NIELIT

CYBER SECURITY

Facebook

- Facebook is **a website which allows users, who sign-up for free profiles, to connect with friends, work colleagues or people they don't know, online**. It allows users to share pictures, music, videos, and articles, as well as their own thoughts and opinions with however many people they like.

- Facebook is at the top of the social media game as **its platform caters to a wide variety of people, incorporating many different media aspects, from photos to messenger to text**. It is not as limited as LinkedIn and Twitter, which typically cater to a specific demographic.

Key Features

- Facebook is free to join and free to use.

- It can be used by anyone wherever they are in the world as long as they have internet access.

- Facebook users can share messages, videos links, photographs and websites.

- Facebook users can join groups or follow people/hobbies that interest them

- You can search by name or email to find people.

- Users can choose to allow access or deny it.

- Privacy settings can be set to only communicate with people you have agreed to allow access.

- Facebook is available 24 hours a day so people can communicate without geographical timelines causing a problem

Facebook Users' Privacy Concerns
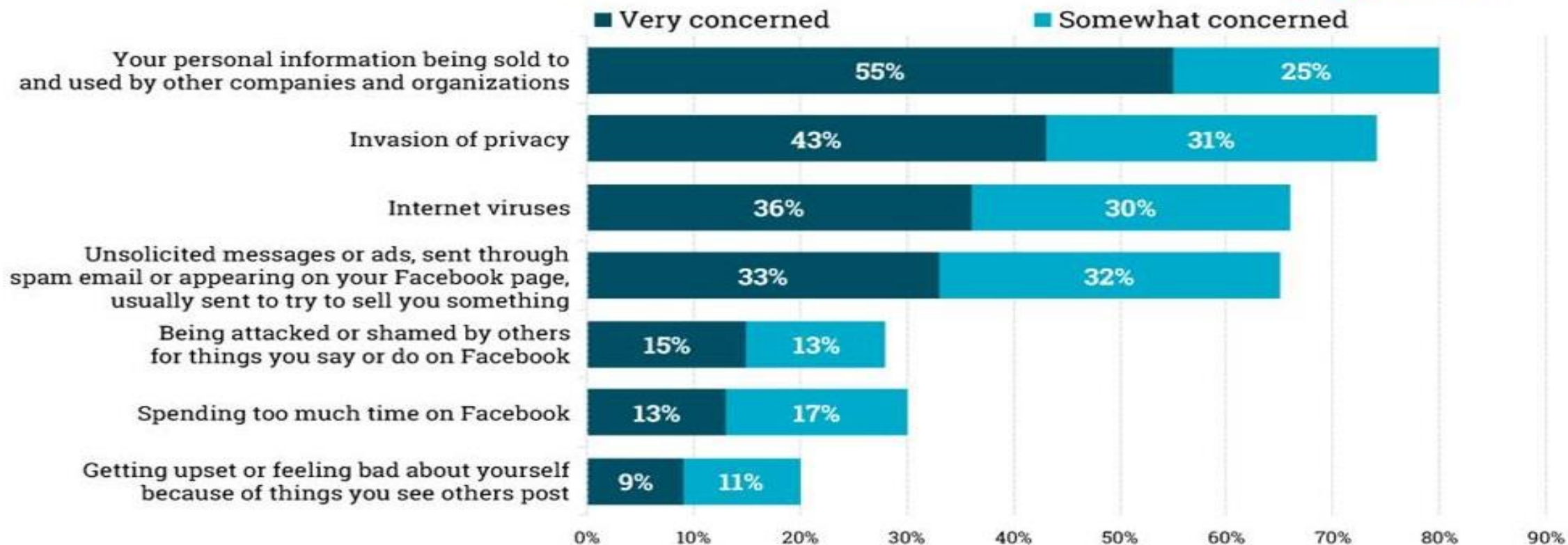
- With billions of users globally, Facebook is obviously doing something right, offering a service that is very much in demand.

- Like other sites on the web, Facebook comes with security and privacy concerns. However, with the volume of information Facebook collects about its users, it pays to be extra diligent with this app.

- Many privacy experts would **recommend deleting the app altogether**, but this is simply not considered an option for many avid users.

- Thankfully, there are steps you can take to make using Facebook more private and secure. Facebook has beefed up its privacy options with areas like **Privacy Checkup** and **Privacy Shortcuts** designed to make it easier for users to navigate. However, with the increase in the number of settings, things can get a little confusing.

- With that in mind, here are 15 tips for protecting yourself and your sensitive information when using Facebook.

Control who can see what's posted on your timeline from

- There may be some special circumstances under which you are happy to share your content far and wide, with people you know and complete strangers. But for the most part, you will want to limit who can check you out on Facebook.

- Facebook has an option that allows you to select exactly who can see your posts. This is available via the **Privacy Checkup** and **Privacy Shortcut** sections, but for the purposes of this post, we'll stick with the regular privacy settings options.

- To limit who can see what you post in the future, start by clicking on the arrow in the top right corner of the toolbar and select **Settings & Privacy** > **Settings** > **Privacy**.

Settings

- ⚙ General
- 🛡 Security and Login
- 📱 Your Facebook Information
- 👤 Privacy
- 👁 Face Recognition
- 🏷 Profile and Tagging
- 🌐 Public Posts
- 👥 Blocking
- 📍 Location
- 🔤 Language and Region

Privacy Settings and Tools

Privacy Shortcuts

Check a few important settings
Quickly review some important settings to make sure you're sharing with the people you want.

Manage your profile
Go to your profile to change your profile info privacy, like who can see your birthday or relationships.

Learn more with Privacy Basics
Get answers to common questions with this interactive guide.

Your Activity

Who can see your future posts?		Friends	Edit
Review all your posts and things you're tagged in			Use Activity Log
Limit the audience for posts you've shared with friends of friends or Public?			Limit Past Posts
Who can see the people, Pages and lists you follow?		Only me	Edit

☐ Under **Your Activity**, the first option is **Who can see your future posts**? Click on **Edit** next to this.

- Now select from:
  - Public (this means everyone).
  - Friends (this is what we would advise).
  - Friends except… (all of your friends except for any you purposefully omit).
  - Specific friends (only those people you choose from your existing list of friends).
  - Only me (your timeline is going to be a bit lonely!)
- Pick whichever option works for you—**Public** should probably be avoided and **Only me** seems a bit pointless—and then that setting will apply for all your future posts.

- Now that you have limited who can see your future posts on Facebook, you may want to add a level of control to determine who can see what has gone before.

- As before, go to **Settings & Privacy** > **Settings** > **Privacy**. Under **Your Activity**, find the entry for **Limit The Audience for Old Posts on Your Timeline** and click on **Limit Past Posts**.

- You'll see a popup explaining the action and you'll need to click on **Limit Past Posts** again to confirm.

Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log

Limit The Audience for Old Posts on Your Timeline   Close

If you choose to limit your past posts, posts on your timeline that you've shared with Friends of friends, and Public posts, will now be shared only with Friends. Anyone tagged in these posts, and their friends, may also still see these posts.

If you want to change who can see a specific post, you can go to that post and choose a different audience. Learn about changing old posts

Limit Past Posts

☐ Do you have something in your **About** section that you don't want to share with the whole world? If so, you need to do something about that…

☐ From your profile page, click on the **Edit profile** button
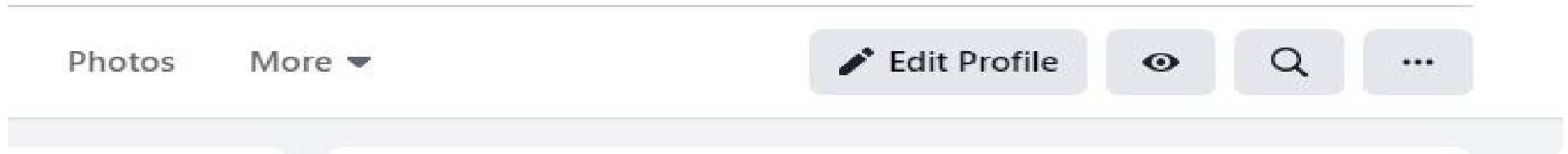
☐ Next to **Customize Your Intro**, select **Edit**. Toggle off any item you don't want to share on your profile.

☐ Better still, you can remove that information entirely. Click the pen icon next to the information you want to delete, then select the three dots icon and select **Delete [Item Name]**.

☐ Voila! Most of your private stuff is now exactly that, though you should be aware that some details, such as your name and cover photo, cannot be given limited visibility under any circumstances.

Limit who can contact you through Facebook

- Limiting who can see your timeline on Facebook will go a long way to protecting your privacy but it won't stop all those bizarre friend requests and other messages you get from people you don't know.

- To ensure random people on Facebook can't get in touch with you, you'll want to change the setting that allows anyone to make contact.

- To do that, go to **Settings & Privacy** > **Settings** > **Privacy** and find the section titled **How People Find and Contact You**. There are several options here, the first one being **Who can send you friend requests?**

- Select **Edit** next to this and a new drop-down menu will appear. You'll want to change that from **Everyone** to **Friends of friends**. Unfortunately, there's no option to completely disable friend requests, although you may want to choose who can see your friends list.

□ While we are not advocates of changing a password regularly for the sake of it, there may come a time when you want to change yours anyway, hopefully because you have come up with a much longer and more complex alternative.

□ To do so, go to the **Security and Login** page. Under **Login**, click on the **Edit** button next to **Change password**.

