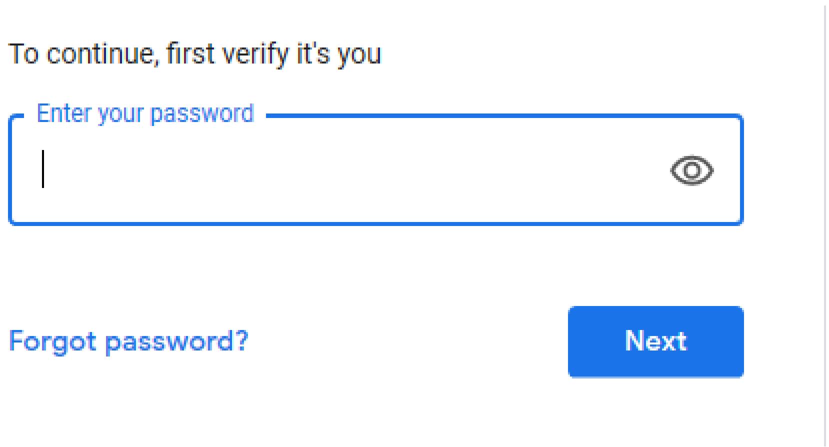
Enter your password and a unique verification code that's sent to your phone.

Keep the bad guys out

Even if someone else gets your password, it won't be enough to sign in to your account.

2 Factor Authentication Example

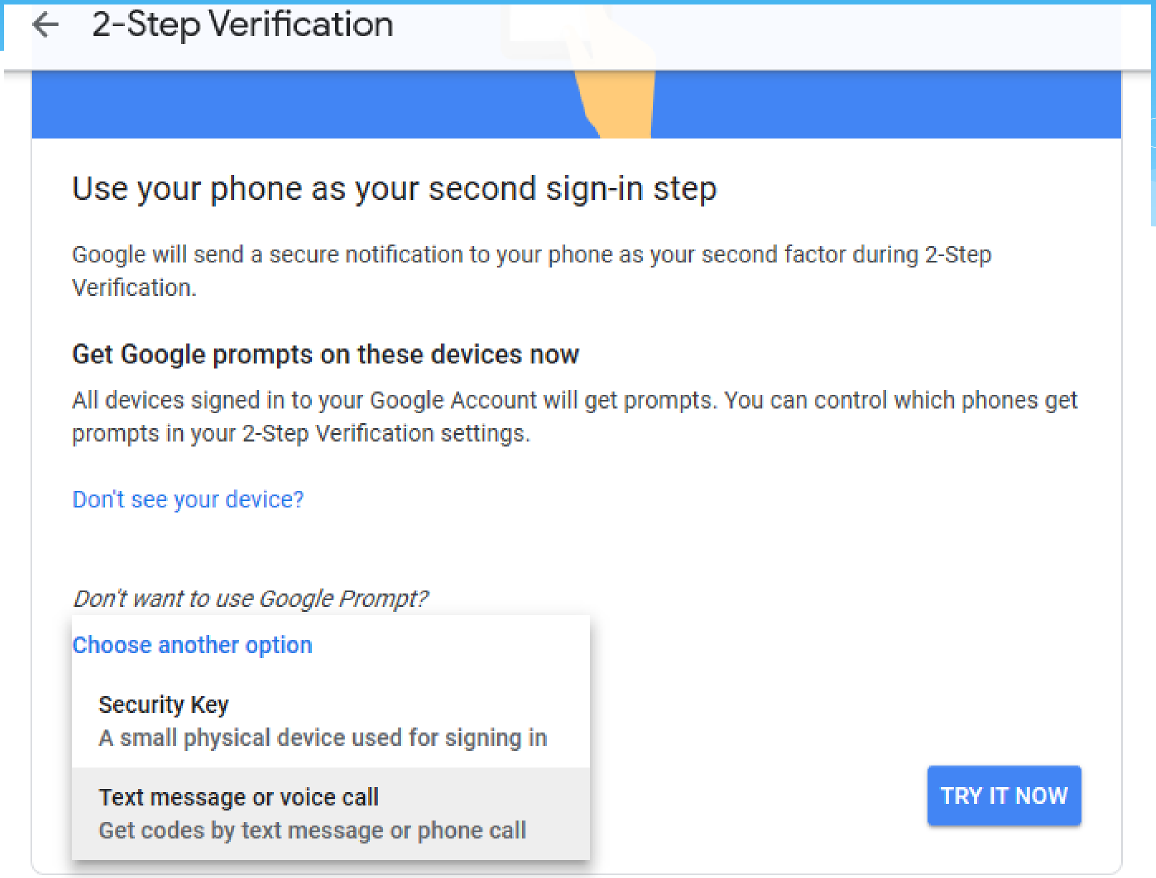
Type in your password at the prompt



To continue, first verify it's you

2 Factor Authentication Example

Select your method of choice



← 2-Step Verification

Use your phone as your second sign-in step

Google will send a secure notification to your phone as your second factor during 2-Step Verification.

