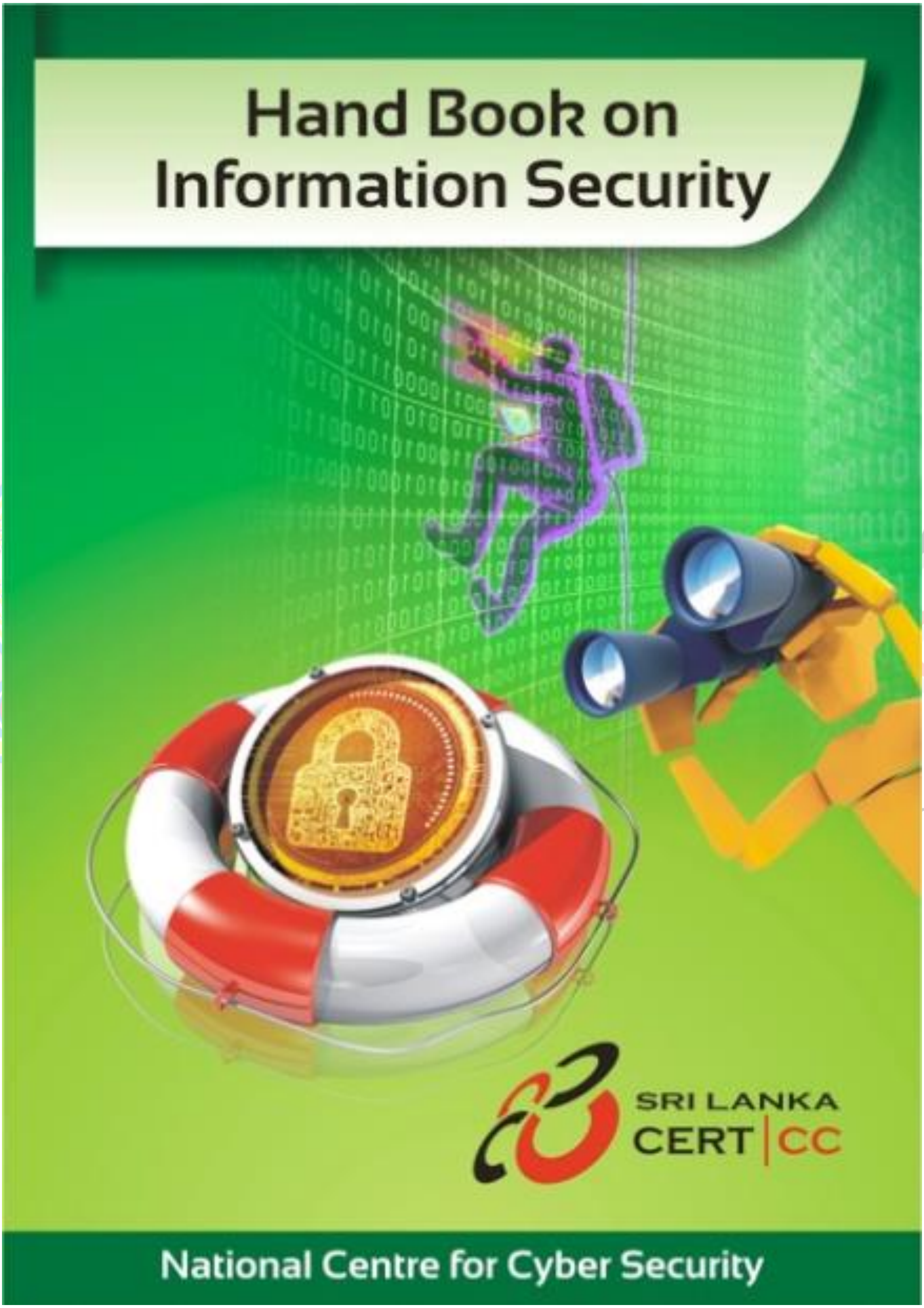


Hand Book on Information Security

SRI LANKA CERT|CC

National Centre for Cyber Security

Contents

1 About Sri Lanka CERT|CC

Cyber-attacks come in many forms, such as Denial of Service (DoS) attacks, website defacement and unauthorized access to systems. These are committed by a wide spectrum of individuals, organized groups and organizations such as fraudsters, terrorist groups thrill seekers and even state funded establishments.

The national CERT|CC (Computer Emergency Readiness Team | Co-ordination Center) acts as the focal point for Cyber security for the nation. It is the single trusted source of advice about the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation, in responding to and recovering from Cyber-attacks.

In anticipation of increased cyber security incidents with the growth of Sri Lanka's IT infrastructure, Sri Lanka CERT|CC was established in 2006 as Sri Lanka's National CERT, by the ICT Agency of Sri Lanka (ICTA). It is a fully owned subsidiary of ICTA and currently under the Ministry of Telecommunications and Digital Infrastructure.

CERT is mandated to protect our constituency, both by reacting to incidents and by proactively strengthening security against potential threats.

Accordingly, Sri Lanka CERT|CC offers three broad Service Categories:

a. Responsive Services

These are services which are triggered by reported events that are capable of causing adverse effects on a constituent's Cyber Systems;

- Incident Handling

This service involves responding to a request or notification by a constituent that an unusual event has been detected, which may be affecting the performance, availability or stability of the services or cyber systems belonging to that constituent.

There are many types of Incidents. Some typical examples are:

- Malware (Viruses, Trojans, Backdoors, etc.)

- Web Site Defacement
- DoS Attack
- Phishing
- System Compromise

b. Awareness Services

These services are designed to educate our constituents on the importance of Information Security and related topics ranging from Information Security Fundamentals and best practices to more immediate issues, such as the latest cyber threats and attacks.

- Alerts
- Seminars & Conferences
- Workshop
- Knowledge Base

c. Consultancy Services

These services are aimed at providing constituents with a means of determining the adequacy of their Information Security systems, and (if found necessary) to take necessary steps to strengthen its defenses.

- Technical Assessment
- Advisory for establishing an Information Security Policy within organizations

2 Introduction

The cyber security threat landscape is constantly changing and threats against individuals and organizations are on the increase. While some may be aware of these threats, some may not know of security preventive mechanisms that should be followed in order to minimize victimization.

Social media has had a lasting impact on the lives of most citizens and this trend is evolving at an exponential rate. It is used by people as a medium to communicate amongst each other to share personal photos, videos, views and reviews on updates relating to our daily life, politics, sports, markets and much more using devices like computers, tablets, and cell phones etc. on the internet. The main purpose and aim of using these websites such as Facebook, WhatsApp, Viber and other websites such as Twitter, Tumblr, video sharing websites like YouTube and Daily-motion and other kind of platforms is to make our life flexible by rapidly sharing almost everything that we come across. People use and rely on social media so much that businesses nowadays cannot resist using these platforms to maximize their productivity and profits.

Although these points that have been highlighted above are the positive aspects of using social media, there can be adverse effects that can be harmful to the general public due to the misuse and abuse of Social media.

This hand book specifically focuses on how to secure yourself on social media platforms, and becoming a victim of various types of online threats and crime, and provide recommendations on effective steps to protect yourselves.

3 Cyber Threats

3.1 Most common cyber threats

3.1.1 Ransomware

Ransomware is a type of malware (malicious software) that locks users from accessing their data in their computer or any mobile device. In order to unlock their data, the users must pay a certain amount of ransom, this is mainly done by the payment method which uses Bitcoin. Although paying is an option for recovering your data, we do not recommend payment because there is no guarantee the attackers will keep their promise.