□ If you're not already using a password manager that auto-populates, you will need to re-enter your existing password, followed by your new one. Re-type the new password and then click on **Save Changes**.

- Until a foolproof biometric alternative comes along, the password is here to stay, and that's not a great option these days. We've previously written tips on creating strong passwords, and argued the merits of password managers, but the truth is, most people still end up using quite weak credentials.

- The best solution to that problem, for now, is two-factor authentication (2FA) and you should enable it on your Facebook account right now.

- To do so, go to the **Security and Login** page and locate the **Two-Factor Authentication** section. Next to **Use two-factor authentication**, click **Edit**.

- Here you will be presented with two methods of 2FA: using a text message or using an authentication app such as Google Authenticator or Duo Mobile.

- Within the **Two-Factor Authentication** section, you can choose to exclude certain devices (for example, your home desktop) from having to use 2FA.

Security and Login > **Two-Factor Authentication**

Help Protect Your Account

If we notice an attempted login from a device or browser we don't recognize, we'll ask for your password and a verification code.

Select a Security Method

Authentication App

Recommended - Use an app like Google Authenticator or Duo Mobile to generate verification codes for more protection.

Use Authentication App

Text Message (SMS)

Use text message (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can't be used to reset your password when two-factor is on.

Use Text Message (SMS)

Block users

- Now that you've locked down your privacy and security, how about blocking troublesome people, messages, and apps?

- To get started, click on the arrow in the top right corner of the toolbar and go to **Settings & Privacy** > **Settings** > **Blocking**.

- If for some reason you want to prevent someone from contacting you or viewing your timeline, you need to block them.

- To do so, find the **Block users** section and simply add their name or email address into the box and click on the **Block** button.

Block users

Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.

Block users | Add name or email | Block

You haven't added anyone to your block list.

- You can also block a user by going to their profile page, selecting the three-dot menu icon, and choosing **Block**.

- Don't want to block someone entirely? Another option is to restrict select users. When you add people to your restricted list, they will only see items you share with everyone or on a mutual friend's timeline.

- They won't see items that you choose to only share with friends.

- This is a good way of limiting what a person can see while avoiding any awkwardness that could arise from removing them from your friend list. The **Restricted list** section can be found in the **Blocking** page.

- If you don't wish to block someone from viewing your timeline, but do want to prevent them from messaging you, then **Block messages** is the appropriate section.

Block messages

If you block messages and video calls from someone here, they won't be able to contact you in the Messenger app either. Unless you block someone's profile, they may be able to post on your Timeline, tag you, and comment on your posts or comments. Learn more.

Block messages from | Type the name of a friend...

- Simply type their name in the box and your mission is complete.

Beware of scams on Facebook

- □ Now that your account is locked down tight, other areas you need to consider on Facebook are the messages you receive and the content you see on others' timelines.

- □ It's worth remembering that malicious actors are always looking for a way to trick their victims. This can often be something benign, such as getting you to like a ridiculous post—celebrity death hoaxes are quite common on Facebook—or replying to a message containing fake news.

- □ Such scenarios often don't pose any real risk but can be incredibly frustrating, saddening, or simply annoying and a good reason to use the blocking settings!

- □ That said, some messages on Facebook pose a real danger.

- □ Much like with your email account, bad actors may sending malware links or phishing messages via Facebook. It's common for hackers to take over Facebook accounts and send such messages to everyone in the victim's friends list.

- □ As ever, if a link looks suspicious, don't click on it and remember that if something looks too good to be true, it probably is.

□ DO's

When you feel uncomfortable with any SM post/mail/chatting, immediately share your concern with your parents or any trustworthy person

Password should be strong with alpha-numeric symbols and special characters

Real life etiquettes and manners apply equally to the virtual space

Always add persons whom you know in real life & with the permission of your parents

Never share your personal details like address, phone number, date of birth etc. on any online platform such as Facebook, Instagram, Blogs, Twitter, chat-rooms etc.

Don't sign up for sites that require a certain age criteria for registration

Do not respond to indecent/offending/ harassing emails/ chats or posts

Don't buy anything online without discussing with your parents

Never share your account passwords with anyone

Don't add people as online friends unless you know them in real life or have met them in person

Do not post indecent/offending/ harassing emails/chats /posts on SM platforms

Never agree to meet an online friend unless and until you do so under your parents/guardian's guidance and supervision

Have an open conversation with your kids about safe browsing and computer use

Make sure that your children understand that they will not get into trouble if they tell you about their problem

Check online activity of your child on Facebook, WhatsApp etc. especially if you notice a sudden change in behaviour

Explain it to your child that all social networking profiles must be set to private

Educate yourself also on social media safety and have open discussions with teens

Keep computer in an open area. Make a rule that doors are always left open when kids are online

If you have found inappropriate content about your child, please contact the nearest PS at the earliest

Tell your children to immediately exit any site that makes them feel uncomfortable or worried

Don't allow your child to have SM accounts if there is an age limit for the same

Do not let young children browse 'Google' or other search engines unnecessarily without supervision

Don't allow your child to use apps like Snapchat that immediately delete the posts

Do not replace physical parental supervision of computer use at home with any safe search engine or any other tool

Be selective about what information you make public. Sensitive information includes real name, date of birth, gender, town, e-mail address, school name, place of work, and personal photos

Periodically review your internet contacts and online activities

On social media accounts keep your privacy settings to the most stringent levels. Only share information about yourself on 'need to know' basis

Be extremely cautious while posting photographs and control who can view them

Block people you don't want to interact with

On WhatsApp and other messaging apps, ensure that 'media auto-download' is deactivated, especially from senders who are not in your contact list

Use strong passwords and use different passwords for different accounts

Contact the nearest PS immediately if you feel your privacy/safety has been compromised online. You can also report your problems online at https://cybercrime.gov.in or https://jofs.jhpolice.gov.in

Never, try to meet a person with whom you've interacted only online without taking somebody else along and such meetings must always be in a public place

Don't share your password with anyone or let anybody else handle your account

Don't trade personal information for "freebies."

Don't accept "friend requests" from people totally unknown to you and from those with whom you don't want to interact with

Don't post personal information such as mobile numbers and personal email ids on social networking sites

Don't share any OTP or other passwords, even with friends

Don't click on unsolicited links sent over Facebook messenger or other messaging services, even if they are sent from your friend's account

Don't accept a friend request only on the basis that the person is a mutual friend of a friend of yours

- Whats App Messenger is a FREE messaging app

- Available in Android, IOS and many other smartphones.

- Whats App uses your phone's Internet connection (4G/3G/2G/EDGE or Wi-Fi, as available)

- Most of us switched from SMS to Whats App to send and receive messages, calls, photos, videos, documents, and Voice Messages.

- End-to-End encryption
  - Whatsapp's end-to-end encryption ensures only you and the person you are communicating with can read what is been sent, and nobody in between, not even Whatsapp.
- Added protection
  - Every message you send has its own unique lock and key
  - Go to Settings-->Account-->Security.

Security

Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them.

Learn more about WhatsApp security.

Show security notifications

Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting.
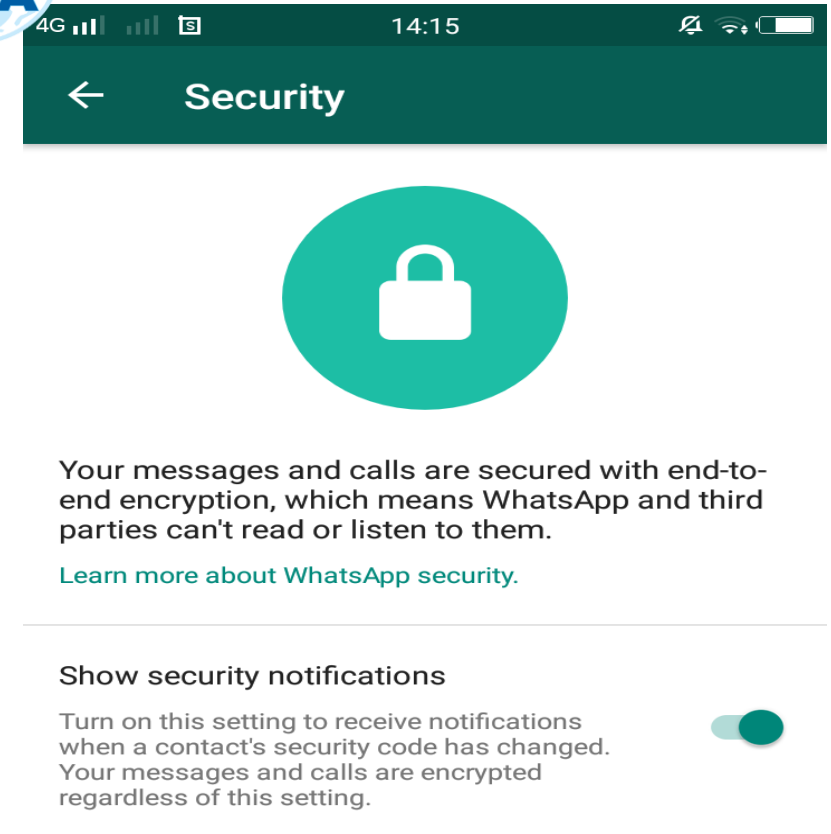
- Few security threats you need to know about.