Get Google prompts on these devices now

All devices signed in to your Google Account will get prompts. You can control which phones get prompts in your 2-Step Verification settings.

Don't see your device?

Don't want to use Google Prompt?

Choose another option

Security Key
A small physical device used for signing in

Text message or voice call
Get codes by text message or phone call

TRY IT NOW

Link to Video Tutorial - https://youtu.be/UVanCLIx2Aw

Signing in to your account will work a little differently

1. **You'll enter your password**

   Whenever you sign in to University Gmail, you'll enter your password as usual.

2. **You'll be asked for something else**

   Then, a code will be sent to your phone via text, voice call, or Google mobile app.

Signing in to your account will work a little differently

1. **You'll enter your password**

   Whenever you sign in to University Gmail, you'll enter your password as usual.

2. **You'll be asked for something else**

   Then, a code will be sent to your phone via text, voice call, or Google mobile app.

Keep sign-in simple

- During sign-in, you can choose not to use 2-Step Verification again on *that particular computer*. From then on, that computer will only ask for your password when you sign in.

- **You'll still be covered**, because when you or anyone else tries to sign in to your account from *another computer*, 2-Step Verification will be required.

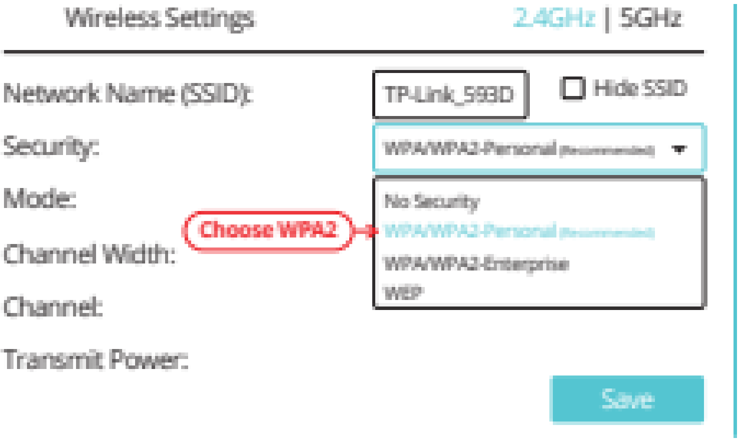
Tips to Work from Home Securely

2. Network Connection

- Avoid Public Wi-Fi - hackers set up such networks in public places, claiming to be legitimate providers, with the purpose of gaining access to users' Internet traffic.
- Secure your home WiFi Network. There are 2 basic must-dos to set this up securely: Change your default router password. If you're still using "admin/admin," "admin/password" or something similar to that log in to your router itself. Change that. Next, when setting up a password for your WiFi network, make sure you choose WPA2. You can request your service provider for a walk through on how to change the default settings and also set up a complex password

Tips to Work from Home Securely

2. Network Connection



Wireless Settings

2.4GHz | 5GHz

Network Name (SSID): TP-Link_593D

□ Hide SSID

Security: WPA/WPA2-Personal (Recommended)

Mode:

Channel Width:

Channel:

Transmit Power:

Choose WPA2

Tips to Work from Home Securely

2. Network Connection

- Use a VPN. Using a virtual private network (or VPN) provides a secure tunnel for all your internet traffic, preventing criminals from intercepting your data –
- Use: https://www.vpn.uonbi.ac.ke

Tips to Work from Home Securely

3. Access to the device

- Keep your work environment private. Keep your home environment safe and ensure nobody is allowed to access your work computer, including your family and kids. Others could unintentionally download malicious software or access files they shouldn’t see. Ensure that your work conversations remain private. If you must share the computer, enable the Guest Account for them to use.
- Avoid printing at home, and if you must, make sure you lock sensitive documents away and shred them before discarding them.

Tips to Work from Home Securely

- Set up a password for your mobile devices.

4. Physical security

- Do not leave your laptops or mobile devices in the car

Tips to Work from Home Securely

5. Backup

- If data is lost and everything else fails, backup is usually the last resort
- Utilize Google Drive to save your files and collaborate securely as well as provide version control if you work on a document as a team.

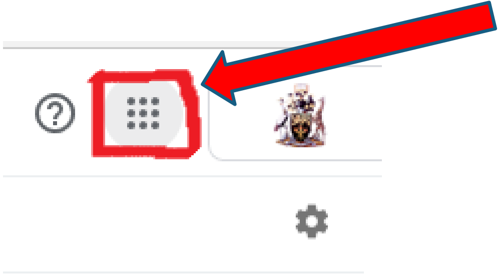
NOTE: When you upload files to Google Drive, they are stored in secure data centers.

- If your computer, phone, or tablet is lost or broken, you can still access your files from other devices.
- Your files are private unless you share them.