How to defend yourself or your organization from Ransomware;

- Comprehensive awareness training to avoid being victimized by phishing emails
- Disabling hidden file extensions
- Disable macro scripts
- Block AppData / Local AppData.
- Take regular backups of your important data.

3.1.2 Adware

Adware programs that are specifically designed to advertise products on your computer and direct you to advertising websites. They are also designed to collect information about your personal preferences or the searching patterns so that they can target more advertisements to your device while you surf the Internet. It is important to remember that Adware collects information with your consent and if you come across a malware without your consent it is categorized as a malicious program.

Adware can get into your computer in mainly two ways;

- Through shareware or freeware programs
- Infected Websites that can result in an unauthorized installation of adware

You cannot uninstall Adware. If you sense a presence of an Adware in your computer, you can simply use an anti-virus software to remove it.

3.1.3 Rootkits

Rootkit is a program that will provide privileged access to your computer without your knowledge. Rootkit contains a combination of a set of malware such as a virus, worm or a Trojan.

When a rootkit is installed, a unauthorized user can remotely access your computer and change the system configuration. A rootkit on an affected computer can also access the log files and spy on the infected computer owner's data.

It is difficult to detect a rootkit and there is no commercial software available to detect it. You can protect your computer from rootkits by updating the patches on your Operating System (e.g. Windows) and updating your anti-virus guard. Don't accept files or open email file attachments from suspicious sources. Be careful when installing software and carefully read the end-user license agreements.

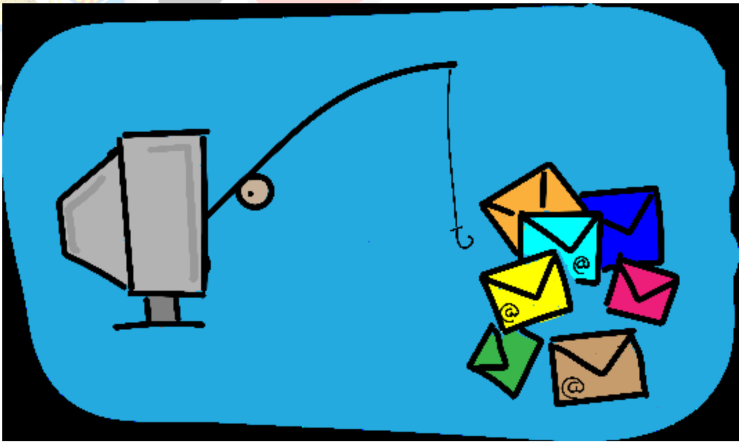
3.1.4 Spyware

Spyware is a malicious program installed on a user's computer without the knowledge of the user to collect sensitive personal information about the user such as identity and payment details. This software is known as tracking software.

3.1.5 Phishing attacks

A Phishing attack is the primary vector for malware attacks and is usually comprised of a malicious e-mail attachment or an email with an embedded, malicious link.

Phishing emails typically falsely claim to be an established or legitimate enterprise such as your bank. Many Phishing victims fall prey to these phishing e-mails and disclose their log-in credentials to fraudsters.



3.1.6 Drive by download

The Drive-by download is a program that is automatically downloaded to your computer without your consent or even your knowledge.

These are triggered simply by a victim clicking a link which, unwittingly injects malicious software (Trojans) on to their computers.

3.2 Most common threats faced by users when using mobile devices

- **Data loss from lost or stolen devices**
  The information obtained through a mobile device that has been stolen or lost has immediate drastic results. If the victim has weak password access, no passwords, and little or no encryption, it can lead to data leakage from the devices.

- **Data misuse from sold devices**
  Users should never sell or discard devices without understanding the risk to their personal data being disclosed. Some data on devices of the previous user can be recovered. The threat level from data loss is high.

- **Information-stealing malware**
  Android users can easily download and install apps from third-party marketplaces other than Google's official "Play Store" which can result in malware containing applications to steal data from the host device.

- **Unsecured Wi-Fi and network access**
  Free Wi-Fi has increased over the past few years. Increased access to public Wi-Fi, along with increased use of mobile devices, creates a high chance for illegal interception of data.

- **NFC and proximity-based hacking**
  Near-field communication (NFC) allows mobile devices to communicate with other mobile devices by using short-range wireless technology. Due to the valuable information being transmitted such as contact information, this is likely to be a target for attackers in the future.

4 Tips to be secure in cyberspace

a. Password policy

- Choose a strong password

Passwords help you to protect your privacy and identity. The strength of a password is the most important factor. If your password is stolen or guessed by someone, he/she can log in to your account. It can cause many problems, including the damaging of your reputation or risk disclosing sensitive financial information.

For a stronger password, use a combination of upper and lower case characters, numbers and special characters such as *, $, £ etc., A strong password should usually have at least 8 characters and these can be a combination of the characters mentioned above. Following are few examples of weak passwords and tips on how you could build a stronger password.

Examples of weak passwords: saman123, samanKV5510, 0771234567

Tip 01: Creating stronger passwords

Use numbers and special characters instead of using normal characters.
Example: 'saman123' is a weak password.
To create a stronger password, you could;

- **Replace letter 'S' with number 5,**
- **The letter 'a' with number 4, and**
- **Replace number 1 with the special character '!'**

The resulting password '54m4n!23' is a much better alternative than 'saman123'.

- Updating the password

You need to update the password on a regular basis. It is recommended to do this once in every three months.

- Keep your password safe.

- Use a Strong password
- Never tell anyone the password or provide even a hint about it
- Choose a password which you can remember easily, do not write it down anywhere
- There could be requests from web browsers or websites to "remember" the password. Do not accept these requests
- Use different passwords for different accounts

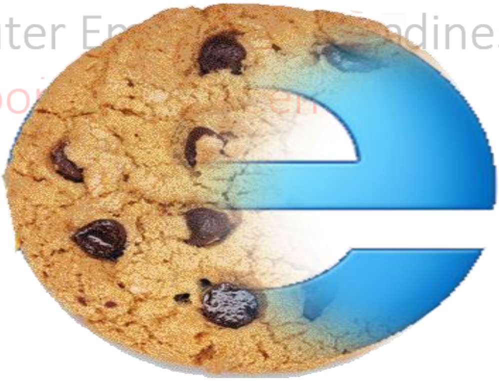
b. Identify Secure Websites

Before entering sensitive information such as credit card details or passwords on a web-site, ensure that the link is secured.

- If it is a secured connection, there should be a "padlock" in the address bar.
- The web address should begin with https://. The 's' stands for "SECURE".

c. Cookies

- Cookies are files on a computer, tablet or smart phone that websites use to store information about the user between the sessions
- Configure the browser to warn the user when a cookie is installed
- Use an anti-spyware program that can scan cookies called "tracker cookies"



d. Avoid Social engineering attacks

- Never open email attachments from unknown sources

- Never click on links in emails received from unknown sources
- If you receive a telephone call requesting confidential data, verify the callers' identity
- Do not insert external storage devices into computers, if the source of the media is unknown

e. **Avoid data loss**

- Regularly back-up your personal files. It will help in case your computer crashes or it is stolen.
- Configure access levels (as who can access and what data can be accessed)

f. **Remove user admin rights for those who do not need it**

g. **Always run patch updates of the operating system (e.g. Windows) and applications**

h. **Invest in solutions such as:**

- Web protection
- Email protection
- Managed online backup
- Mobile device management
- Password manager

i. **Install and subscribe to a genuine antivirus software or virus guard**

j. **Install real-time anti-spyware protection**

k. **Keep anti-malware applications current**

l. **Perform daily scans**
m. **Disable auto run**

n. **Disable image previews in Outlook**

o. **Don't click on unknown email links or attachments**

p. **Surf smart**

q. **Lock the computer when you go away**

r. **Remember to logout when you access your email or social media accounts from a public place with free Wi-Fi**

4.1 How to minimize mobile device threats

- Enable a pass code
- Enable Fingerprint/Biometric lock if available
- Turn off Wi-Fi and Bluetooth when not in use
- Turn off location services of apps
- Keep your system (IOS or Android) updated
- Enable find my device feature (iPhone/Android phones) if possible
- Avoid downloading/using untrusted third party apps and check permissions before installing apps
- Avoid texting or emailing private and sensitive information
- Install mobile security apps
- Always log out from Banking, Shopping or any other social media sites after use
- Ensure that the text messages are correct and coming from the correct domain, look for obvious spelling and grammar mistakes, and call the appropriate company if the text messages seems strange or suspicious

5 Security controls for email and social media accounts

a. There are various privacy and security controls provided by email and social media service providers.