  - Web Malware

  - Unencrypted Backups

  - Data Sharing between Facebook and Whatsapp

  - Crash Notifications

  - Snooping on other Whatsapp User messages

- Malicious cybercriminals are looking to exploit the popular messaging app.

- With the launch of a web interface and desktop application hackers were quick to pounce with fake WhatsApp websites and applications that stole data and distributed malware

Few tricks used by hackers

□ Hackers masqueraded WhatsApp Desktop applications.

□ Created websites pretending to offer access to WhatsApp Web.

□ Tip: Although WhatsApp does offer a client for both windows and mac, the safest option is to go directly to the source at **https://web.whatsapp.com/**
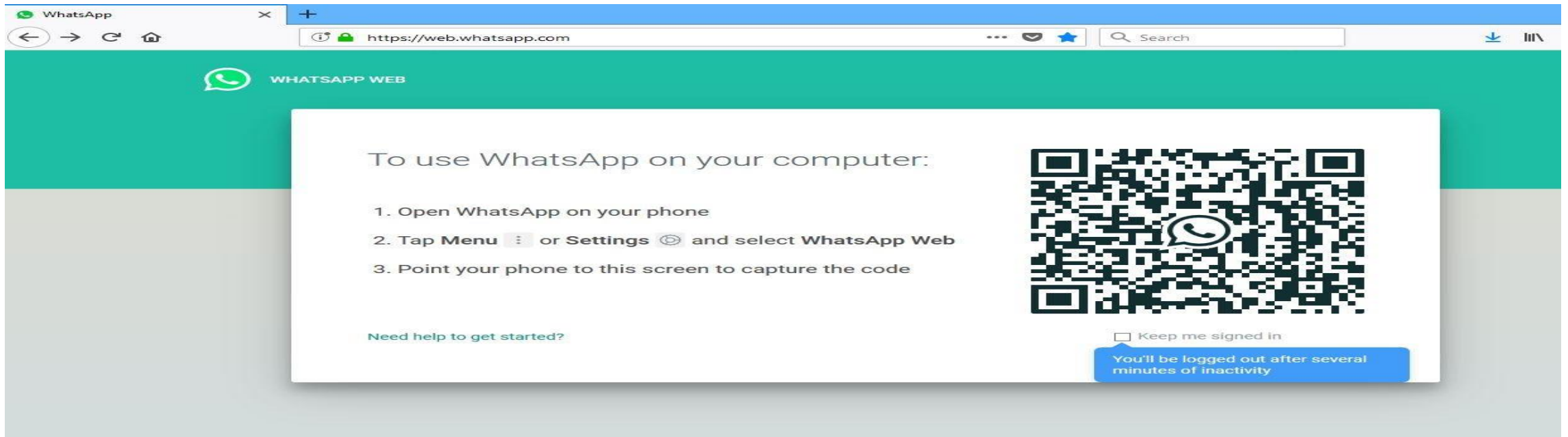
- The backups that WhatsApp create contain the encrypted messages on your device.

- The backup itself is not encrypted

- Vulnerable as there is no ability to change your backup location

- No end-to-end security in the case of an backup and legal agencies can access with a warrant.

- **Tip: It is always better to avoid abusing, bullying through Whatsapp messages and do not forward hoax calls and other threat messages.**
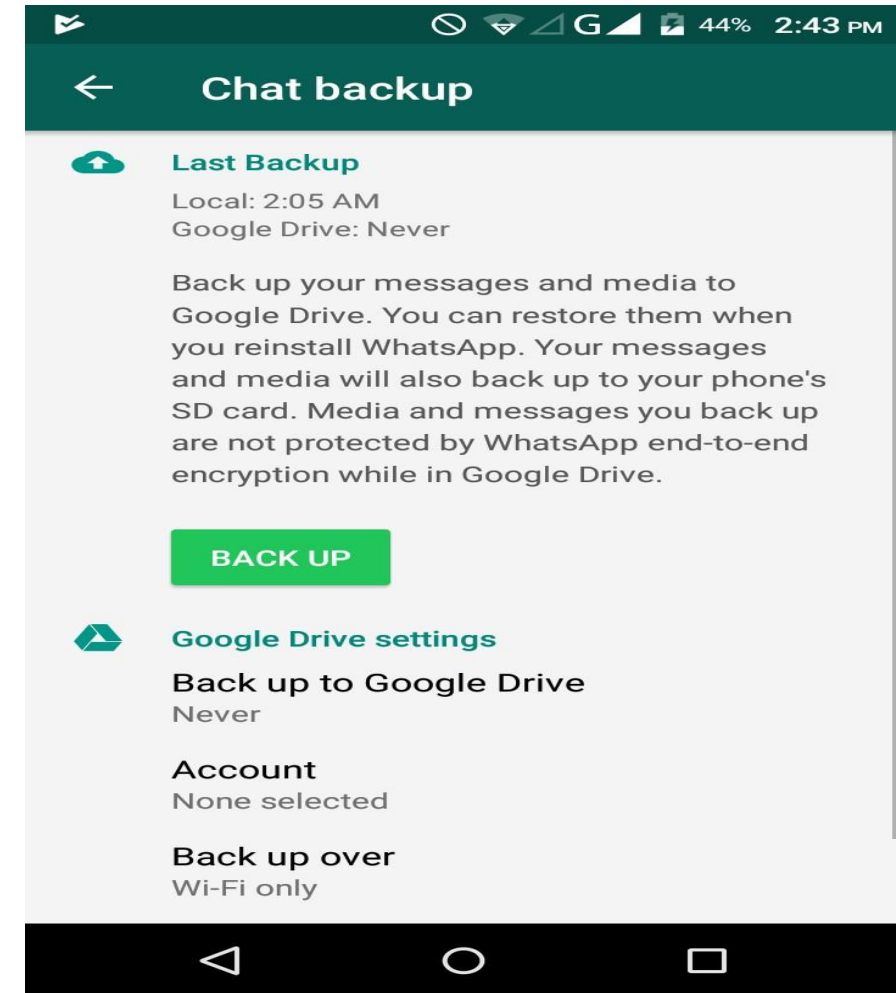
- WhatsApp users discovered that they could crash the target's WhatsApp messenger installed on the cell phone.

- For this, send a message that is more than 7MB.

- When target person tries to open the thread whatapp will crash.

- The target can regain control by deleting the thread.

- Malicious people achieve the same thing by sending a message that is lesser than 2KB and it must contain special characters.

WhatsApp isn't responding

X   Close app

⏱   Wait

❗   Send feedback
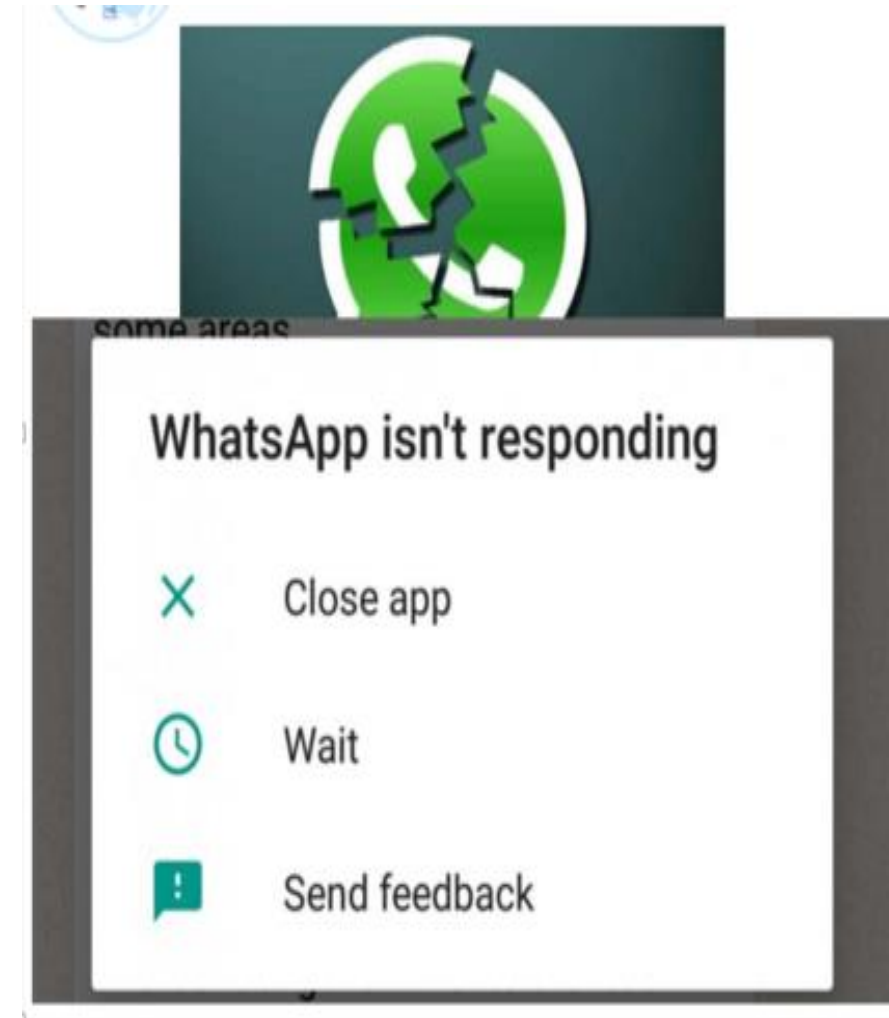
5. Snooping on other Whatsapp User messages

- Xnspy, is a monitoring software, which allows users to access target's WhatsApp messenger to all chats, photos and videos exchanged, and call logs.