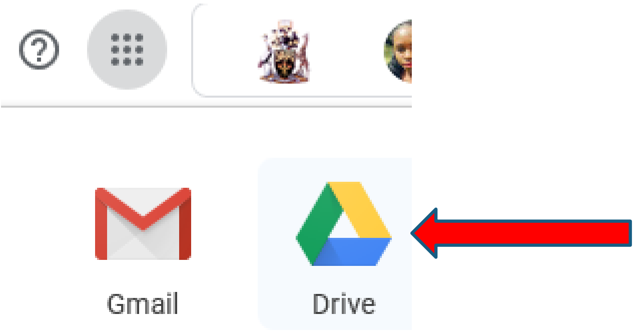
Tips to Work from Home Securely

Google Drive Example

Click on the 9 dots to open Google Apps

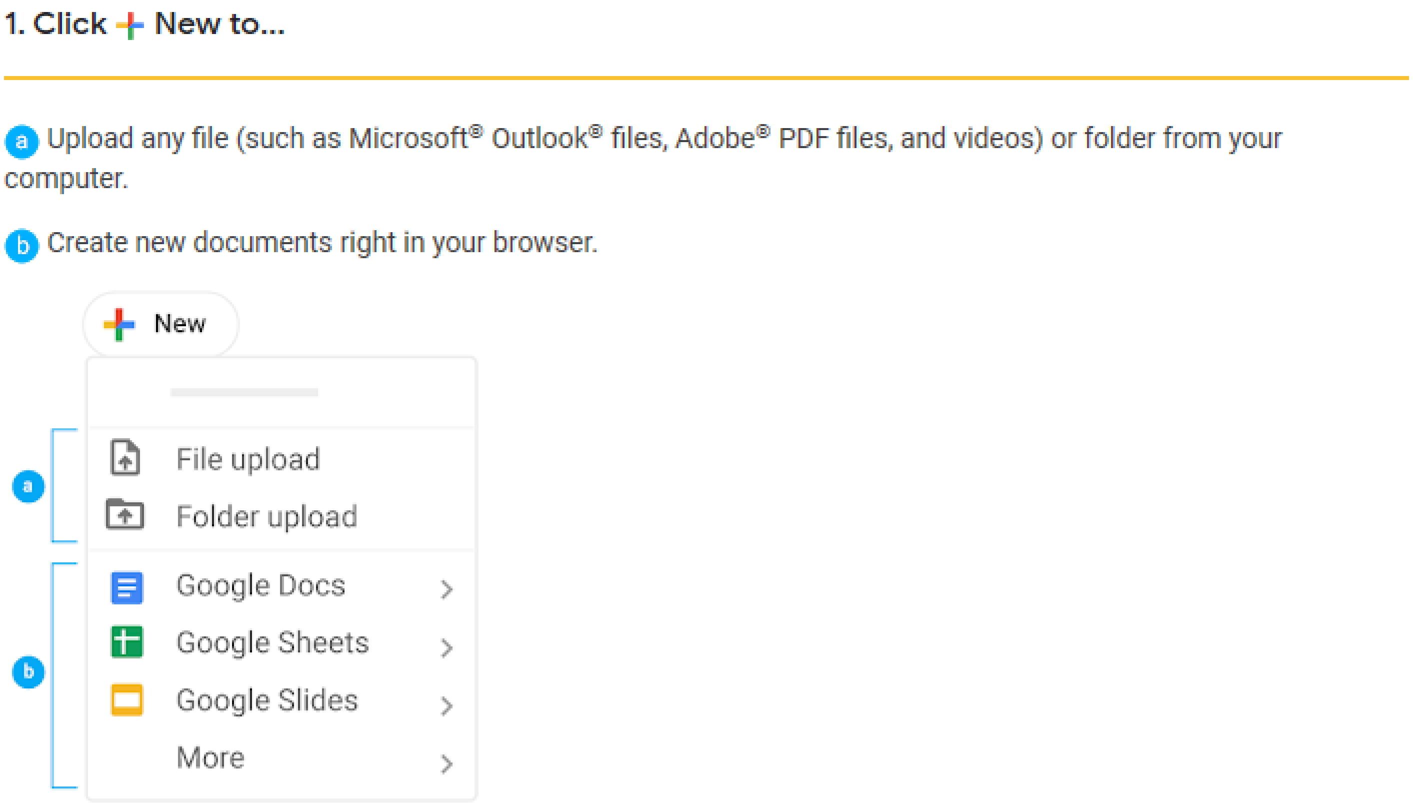


- Click on the Drive Icon



Tips to Work from Home Securely