Social media services such as Facebook, Twitter, LinkedIn and Email services such as Gmail, Yahoo, Hotmail etc. provide privacy settings that should be made good use of.

b. Using passwords is fundamental in securing your social media or email accounts. In addition, you could use a mechanism known as “Two-factor authentication or Two-factor verification”. Some websites provide this service to its users and this is how it works.

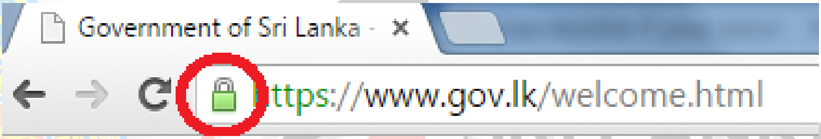
Two-factor Verification Process
Step 01: Similar to using a recovery/alternative email address, use your phone number to do the same.
Step 02: When you sign-in to your social media/email account, you will first enter your password as usual.
Step 03: Then, a code will be sent to your mobile phone via a text message or voice call. This is a one-time code, meaning that each code can only be used once.
Step 04: Enter this code when prompted by the website to complete account sign-in.

If you are in the habit of frequently using Internet cafes, computer laboratories in schools/universities etc., it is advisable to use the above mentioned protection mechanisms to stay safe online. When leaving such places, make sure to log out of your accounts and change the passwords as soon as you get to a safe network.

6 Securing email accounts

a. Be vigilant when you receive messages via emails or websites requesting information about your account details or passwords. It can be a phishing mail to collect your personal information. Only provide the requested information if you can verify that it came from a trusted party.

If the email contains any links don't click. Copy and paste it on the browser and check whether the secure http header (**"https") is** there**.** Some Web browsers display a **'lock icon'** or **'the padlock'** when you are on a secure web site (See example below).



b. Always check the sender's email address very carefully before taking any actions based on the email content. Mere checking of the display name of the sender is NOT sufficient.

c. Using a strong password which will not be able to predicted by another person;

- Use numbers, upper case characters, special characters such as $, @, _, / when Creating the password.
- Do not include your name, contact numbers, NIC or common words as the password.
- There should be at least 8 characters in the password.
- Remember not to disclose the password to others.

d. Use two-factor authentication so that whenever you login to your email you will get a message to your mobile number or to the email address.

e. Be proactive in protecting your privacy. Never send your personal details (name, address, telephone number, NIC number, driving license number, family members' details, or passport number) to individuals that you do not know personally.

f. Take maximum use of the privacy settings provided by the Email service providers. When uploading or publishing pictures or personal information on social media, make sure that such information can only be seen by the friends/people you trust.

g. Think twice when clicking links or URLs received via emails. For instance, if the email claims to be from your bank, call the bank first to verify that they have actually sent you the said email.

h. If anyone tries to violate your privacy or to destroy your online reputation, never hesitate to report such instances to relevant authorities (e.g. Sri Lanka CERT) or block/deactivate such accounts if they belong to you.

i. Don't fall prey to online scams such as winning fake lotteries or appeals for money claiming to be from legitimate organizations.

j. Never expose your password to anyone. Never write it down on post-it notes or on your desk calendar at work where others can easily see it.

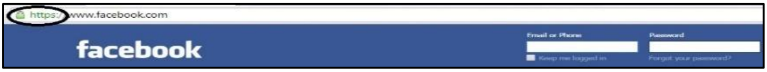
7 Securing social media accounts

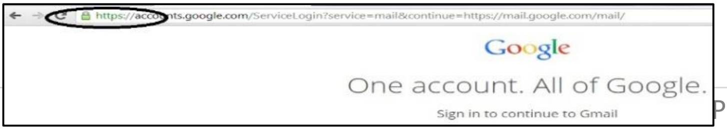
a. If your email or social media accounts are created for you by someone else, it is important to keep a record of details such as birthday, alternative email accounts etc., that he/she has used when creating your account. In case you forget your password or your account becomes inaccessible due to a security breach, you need the details mentioned above to recover your password or regain access to your account.

b. Always keep your social media accounts and related email accounts active. If you believe that your social media account has been compromised or hacked, you need the related email account to regain access to your account. Also make sure to provide a recovery email address or an alternative email address for your email account. This will help you to regain control of your email account in instances where the password has been stolen or changed.

c. Never enable "Remember Password" option when surfing via a mobile phone or public computers. Some Web browsers such as Firefox offers 'Password Manager' option. This could store usernames and passwords you use to access websites and then automatically fills them in for you the next time you visit. In the unfortunate event of losing your mobile phone for instance, anyone who finds it can easily gain access to your accounts.

d. When using email/social media accounts, be vigilant about SMS or email messages you may receive prompting you to verify your login details. In some instances, such messages will redirect you to a website upon clicking on a link. When this happens, always check if the http header is **"https".** **"https"** is a is a protocol for secure communication over a computer network and this means that information exchanged between you and the web site is secure. Follow the same principle when entering your username and password to login to Web accounts (see examples below).




https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/
Google
One account. All of Google.
Sign in to continue to Gmail

7.1 Facebook

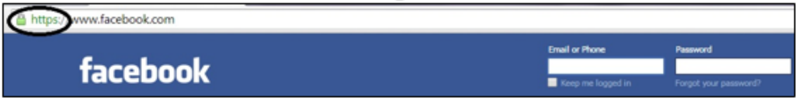
Facebook is a popular free social networking website that allows users to create profiles, upload photos and video, send messages and keep in touch with friends, family and colleagues.

7.1.1 How to keep your Facebook account secure?

a. Make sure that you have set the Privacy settings on your Facebook account.

b. When you are directed to the face book site, always check whether the url includes **“https”.” https”** means the information exchanged between you and web site is secure. Some web browsers show the “**lock icon”** when you are in a secure web site.

c. Use a strong password which cannot be guessed.



d. I f someone else has created the Facebook account for you then you should keep your account information such as email address, contact, birthday, date they have created the account noted safely. So that you will be able to recover your account in an inaccessible situation due to security breach.

e. Use two-factor authentication so that whenever your login to the face book you will get a message to your mobile contact or to the email address.

- Setting→security→Use two-factor authentication
- select “**add phone number”**
- Then select the link **“set up”** to set two-factor authentication

f. If your login to your Facebook account through public locations, make sure that you have successfully logged out before leaving the place, and change the password as soon as you get to a safe network.

g. Never accept requests from fake profiles/unknown person even though sometimes that person may have lots of mutual friends.

h. Make sure when you are sending friend requests that those accounts are genuine.

i. When you upload photos, selfies or other posts it is safer if you customize it so that the information can be viewed only if the person is in your friend list. This way your photos will be secure.