- Tip: The best way to prevent a stranger accessing your WhatsApp is by making sure you never leave your phone lying around, or with someone whom you do not trust.

- It is better to install a tracking software or get a your phone's Mac address.

- Always be courteous in replying after reading messages.

- Show patience for receiving photos after the party/vacation.

- Avoid making fuss over others online behavior.

- Make Appropriate Use of Emoji's.

- Be clear in both words and approach.

- Avoid spreading fake news.

- Avoid getting into multiple topics at one go

- Do not argue over silly matters

- Never begin a topic that would

- hurt religious or cultural sentiments.

- Don't spam with unnecessary chains and forward messages

- Control what you see and with whom you interact

- Control what you share

Tools

☐ On WhatsApp, there are some basic controls that you can adjust as you see fit to help you protect yourself:

1. Control who sees your information

□ You can set your last seen, profile photo and/or status to the following options:

□ Everyone: Your last seen, profile photo and/or status will be available to all WhatsApp users.

□ My Contacts: Your last seen, profile photo and/or status will be available to your contacts from your address book only.

□ Nobody: Your last seen, profile photo and/or status will not be available to anyone.

□ Read Receipts are always sent for group chats, even if you turn off the option in your privacy settings.
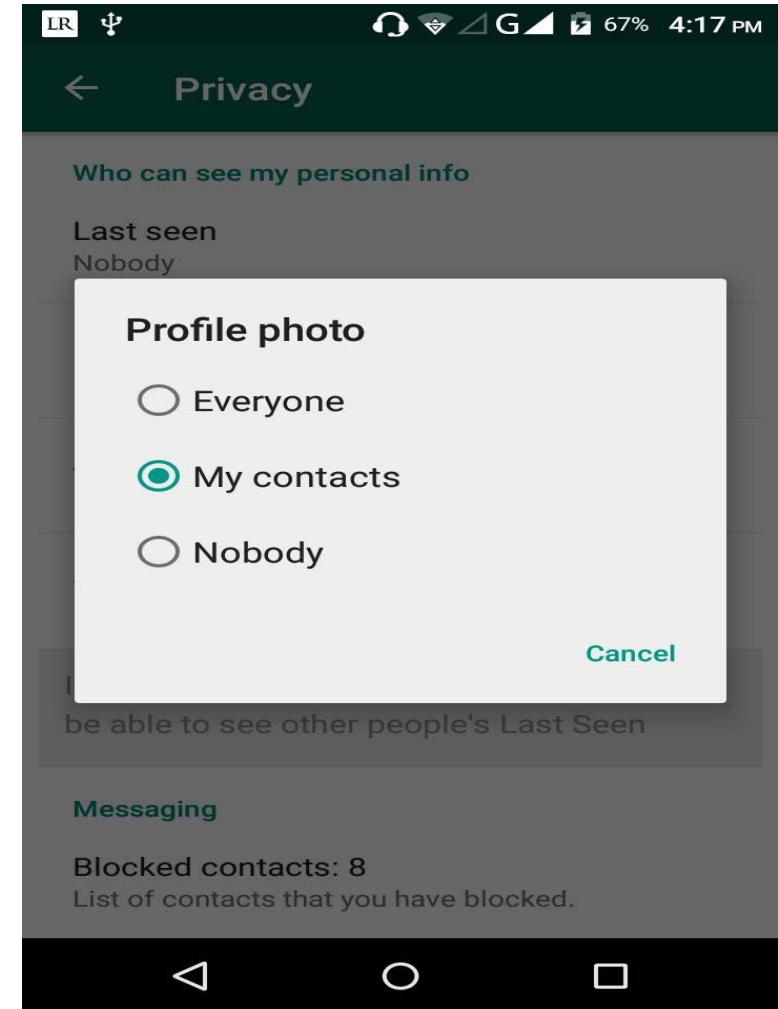
- By default, WhatsApp sets your privacy settings to allow:

- Any WhatsApp user to see your read reciepts, last seen, about and profile photo.

- Your contacts to see your status updates.

- To change these settings, simply go to WhatsApp > Menu Button > Settings > Account > Privacy.
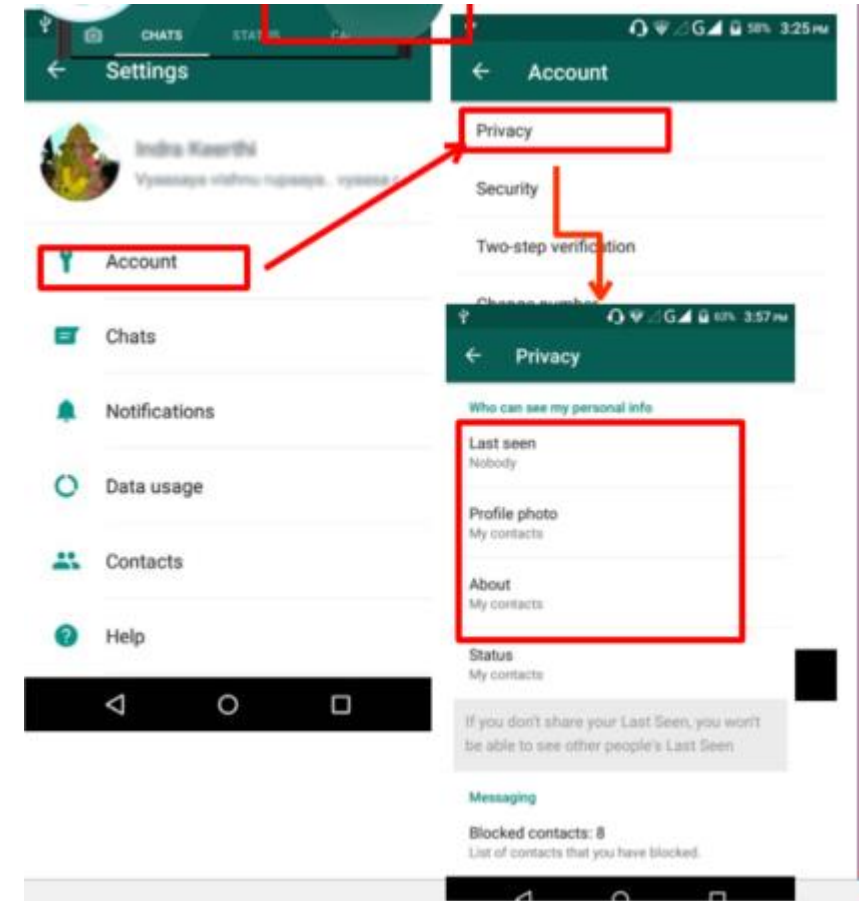
□ By default, WhatsApp sets your privacy settings to allow:

□ Any WhatsApp user to see your read reciepts, last seen, about and profile photo.

□ Your contacts to see your status updates.

□ To change these settings, simply go to WhatsApp > Settings > Account > Privacy.
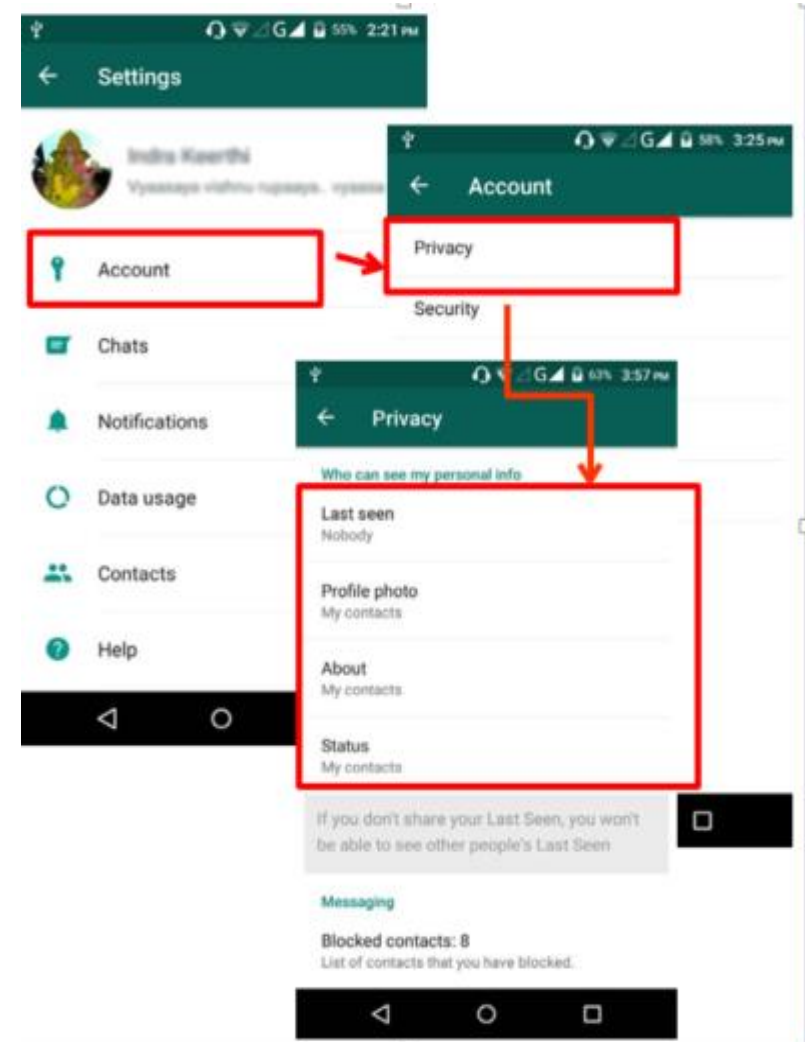
□ If you do not share your last seen, you won't be able to see other people's last seen.