Create new documents, right in your browser



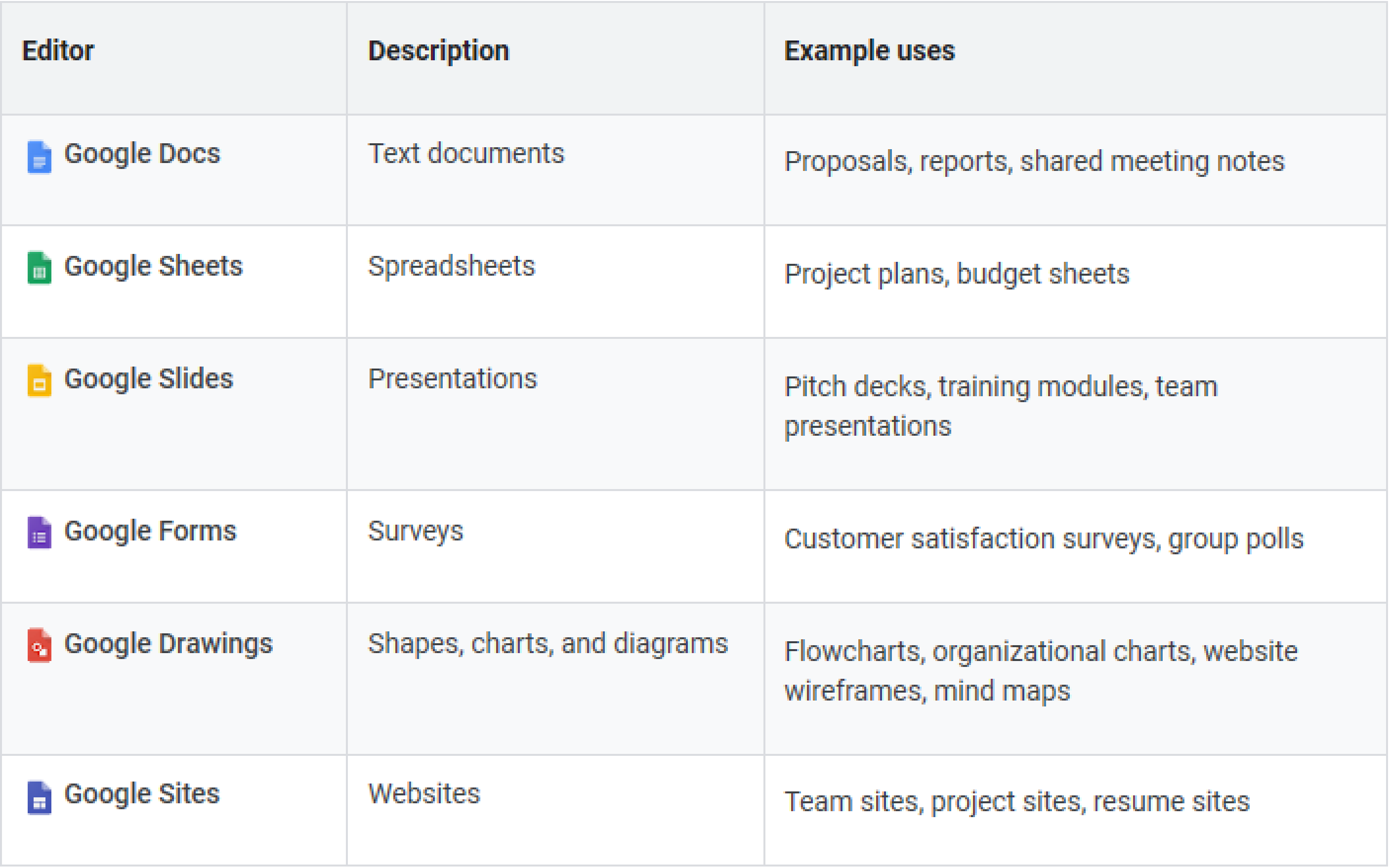
1. Click + New to...

a Upload any file (such as Microsoft® Outlook® files, Adobe® PDF files, and videos) or folder from your computer.

b Create new documents right in your browser.