7.1.2 How to know if your Facebook account is being hacked?

a. Personal details such as Your name, birthday will be changed even though you have not changed.

b. You are not able to login because email or password has been changed.

c. Friend requests are sent from your account to unknown people.

d. Messages have been sent from your account, even though you didn't write them.

e. Posts are appearing on your timeline that you didn't post.

f. If you have set two factor verifications settings, you will receive a message to your mobile or email address when a hacker tries to enter your Facebook account.

7.1.3 How to recover a hacked Facebook Account?

a. If you still have access to your face book account immediately change your password.

b. If the hacker has changed your password and you don't have access to your Facebook account, then reset your password by using **"forgot your password".** It will let you retrieve your password.

If you need to **Find Your Account**, you can either enter the email address you used to register with Facebook or any other secondary email address you added, as well as your phone number. Facebook will send a recovery code to your recovery email addresses or the telephone number you have provided in your account recovery option. This is the only option available to recover the account. Use that code to reset your account password. Remember that you must keep those accounts equally secure, at least by using a strong password and ideally by enabling two-factor authentication.

c. **Report the Facebook account**

If your account wasn’t simply hacked, but posts are appearing on your timeline that you didn't post and send spam to your friends, you must “**report it as compromised”.** Use www.facebook.com/hacked to report.

7.1.4 How to report a fake Facebook account?

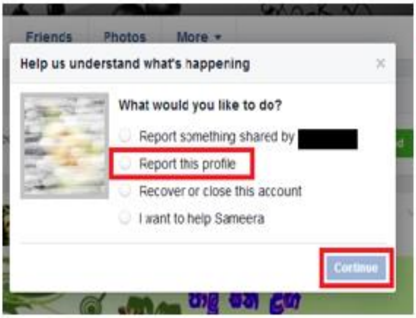
a. Search for the fake account

b. Once you go to that fake profile through your original Facebook account, Click the drop down list ••• next to the messages button in the cover photo. select ‘Report/Block’.

c. You’ll see a popup; there you have to select the ‘Report’ type.

d. Select ‘This profile/timeline is pretending to be someone or fake’. then select the option “Pretending to be me”.

e. Click Continue to submit your report. And proceed with the instructions. Make sure that you submit the report successfully.



Help us understand what's happening ×

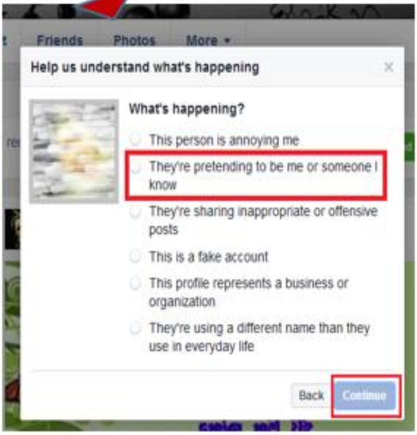
What would you like to do?

○ Report something shared by [redacted]

○ Report this profile

○ Recover or close this account

○ I want to help Sameera



Help us understand what's happening ×

What's happening?

○ This person is annoying me

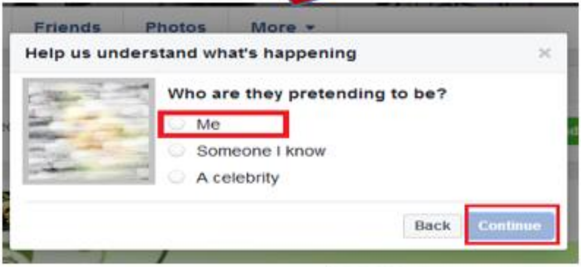
○ They're pretending to be me or someone I know

○ They're sharing inappropriate or offensive posts

○ This is a fake account

○ This profile represents a business or organization

○ They're using a different name than they use in everyday life



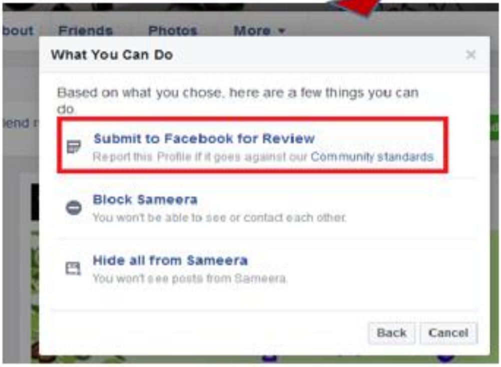
Help us understand what's happening ×

Who are they pretending to be?

○ Me

○ Someone I know

○ A celebrity



What You Can Do ×

Based on what you chose, here are a few things you can do.

Submit to Facebook for Review
Report this Profile if it goes against our Community standards.

Block Sameera
You won't be able to see or contact each other.

Hide all from Sameera
You won't see posts from Sameera.

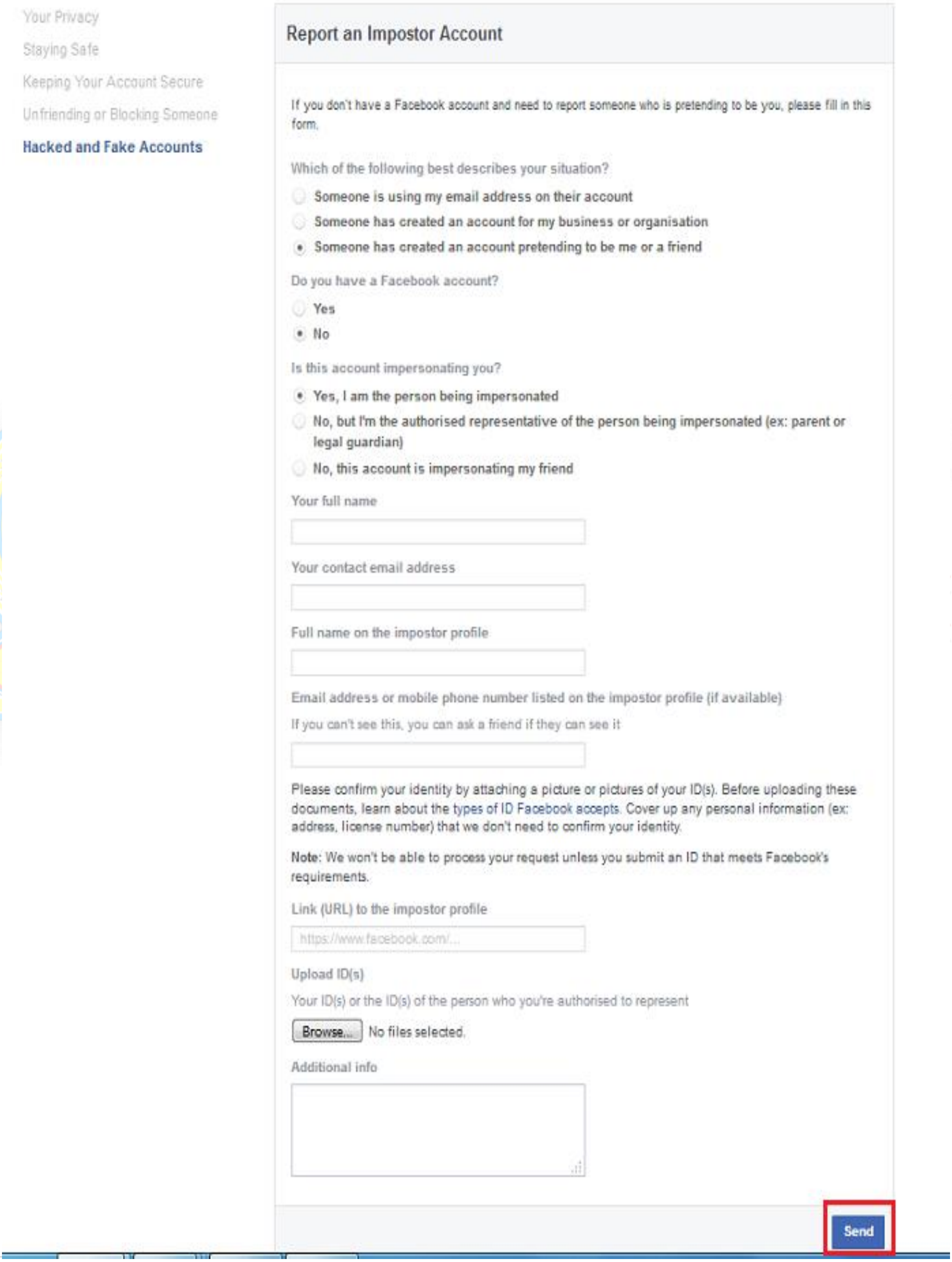
7.1.5 How to report a fake Account if you're not on Facebook