□ There is no way to hide when you are

□ online or typing.

□ If you turn off read receipts, you won't be able to see read receipts from other people. Read receipts are always sent for group chats.

□ If a contact has disabled read receipts, you will not be able to see that they have viewed your status update.

Go to the Status screen.

☐ Tap the Menu Button > Status privacy.

☐ Choose who can see your status updates.

☐ Note: Changes to your privacy   settings won't affect status updates that you have already sent.

□ Your status updates cannot be seen by people whose numbers are not saved in your phone's address book.

□ You can choose to share your status updates with all of your contacts, or with selected contacts only.

□ By default, your status updates are set to be shared with all your contacts.
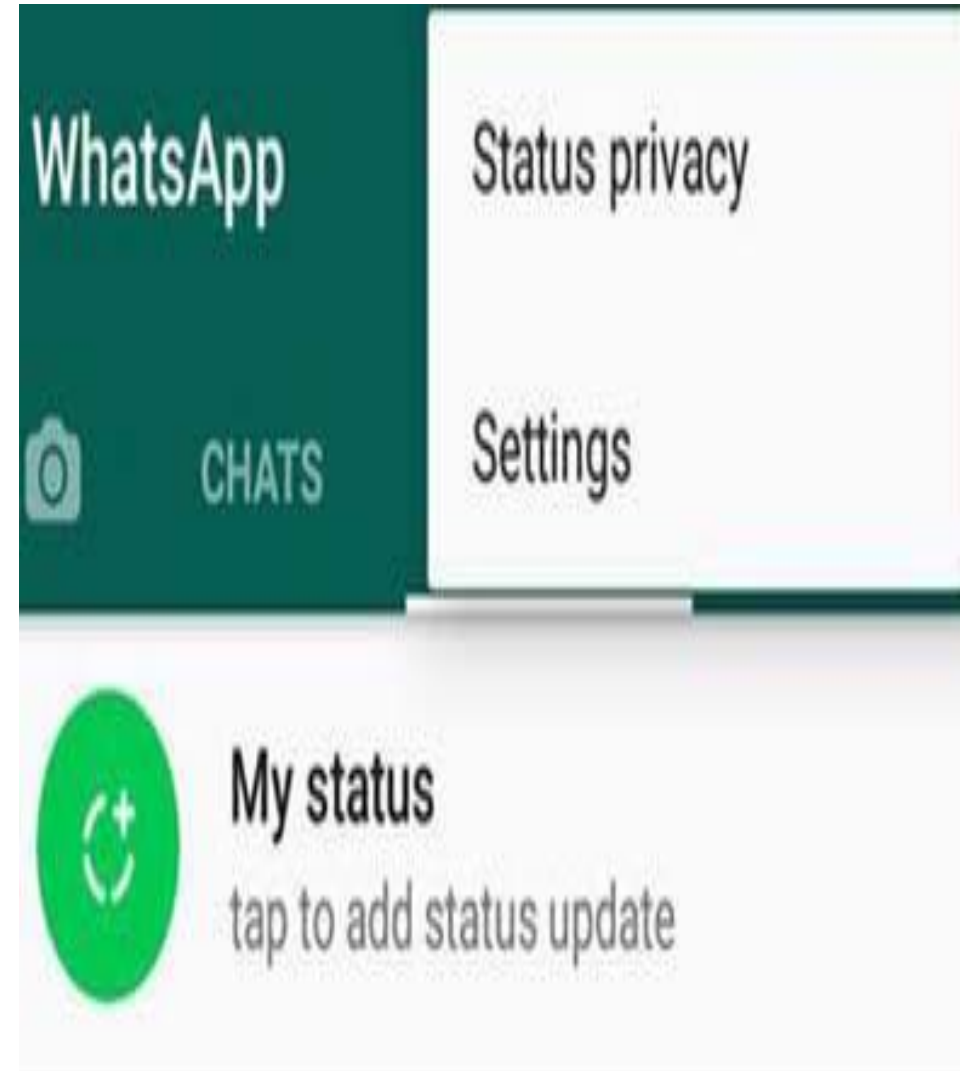
To change your status privacy:

- Go to the Status screen.

- Tap Privacy on the top left of your screen. Choose who can see your status updates.
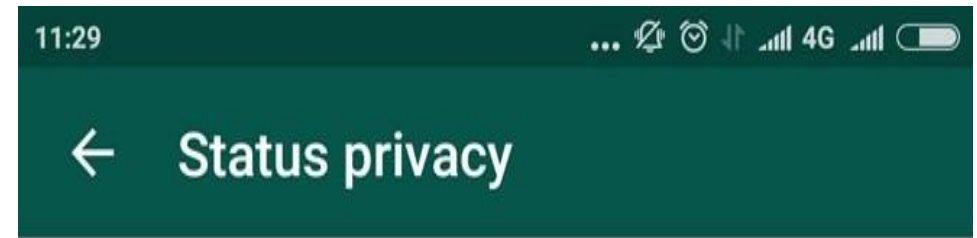
- Note: Changes to your privacy settings won't affect status updates that you have already sent.

- Go to the Status screen.

- Tap the three dots next to My Status.

- Select the status updates you wish to forward, then tap Forward.

- Choose from Frequently Contacted, Recent Chats or use the Search bar to look for a contact or group, then tap Forward.
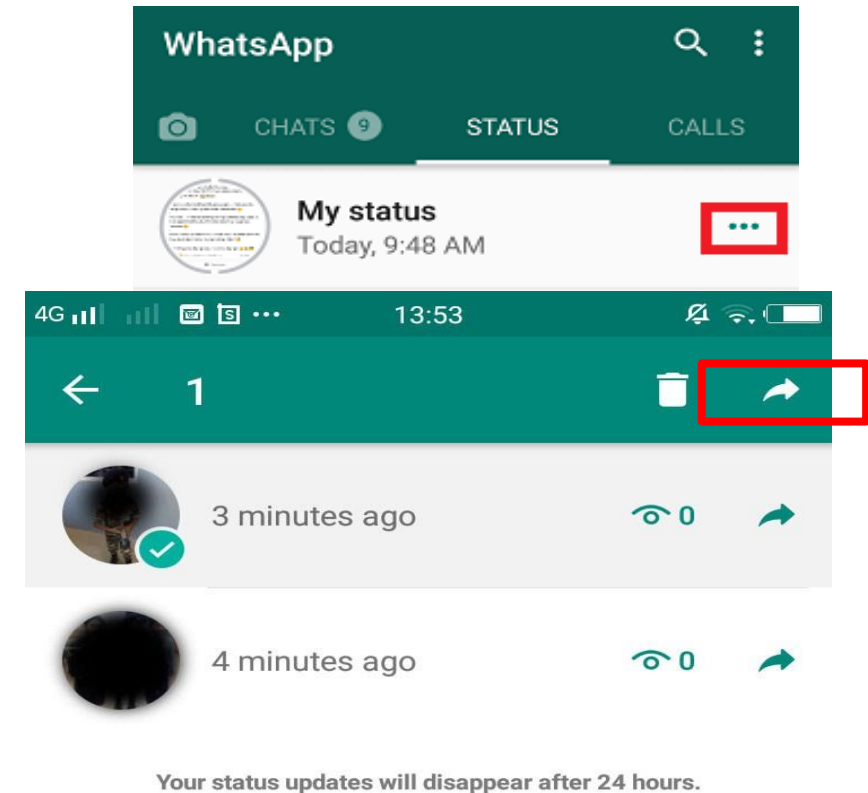
- Status updates automatically disappear after 24 hours. You can also manually delete your status update, which removes it from your contacts' phones.

- To manually delete your status update:

- Go to the Status screen.

- Tap the three dots next to My Status.

- Long press on the status update you wish to delete.

- Tap Delete.

- You can mute the status updates of a particular contact so they won't appear at the top of the status list anymore
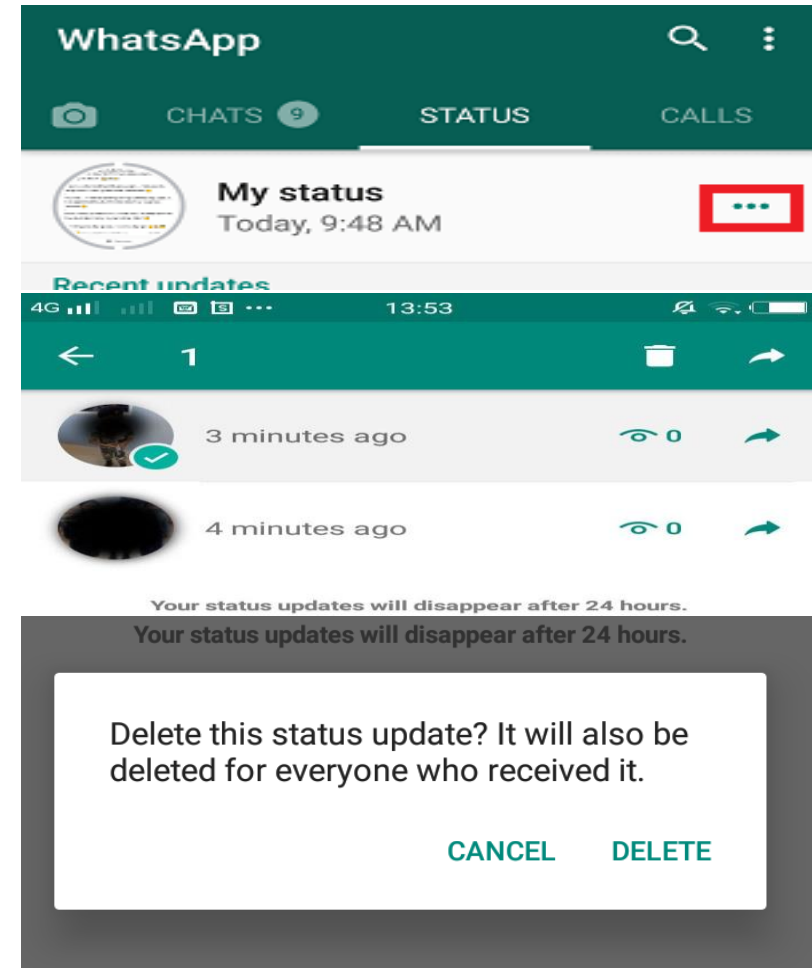
- **Muting a status update**

- You can mute the status updates of a particular contact so they won't appear at the top of the status list anymore.