Tips to Work from Home Securely

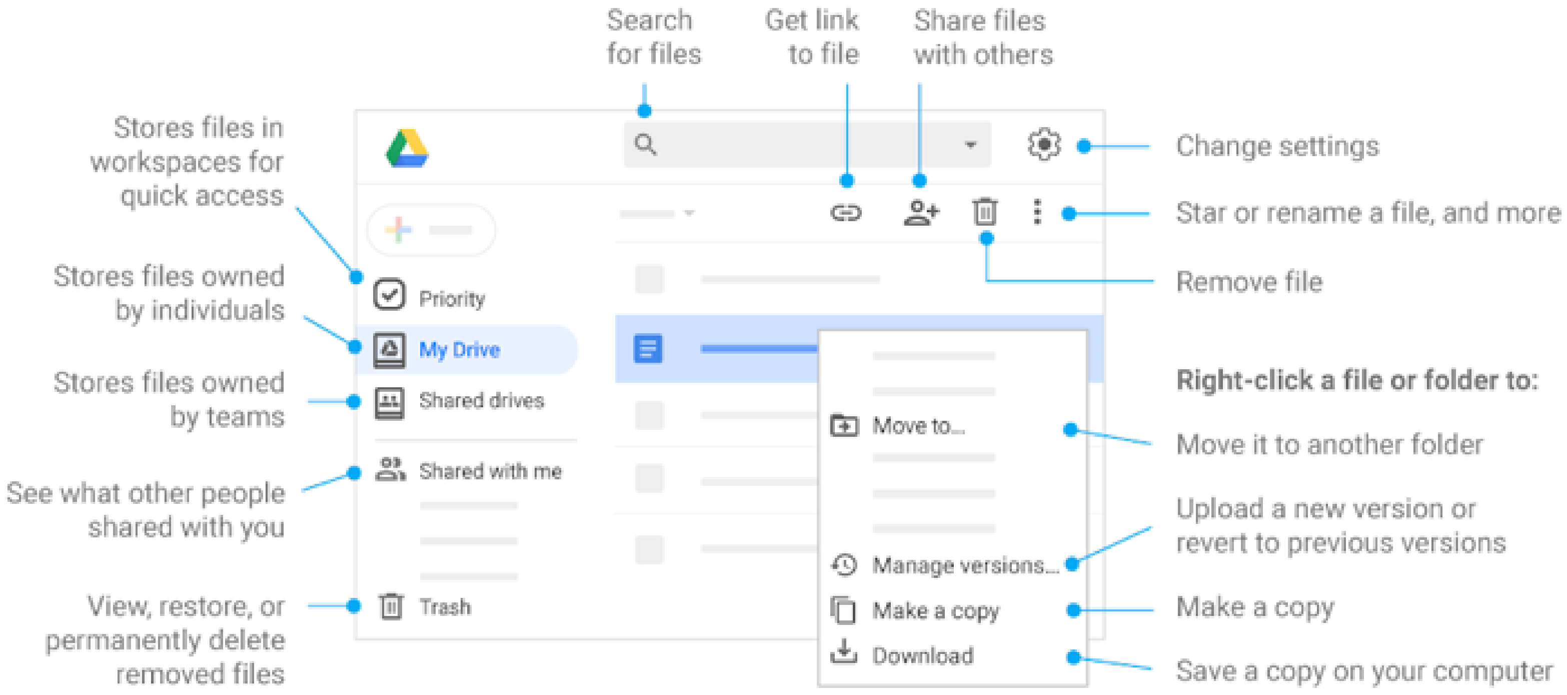
Types of Material you can create



Editor	Description	Example uses
Google Docs	Text documents	Proposals, reports, shared meeting notes
Google Sheets	Spreadsheets	Project plans, budget sheets
Google Slides	Presentations	Pitch decks, training modules, team presentations
Google Forms	Surveys	Customer satisfaction surveys, group polls
Google Drawings	Shapes, charts, and diagrams	Flowcharts, organizational charts, website wireframes, mind maps
Google Sites	Websites	Team sites, project sites, resume sites

Tips to Work from Home Securely

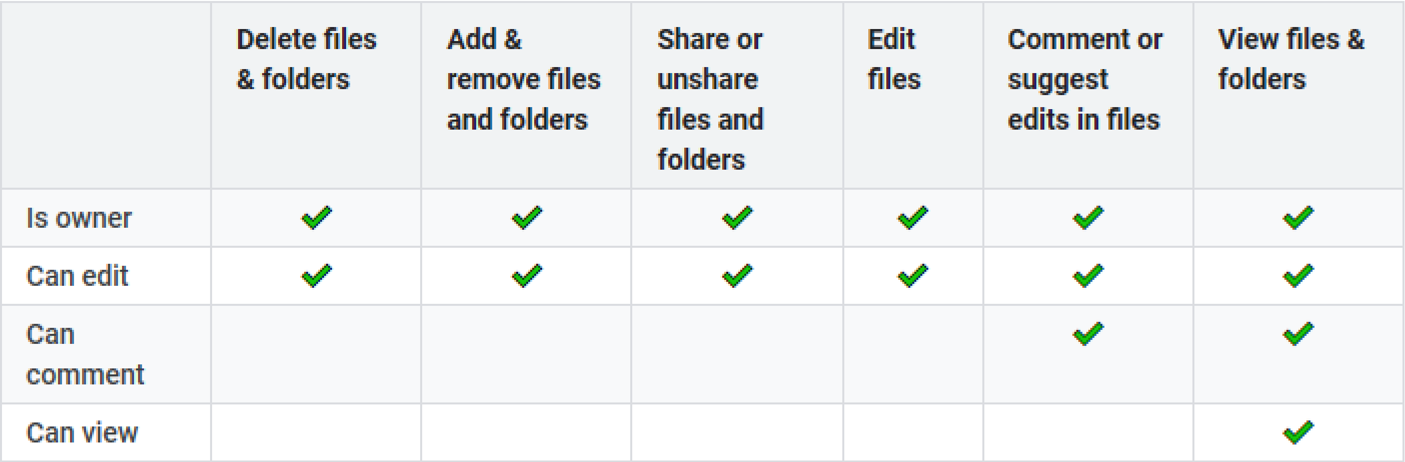
Work with Files stored in Drive



Search for files
Get link to file
Share files with others
Stores files in workspaces for quick access
Change settings
Star or rename a file, and more
Stores files owned by individuals
Remove file
Priority
My Drive
Stores files owned by teams
Shared drives
Right-click a file or folder to:
Move to...
Move it to another folder
See what other people shared with you
Shared with me
Upload a new version or revert to previous versions
Manage versions...
View, restore, or permanently delete removed files
Trash
Make a copy
Make a copy
Download
Save a copy on your computer