a. Click the **"Help"** link on Facebook's login screen**.** This is located at the very bottom of the login screen.

b. Click the **"Report Something"** a list of links appears. The "Report abuse" link is located towards the bottom.

c. Select the **"Don't Have an Account"** link from the list. After you select this link, several options will appear. Choose the option that corresponds to the violation you want to report.

d. Choose **"fill out this form** "link. Once you are directed to the "Report a Violation of Facebook Terms" form fill that form and attach the picture of Government-issued ID of the person being impersonated click **"send"** as shown below.



Report an Impostor Account

If you don't have a Facebook account and need to report someone who is pretending to be you, please fill in this form.

Which of the following best describes your situation?

○ Someone is using my email address on their account

○ Someone has created an account for my business or organisation

● Someone has created an account pretending to be me or a friend

Do you have a Facebook account?

○ Yes

● No

Is this account impersonating you?

● Yes, I am the person being impersonated

○ No, but I'm the authorised representative of the person being impersonated (ex: parent or legal guardian)

○ No, this account is impersonating my friend

Your full name

Your contact email address

Full name on the impostor profile

Email address or mobile phone number listed on the impostor profile (if available)

If you can't see this, you can ask a friend if they can see it

Please confirm your identity by attaching a picture or pictures of your ID(s). Before uploading these documents, learn about the types of ID Facebook accepts. Cover up any personal information (ex: address, license number) that we don't need to confirm your identity.

Note: We won't be able to process your request unless you submit an ID that meets Facebook's requirements.

Link (URL) to the impostor profile

https://www.facebook.com/...

Upload ID(s)

Your ID(s) or the ID(s) of the person who you're authorised to represent

Browse... No files selected.

Additional info

7.2 WhatsApp

WhatsApp is a popular free social networking mobile app that allows users to create an account, send messages, photos and video, and keep in touch with friends, family and colleagues.

7.2.1 How to configure privacy settings on WhatsApp?

Once you go to WhatsApp, tap on the Menu button displayed at the top right corner and then select icon just after the search bar.

Go to **settings** → **Account**→ **Privacy**

Then you can set the following options separately for last seen, profile photo about (personal information) and status

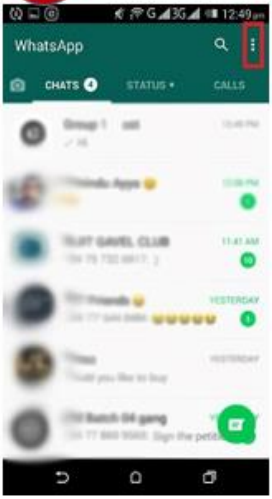
- **Everyone**
  Your last seen, profile photo and/or status will be available to all WhatsApp users.

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

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

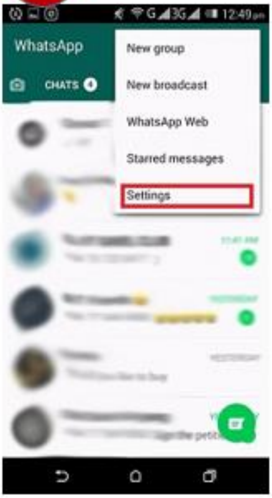
7.2.2 Steps to configure privacy settings on WhatsApp

1


WhatsApp

CHATS 4 STATUS CALLS

2


WhatsApp

CHATS 4

New group

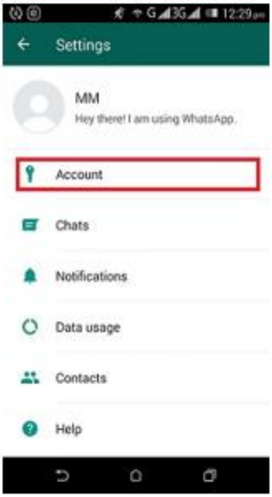
New broadcast

WhatsApp Web

Starred messages

Settings

3


Settings

MM
Hey there! I am using WhatsApp.

Account

Chats

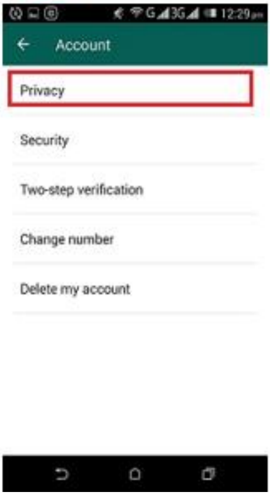
Notifications

Data usage

Contacts

Help

4


Account

Privacy

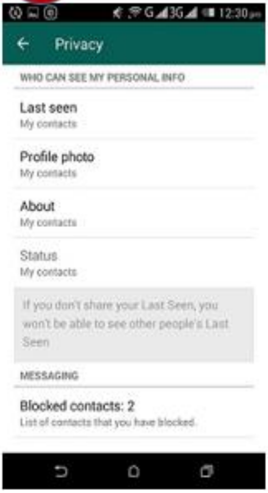
Security

Two-step verification

Change number

Delete my account

5


Privacy

WHO CAN SEE MY PERSONAL INFO

Last seen
My contacts

Profile photo
My contacts

About
My contacts

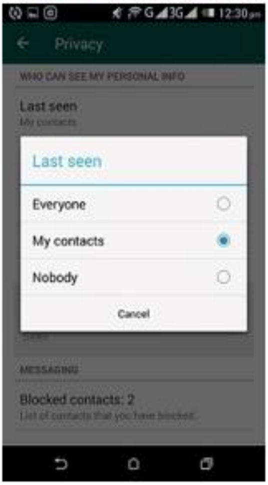
Status
My contacts

If you don't share your Last Seen, you won't be able to see other people's Last Seen

MESSAGING

Blocked contacts: 2
List of contacts that you have blocked.

6


Privacy

WHO CAN SEE MY PERSONAL INFO

Last seen
My contacts

Last seen

Everyone ○

My contacts ●

Nobody ○

Cancel

MESSAGING

Blocked contacts: 2
List of contacts that you have blocked.

7.2.3 How to configure security settings on WhatsApp?

WhatsApp has performed a magnificent feat in bringing end-to-end encryption for all communications

a. Make sure that WhatsApp has access to your camera. You may have already allowed this when you install WhatsApp.

b. Open a conversation with your friend in WhatsApp and then select the person's name at the top of the conversation.