- **To mute a status update:**

- Go to the Status screen.

- Long Press on your contact's status update you wish to mute.

- Tap Mute.
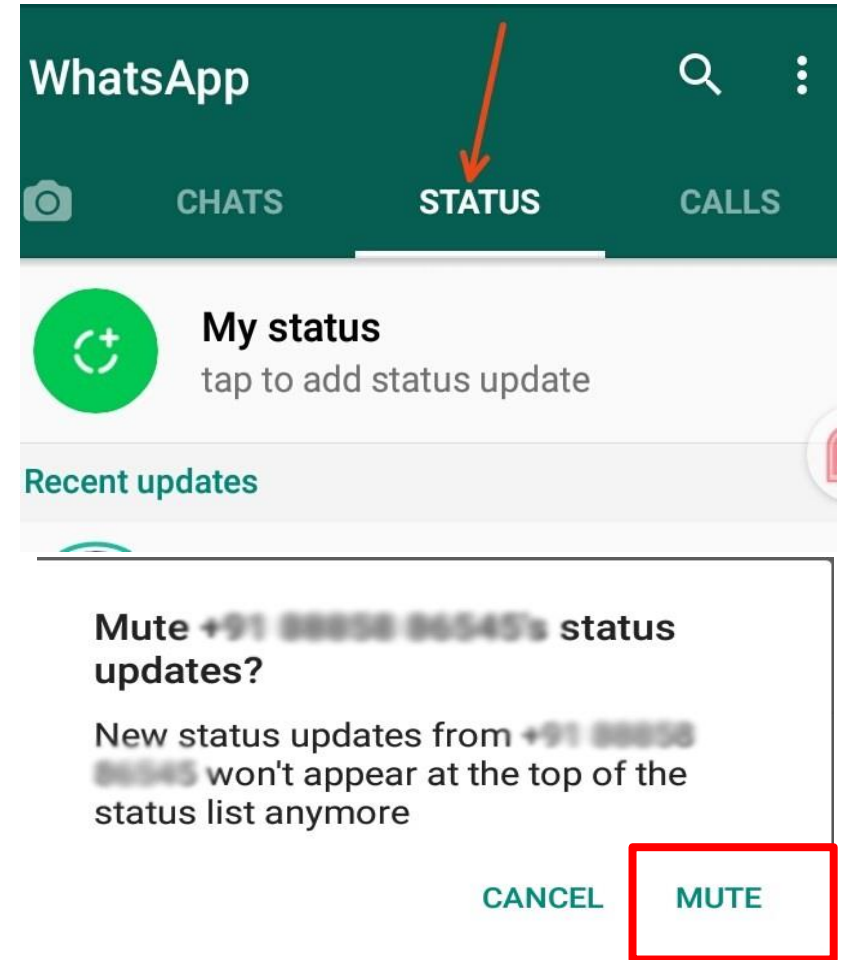
To unmute a status update:

- Go to the Status screen.
- Scroll down to see the Muted
- statuses.
- Long press the contact you wish to unmute
- Tap Unmute.
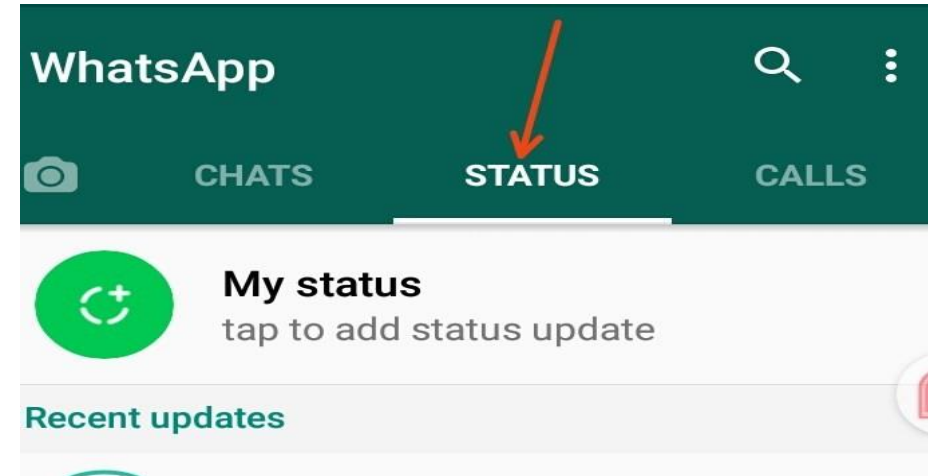
☐ Open WhatsApp.

☐ Open the Application Menu (Swipe down from the top of the screen).

☐ Tap Settings > Privacy Settings > Blocked Contacts. This page displays all contacts that you have blocked.

☐ Tap Add Contact icon at top right of the screen to select a contact to block.
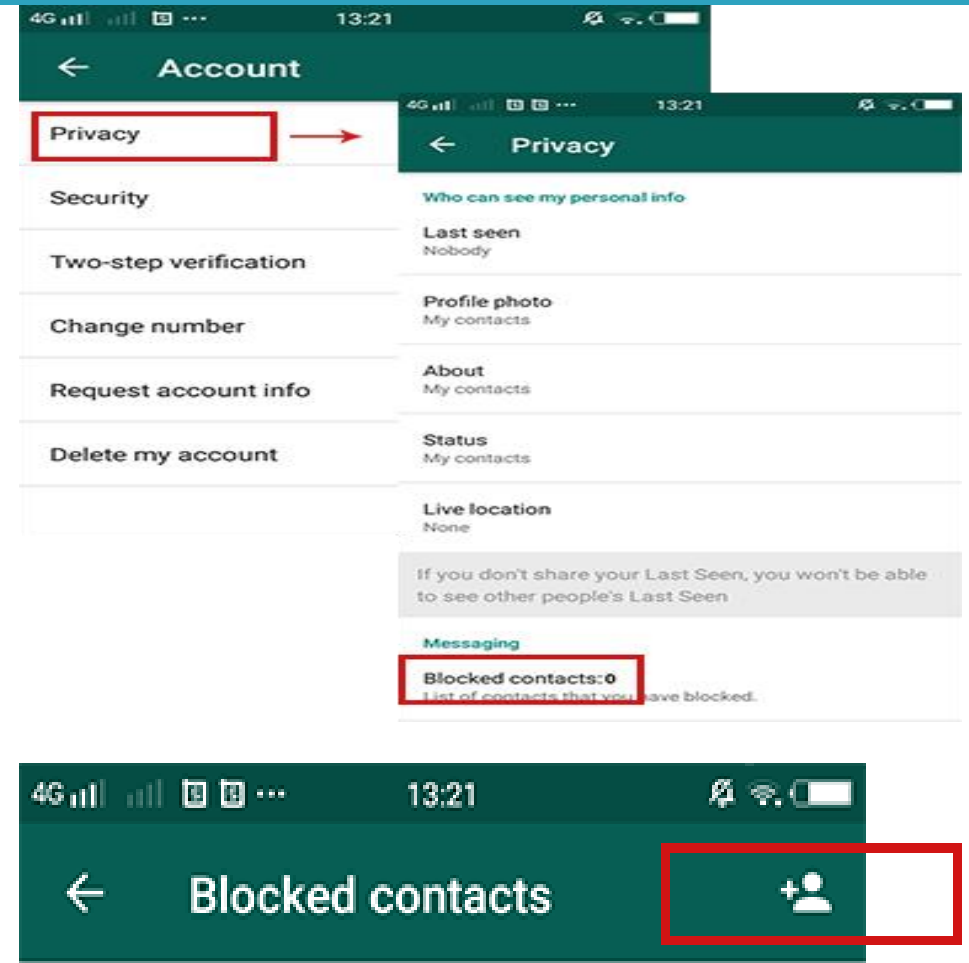
- Instagram is a social networking app made for sharing photos and videos from a smartphone/device.

- Similar to Facebook or Twitter, everyone who creates an Instagram account has a profile and a news feed.

- Other users who follow you will see your posts in their own feed.

- The name "Instagram" is a portmanteau of "instant camera" and "telegram".

Quick Facts

- When you post a photo or video on Instagram, it will be displayed on your profile.