Tips to Work from Home Securely

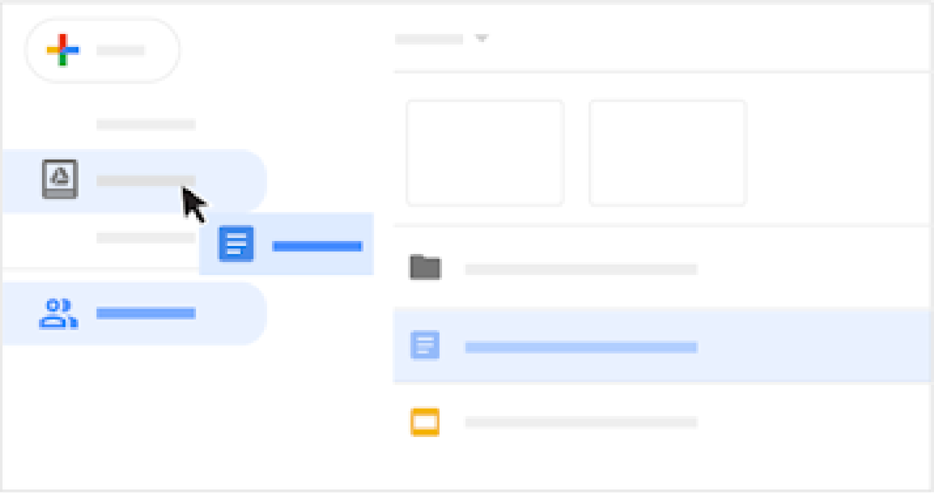
- Share your files and folders by clicking Share 👤+ and then choose what collaborators can do.
- They'll get an email notification, too.



	Delete files & folders	Add & remove files and folders	Share or unshare files and folders	Edit files	Comment or suggest edits in files	View files & folders
Is owner	✓	✓	✓	✓	✓	✓
Can edit	✓	✓	✓	✓	✓	✓
Can comment					✓	✓
Can view						✓

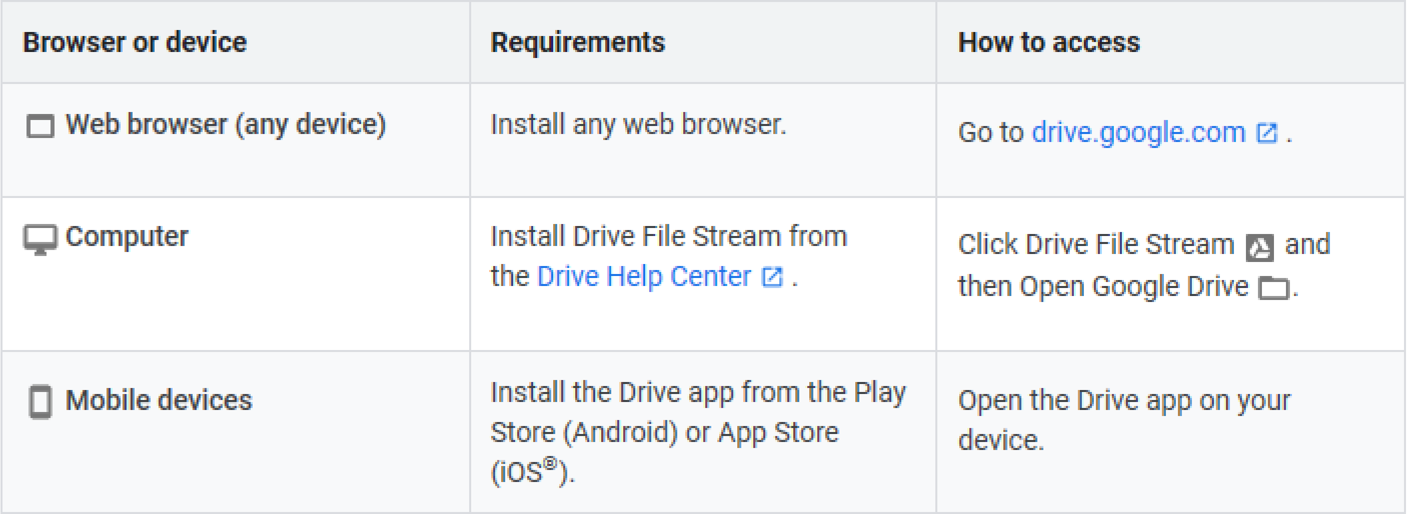
Tips to Work from Home Securely

- Note, when you move a shared file to My Drive, it only moves the file in your view, not anyone else’s



Tips to Work from Home Securely

- Access your files from any device.