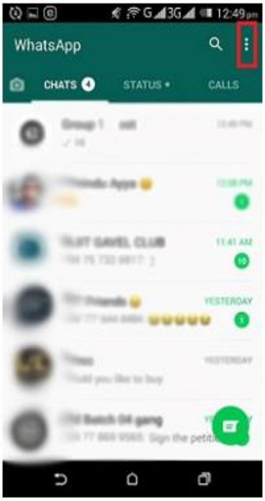
c. This will open the contact window for that person. Near the bottom of that screen you will see a setting for Encryption.

d. Tap on the encryption field, and you will view a screen that displays a QR code as well as a 60-digit decimal code that represents the contents of that QR code.

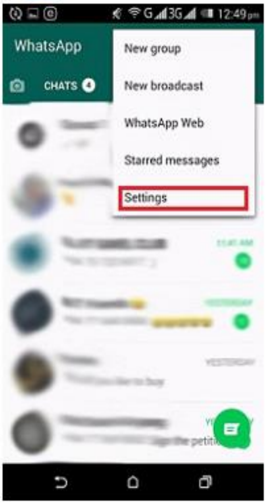
e. At the bottom of the QR code screen, there is a link that will enable you to scan your friend's code, and they can do the same for your code.

7.2.4 Steps to configure security settings on WhatsApp

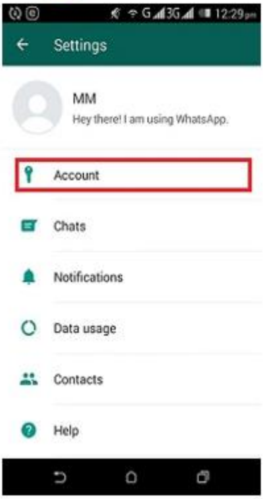
1



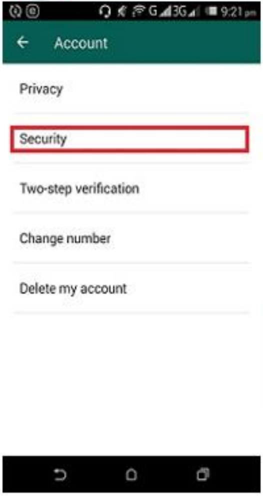
2



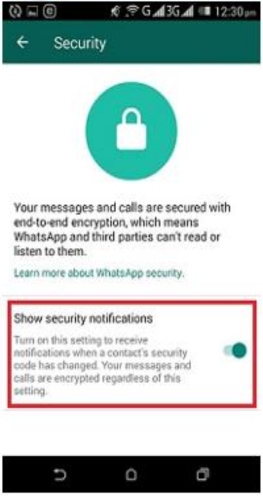
3



4



5


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.

7.2.5 How to configure two-step verification settings on WhatsApp?

a. Once you go to WhatsApp, tap on the Menu button displayed at the top right corner and then select drop down icon just after the search bar. Then select, **Settings → Account → Two-step verification →Enable**

b. Once you do that, the app will ask you to provide an email and set a six-digit passcode.

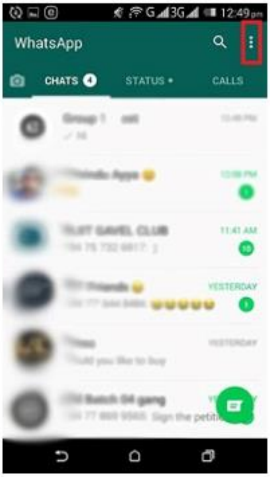
c. On next screen, enter your email ID (optional) to enable passcode recovery via email. (It's recommended to use email as backup so that you're not locked out of your account if you forget your passcode.) Then tap "Done".

d. Next time when you reconfigure your WhatsApp account on your new phone or want to add a new phone number to your account, the messaging app will require you to enter and confirm this six-digit secret code.

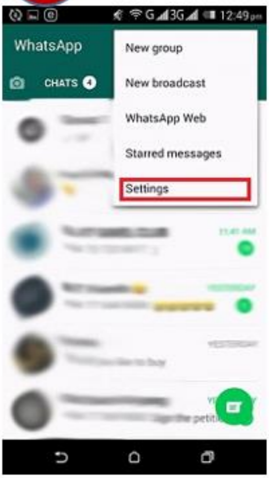
e. Importantly, two-step verification can be disabled within the app without a passcode so your account could still be compromised if your phone falls into the wrong hands. But the update should help lock things down in case someone tries to hijack it from afar.

7.2.6 Steps to configure two-step verification settings on WhatsApp

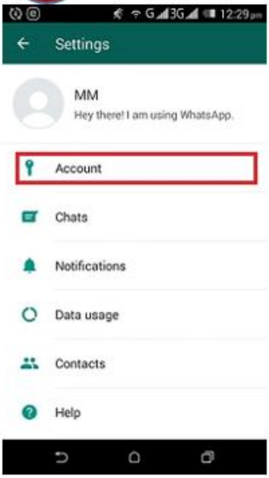
1



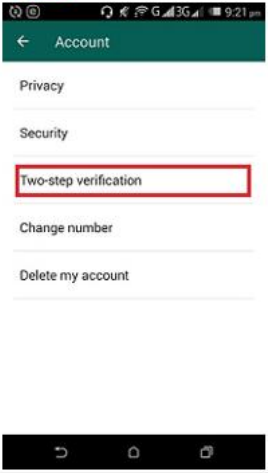
2



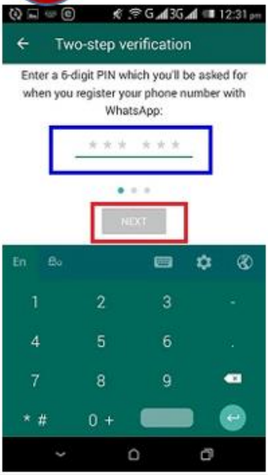
3



4

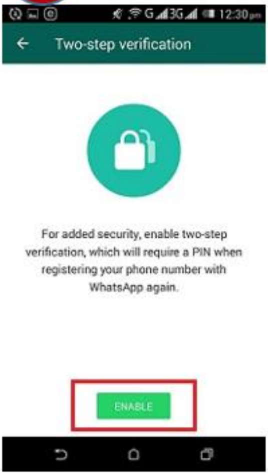


5



Enter a 6-digit PIN which you'll be asked for when you register your phone number with WhatsApp:

6



For added security, enable two-step verification, which will require a PIN when registering your phone number with WhatsApp again.

7.2.7 How to change the number on WhatsApp account?

- Make sure your new “phone number “can receive SMS and/or calls and has an active data connection before changing the number.

- Make sure your “old phone number “is currently verified in WhatsApp on your phone. You can see what number is verified in WhatsApp by navigating to **WhatsApp** → **Settings** and tapping on your profile photo before changing the number.

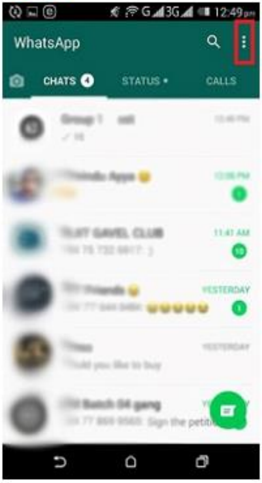
- Once you go to WhatsApp, tap on the Menu button displayed at the top right corner and then select drop down icon just after the search bar. Then select, **Settings** → **Account** → **Change Number.**

- Enter your current WhatsApp phone number in the first text box. Enter your new phone number in the second text box. Then tap “**Done”** to continue

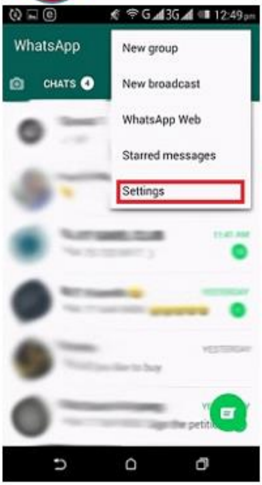
- If you Change Number, as long as you continue using the same phone your chat history will be available on your phone with the new phone number.