- Instagram is a great networking tool, but can be exploited to access private photos, geo-locate, delete photos, edit comments and post new photos.

- An Instagram account can be directly linked to a Facebook account. Using hashtags on Instagram posts will enhance a user's engagement.

- A hashtag improves user's chances of having their photo seen by other users who do not directly follow them.

History of Instagram

- Instagram was founded in 2010 by Stanford graduates Kevin Systorm and Mike Krieger. Initially, Systorm and Kreiger created an HTML5 check-in project called Burbn which was then redeveloped to cater only photo-sharing uploads.

- On October 6, 2010, Instagram was added to the Apple App Store, generating 10,000 registered users within the first few hours of it's app life.

- In April 2012, Instagram was added to Android phones and was downloaded more than one million times in less than one day.

- In late 2012, Instagram was purchased by Facebook for $1 billion.

Demographics

- Instagram currently has about 150 million monthly active users, 75 million daily users and about 25% of global internet users use Twitter.

- Users are divided equally with 50% iPhone users and 50% Android.

- 90% of users are under the age of 35.

- Education demographics: Users with some college education are the most active on Instagram with 23% and college graduates have the second highest activity at 18%. Users with a high school diploma or less make up another 15%.

- 24% of all users use the app several (3+) times a day

Main functions

- Users can upload photographs and short videos.

- Videos are a maximum of 15 seconds long.

- Photos can have filters added to them as well as in-app editing and a 'Lux' effect.

- Frames can also be added to each photo.

- Instagram Direct allows users to send photos only to specific users instead of publicly.

- There are five tabs on Instagram:
  - Home,
  - Explore,
  - Upload,
  - News
  - and
  - Profile.

- The Explore tab has a scrolling list of photos curated by Instagram for you (based on accounts/photos you have already liked and followed) as well as a search bar to find specific usernames and hashtags.

- Profiles are provided for users similar to other social media sites. These contain biographical information, recently shared photographs and a user photo.

- The Yorkshire and Humber Regional Cyber Crime Unit (RCCU) protect team have produced this documentation regarding public Instagram safety.

- This document demonstrates the options available to users.

- There are step-by-step instructions on how to view and change your preferences throughout your account settings.

- The options you choose are personal preference.

- This document contains recommendations for your settings and shows you how to access them.

- Sign in to your Instagram account here.

- Upon logging into Instagram, in the top right corner,

- Please select the following:
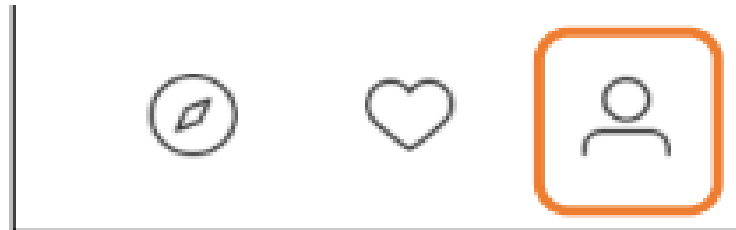
- You will be directed to your Profile. Please click the settings button shown in the orange outline:

- The following drop-down menu will be displayed after clicking the settings button:

- Using these options, we will navigate through the various security settings available for you to editing.
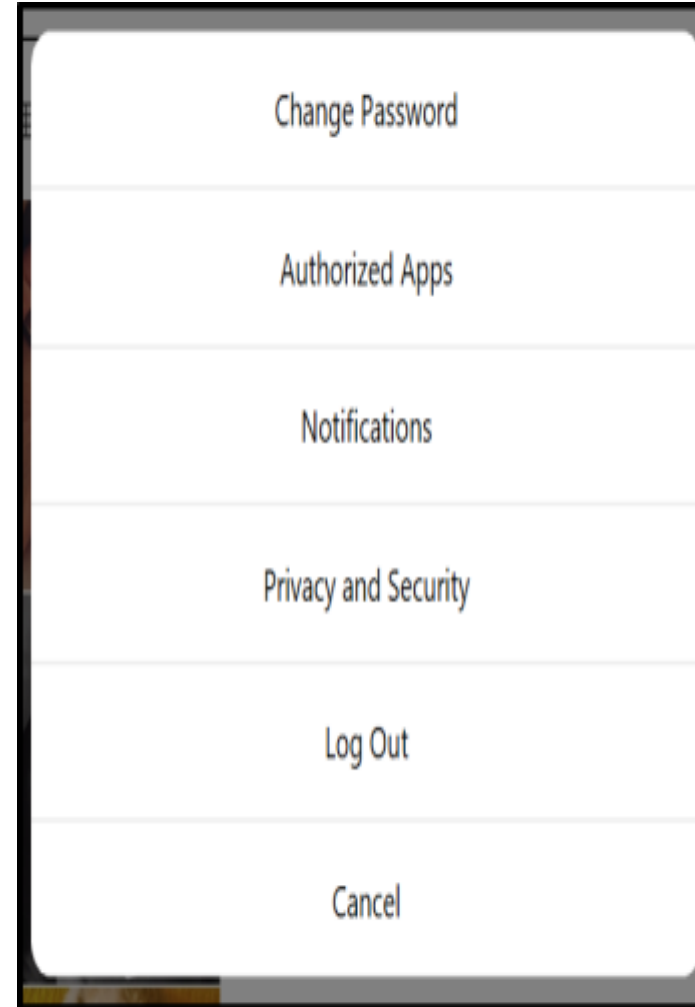
Change Password:

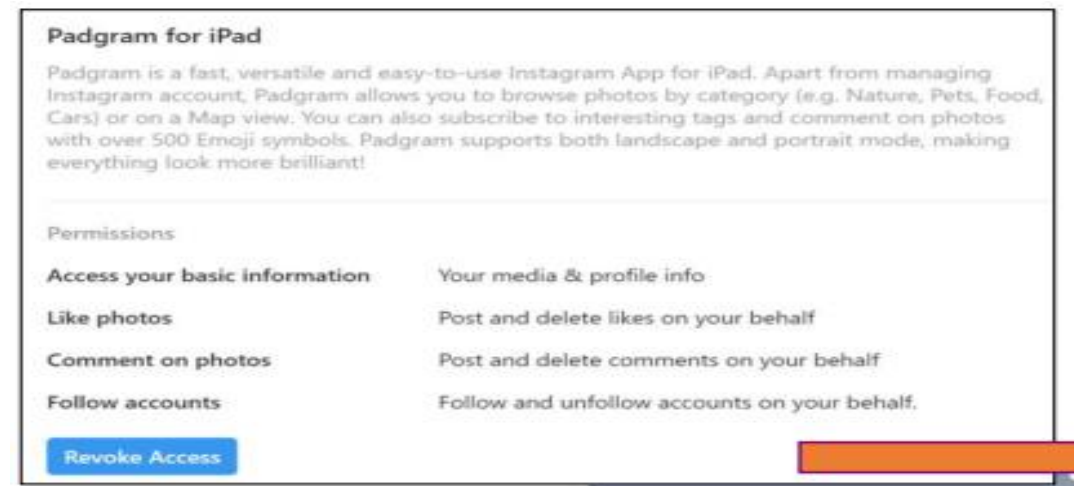- Choose the following option in the drop-down settings menu:

Change Password

- This section can be edited by you! Below we have covered the 'Change Password' option and our suggestions for you and your cyber safety.

- The following menu will be displayed at the left side of the page and will be used to navigate through the settings mentioned in this document.

- The 'Change Password' option is highlighted in black because it is the page which is currently displayed to you.

Edit Profile

Change Password

Authorized Applications

Email and SMS

Manage Contacts

Privacy and Security

- Here are the input fields available to change your password.

- You are required to know your old password to create a new one.

- The page will refresh with empty input boxes and a small box will pop-up at the bottom of the screen saying, 'Password has changed'.

Password Guidance!

The password guidance suggested by the **NCSC** is:

THREE RANDOM WORDS

Use unrelated words which are not in relation to you, your hobbies and your life.

Old Password   •••••••••••••••••••••

New Password   •••••••••••••••••••

Confirm New Password   •••••••••••••••••••••

Change Password

Authorized Applications:

□ Choose the following option in the drop-down settings menu:

□ This section can be edited by you! Below we have covered the 'Authorized Applications' option and our suggestions for you and your cyber safety.

□ You can remove any applications you do not want to provide permissions. For example, it will not allow an unauthorized application to make any changes such as posting or deleting likes and comments

□ Click 'Revoke Access' and another box will appear to double enforce your option. Click 'Yes' or 'No' to revoke an application's access.