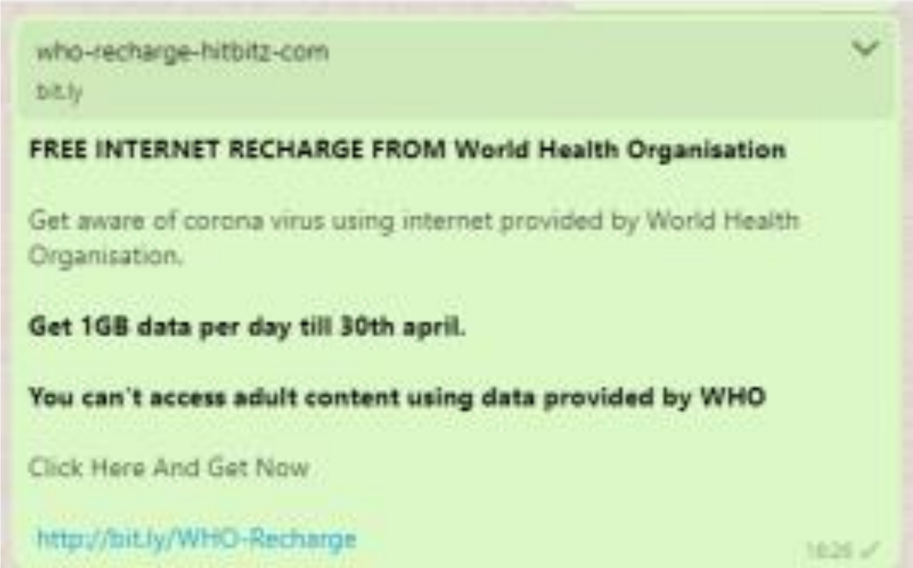
Browser or device	Requirements	How to access
Web browser (any device)	Install any web browser.	Go to drive.google.com .
Computer	Install Drive File Stream from the Drive Help Center .	Click Drive File Stream and then Open Google Drive .
Mobile devices	Install the Drive app from the Play Store (Android) or App Store (iOS®).	Open the Drive app on your device.

Basic Security Hygiene

- Install anti-virus software, and enable its automatic updating e.g. on Windows 10 there is the built in Windows Defender Antivirus.
- The firewall on the computer should be turned on, and the traffic that is allowed should be chosen very carefully – only the applications that are trusted should be allowed to communicate with the Internet.
- Links in emails should be clicked very carefully – some links might take you to infected websites, and it is enough for you to spend a fraction of a second on such a website for a virus to penetrate the computer.

Basic Security Hygiene

- Be careful on clicking links on forwarded messages on various platforms, including on Calendar invites
- Exercise caution in handling any message with COVID-19-related topics, such as email attachments and hyperlinks. Perform due diligence of any social media plea, text, or call related to COVID-19.



who-recharge-hitbitz-com
bit.ly

FREE INTERNET RECHARGE FROM World Health Organisation

Get aware of corona virus using internet provided by World Health Organisation.

Get 1GB data per day till 30th april.

You can't access adult content using data provided by WHO

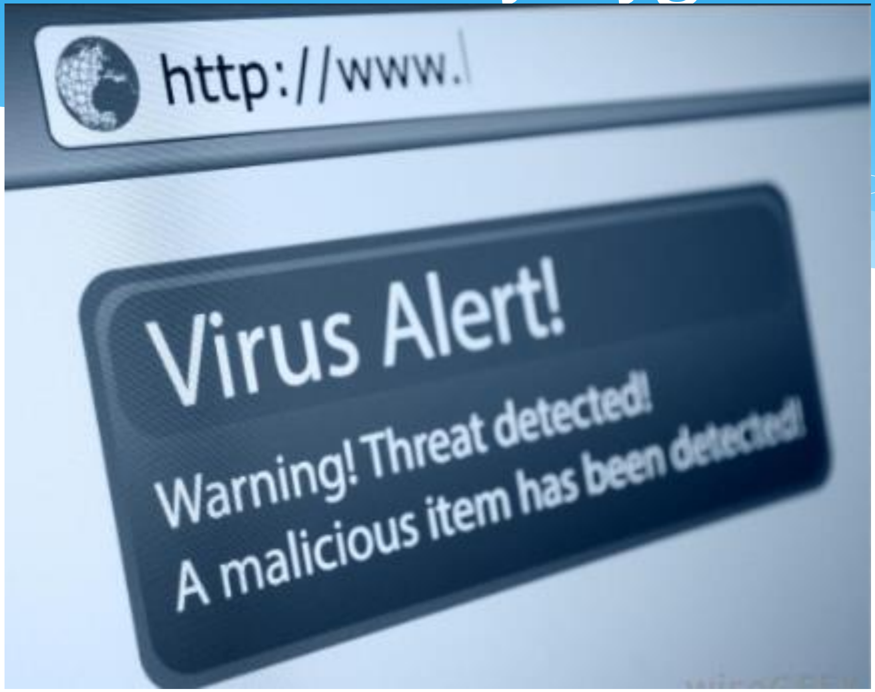
Click Here And Get Now

http://bit.ly/WHO-Recharge

Basic Security Hygiene

- Phishing scams are rife. Be aware of phishing scams targeting remote workers with sensational or emotional messages. Without your colleagues around, you need to be extra vigilant of both email and phone scams.