7.2.8 Steps to change the number on WhatsApp account

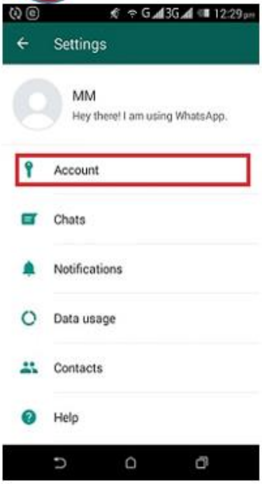
1



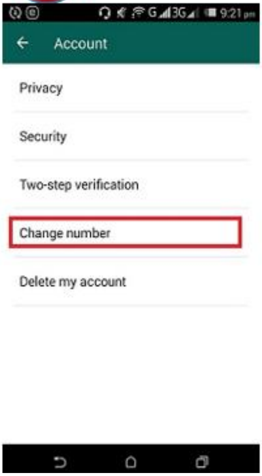
2



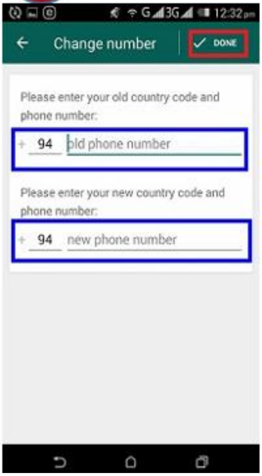
3



4



5



Please enter your old country code and phone number:

+ 94 old phone number

Please enter your new country code and phone number:

+ 94 new phone number

7.2.9 How to delete the WhatsApp account?

a. Removal of all the information in your chats and media files in WhatsApp is however not a permanent process. It does not guarantee permanent deletion of all data in such a way that they are unrecoverable.

b. Check all the information in the 'WhatsApp' and 'WhatsApp Attachment' before you start deleting your account. This will help in permanently erasing all the data, and. This will ensure that no privacy leak happens when you delete the account.

c. Once you go to WhatsApp, tap on the Menu button displayed at the top right corner and then select drop down icon just after the search bar. Then select, **Settings** → **Account** → **Delete my account.**

d. A text box will appear on the screen, enter the complete phone number of your device including the international code.

e. Now tap on, **"Delete my Account".**

f. Things you should know when deleting the WhatsApp account;

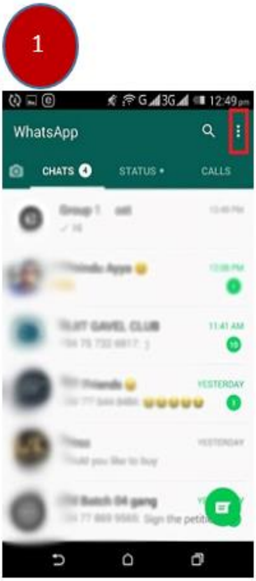
- When you have completed the WhatsApp account deletion, contacting you via your WhatsApp account will not be possible. If you were part of your friends' list of favorite persons to contact, your detail and name would not appear any more.

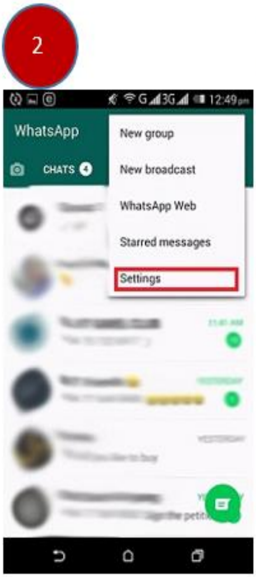
- All the conversation, messages and chats will be erased from your device and you will be unable to access such information. If WhatsApp is synchronized the data can be recovered.

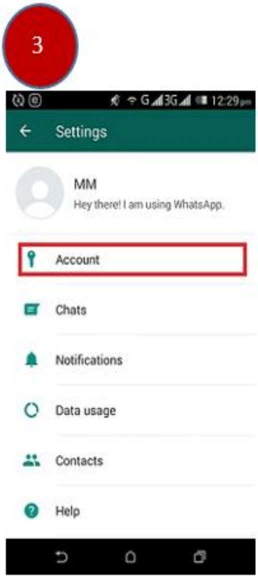
-

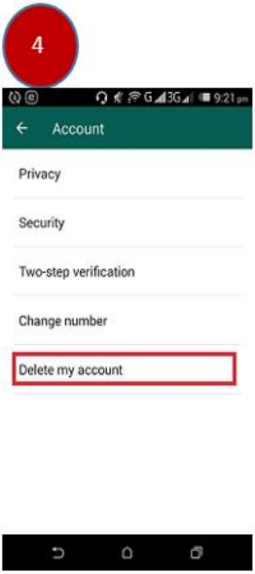
- You name as well as the number will not be part of the WhatsApp groups you belonged to earlier.

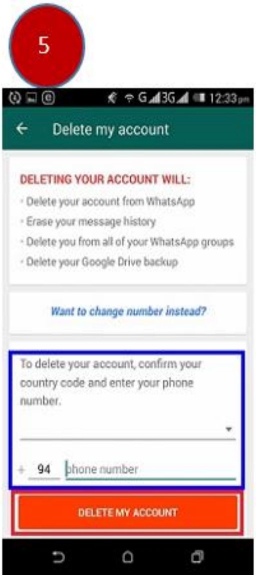
7.2.10 Steps to delete the WhatsApp account











DELETING YOUR ACCOUNT WILL:

- Delete your account from WhatsApp
- Erase your message history
- Delete you from all of your WhatsApp groups
- Delete your Google Drive backup

Want to change number instead?

To delete your account, confirm your country code and enter your phone number.

+ 94 phone number

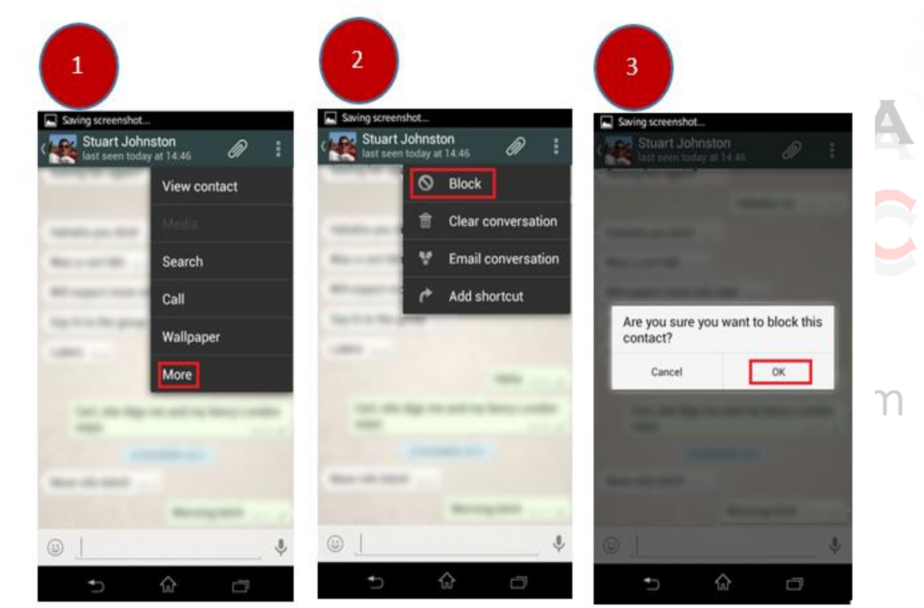
DELETE MY ACCOUNT

7.2.11 How to block WhatsApp contacts?

Open the WhatsApp application and select the contact you want to block. When you click on the three vertical dots located in the top right of the screen (settings menu), a drop down list will appear with an option **"More"**. Tap that option.