Email and SMS:
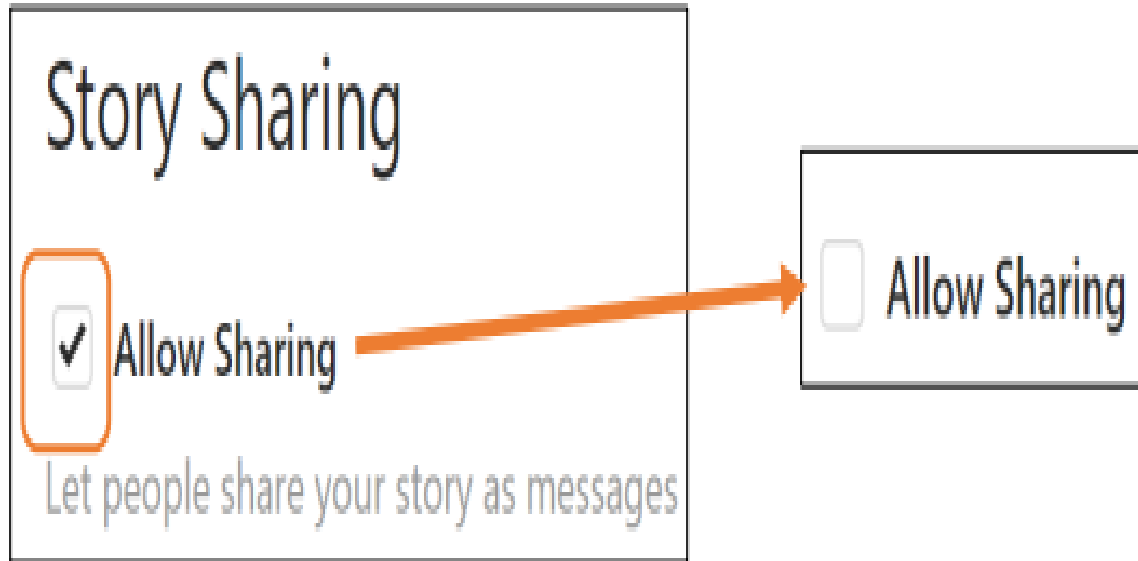
- Choose the following option in the drop-down settings menu:

- This section can be edited by you! Below we have covered the 'Email and SMS' option and our suggestions for you and your cyber safety.

- You can choose the options you are subscribed to:

- For example, if you no longer wish to receive 'News emails' then untick the box

- Choose the following option in the drop-down settings menu:

Privacy and Security

- This section can be edited by you! Below we have covered the 'Privacy and Security' option and our suggestions for you and your cyber safety.

- You must decide whether you want your account private or public. We advise that you have your account on private.

- This allows you to choose who can see your account because they send a request which you can accept or decline.

☑ Private Account

Account Privacy

☐ Private Account

When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected.

- You must tick the box to activate your private account. The setting will be automatically saved. You will have to accept any friends which now send you a reque

- You may wish to allow people to share a 'Story', to their friends, that you have created.

- This means your story could be potentially shared between multiple or many people.

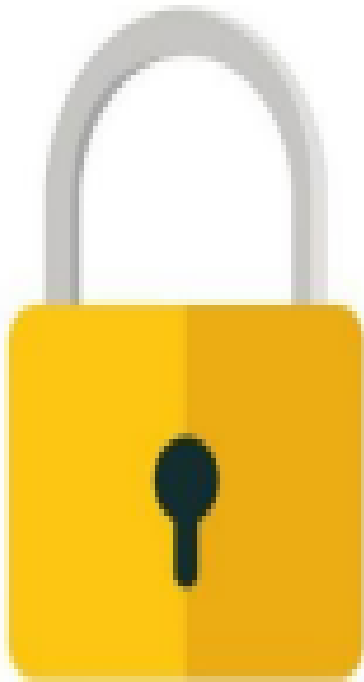Your account data stored by Instagram can be viewed by you!

- Enabling Two-Factor Authentication adds a second layer of security when you log into an account.
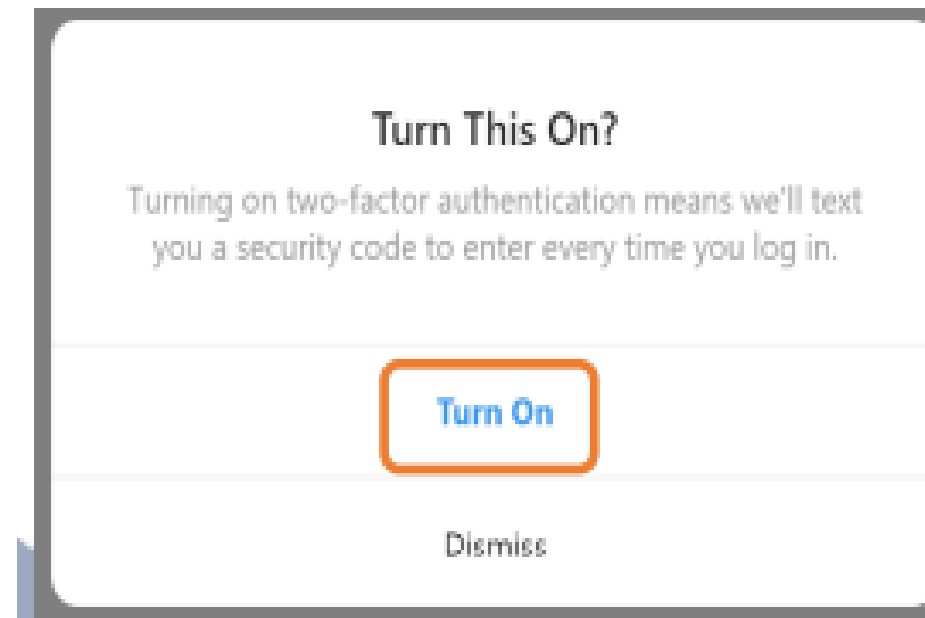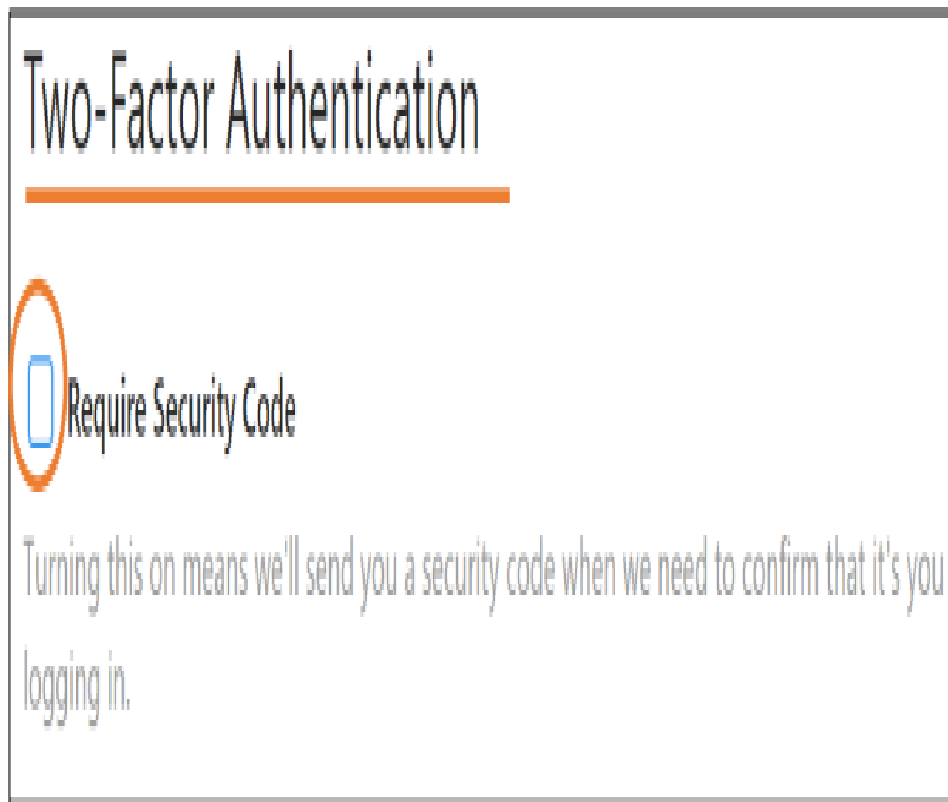- Click 'Enable Two-Factor Authentication' for more options.

Two-Factor Authentication

Enable Two-Factor Authentication

☐ You need to tick the Require Security Code box.

☐ This box will then appear on the screen. Click 'Turn on':

□ Now enter the confirmation code which will have be sent to your mobile number which you will add to your Instagram account.

Confirmation

Enter the confirmation code we sent to 07.   If you didn't get it, we can resend the code

.

Confirmation
Code   *****|

Didn't enter the right phone number? Change it

Done

Prevention

- Don't post information, photos or videos you wouldn't want made public.

- Always use strong and unique passwords. Enable personal verification as a tool if you forget your password.

- Do not allow access to 3rd party apps that may collect your information.

- Keep backups of your posts if they are important to you or your business.

- Unfollow or block those that threaten your wellbeing.

- Disable geolocation on posts, tailored ads and others ability to tag you in photos.

- Use a "link checker" service to ensure all links are safe before clicking! Use private accounts so that only those who you permit can see your content.

Detection & Response

- Your account is leaving comments or sharing things that you haven't posted.

- Without acting, your account starts to follow people you don't know and also like their images.

- There are images on your account which you KNOW aren't yours.

- You don't have access to your account anymore and you are 100% sure that you're using the right password and it's not a technical glitch.

- If your registered Instagram account email was changed, there should be an email from Instagram confirming that you've changed your email.

- If you don't get this email reset your password then report your account as being compromised to Instagram.

- Inform Instagram immediately if your account has been compromised by going to their Help Centre (see https://help.instagram.com)

Security Tips

- Pick a strong password.

- Make sure your email account is secure.

- Change the passwords for all of your email accounts and make sure that no two are the same. Logout of Instagram when you use a computer or phone you share with other people.

- Don't check the "Remember Me" box when logging in from a public computer.

- Think before you authorize any third-party app.

- Update your accounts as per new security tips and guidelines of Instagram.

Thank You ! ! !