Basic Security Hygiene



http://www.

Virus Alert!

Warning! Threat detected!

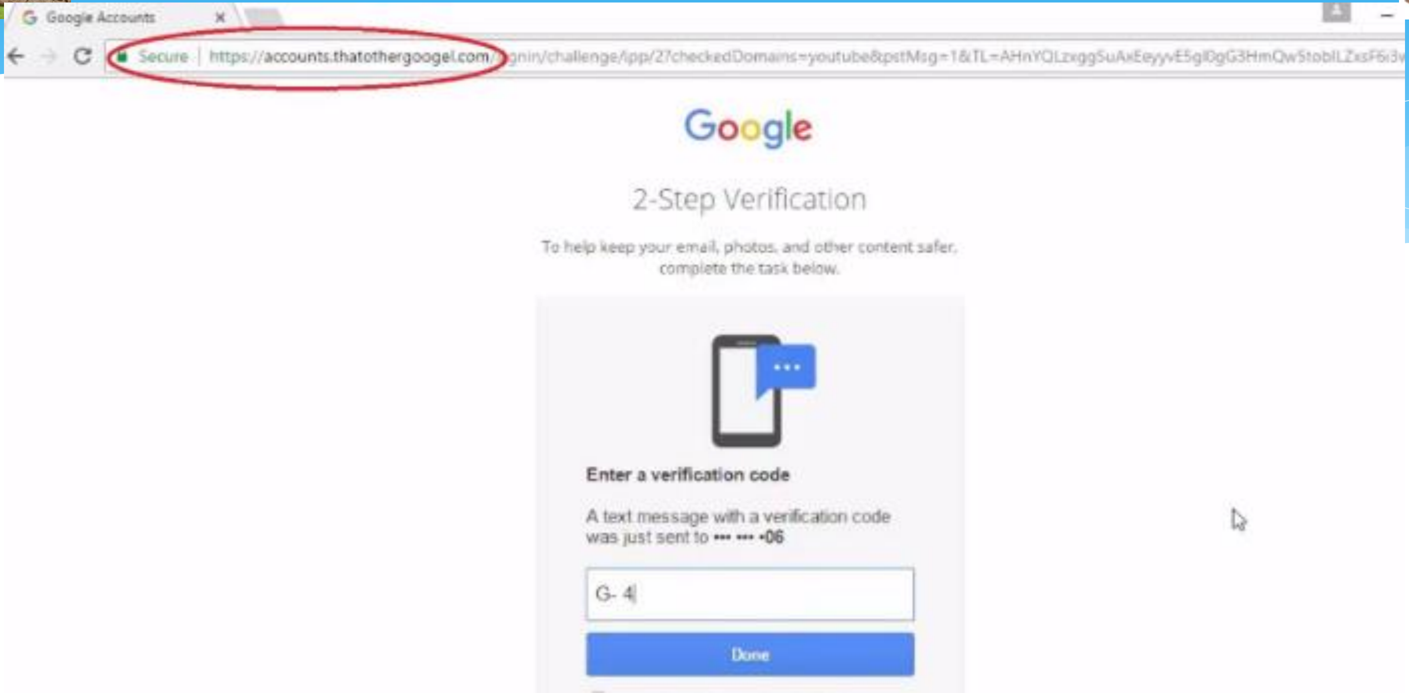
A malicious item has been detected!

- Be extra careful of fake news and malicious websites taking advantage of newsworthy events, Warning threat detected! such as the COVID-19 pandemic.

Basic Security Hygiene

Your passwords are the key to the kingdom. Without the University network to protect you, the power now lies squarely in your hands, or your passwords. Make sure your password for each critical site is strong and unique.

Basic Security Hygiene



Secure | https://accounts.thatothergoogel.com/gnin/challenge/ipp/2?checkedDomains=youtube&pstMsg=1&TL=AHnYQLzxggSuAxEeyyvE5gl0gG3HmQwStobILZxsF6i3v

Google

2-Step Verification

To help keep your email, photos, and other content safer, complete the task below.

Enter a verification code

A text message with a verification code was just sent to ••• ••• •06

G- 4

Don’t fall for “credential phishing” attacks, where scammers trick you to hand over your username and passwords. Best is to not ever click on links asking you to update details. Rather bookmark the sites you frequently visit

Tips to Work from Home Securely

Read the ICT Policy – Available on the Intranet

- It is there to keep you, the University and the corporate data safe. In turn, this allows you to work in the comfort of your home. You are our strongest line of defense, so remember to remain super vigilant

THE END