Then Click Block and then select OK to confirm that you want to block the selected person.

7.2.12 Steps to block WhatsApp contacts



Are you sure you want to block this contact?

7.3 Viber

Viber is a popular free social networking mobile app that allows users to create an account, send photos and video, messages and keep in touch with friends, family and colleagues.

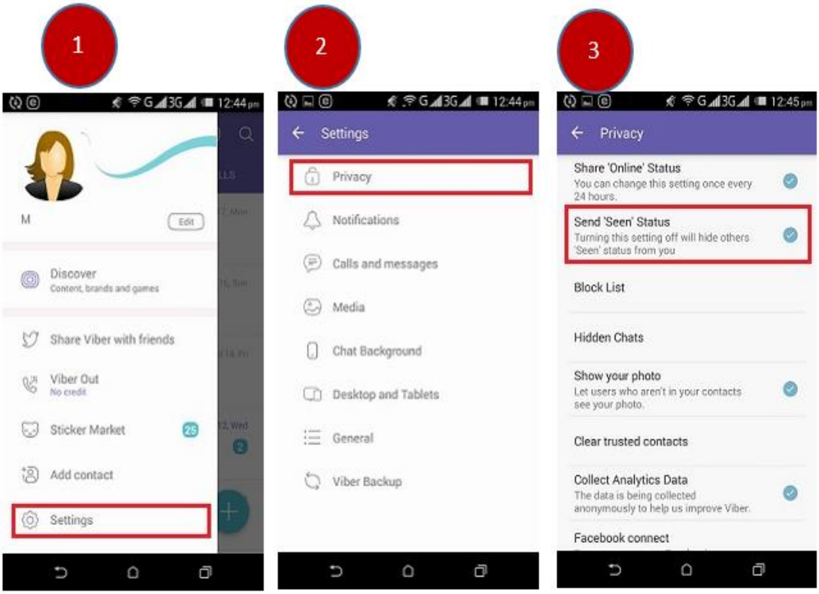
7.3.1 How you can protect your privacy while using Viber?

a. Customize your Viber privacy settings

b. Prevent others from being notifying that you saw the messages;

The "seen" status of messages will be displayed on the screen of the contact you are communicating with once you open their message on your phone.

Select Settings→ Privacy → turn this feature off.



Share 'Online' Status
You can change this setting once every 24 hours.

Send 'Seen' Status
Turning this setting off will hide others 'Seen' status from you

Block List

Hidden Chats

Show your photo
Let users who aren't in your contacts see your photo.

Clear trusted contacts

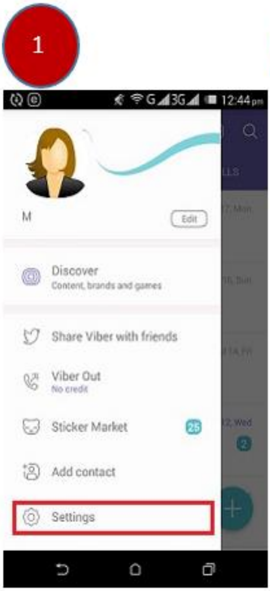
Collect Analytics Data
The data is being collected anonymously to help us improve Viber.

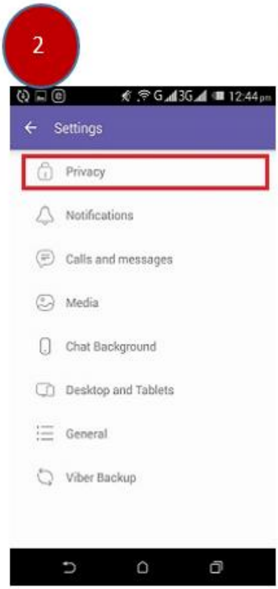
Facebook connect

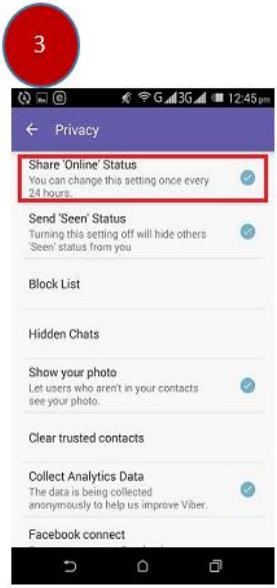
c. Change your login status.

If you are trying to avoid talking to some of your Viber contacts, but you wish to check some of your messages at the same time and talk to people who are important to you;

Select Settings→ Privacy → turn off the **"Share Online Status".**







Share 'Online' Status
You can change this setting once every 24 hours.

Send 'Seen' Status
Turning this setting off will hide others 'Seen' status from you

Block List

Hidden Chats

Show your photo
Let users who aren't in your contacts see your photo.

Clear trusted contacts

Collect Analytics Data
The data is being collected anonymously to help us improve Viber.

Facebook connect

7.3.2 How to back up your Viber chats?

a. Once you click "Settings" you will be taken to a page called "Calls and Messages". you will see "Email message history".

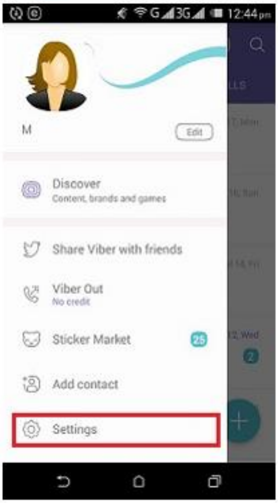
b. Tap the button and choose an application to email message history. Next, you need to choose "Email" and choose your preferred email address where your message history will be backed up.

c. Now the next thing is to set up your email account. Login to your email by entering your email ID and password then click "next". make sure you are connected to the internet because it will not work without being online. After setting up your email, select "Done".

d. In the next screen enter the email address that you will like to receive your message history backup and hit the arrow button that can be located on the top right corner of the app.

7.3.3 Steps to back up your Viber chats

1



12:44 pm

M

Edit

Discover
Content, brands and games

Share Viber with friends

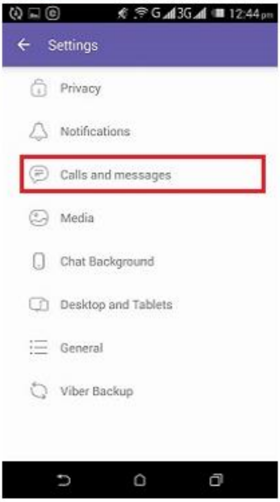
Viber Out
No credit

Sticker Market 25

Add contact

Settings

2

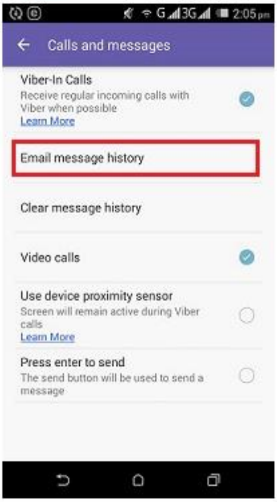


12:44 pm

Settings

- Privacy
- Notifications
- Calls and messages
- Media
- Chat Background
- Desktop and Tablets
- General
- Viber Backup

3



2:05 pm

Calls and messages

Viber-In Calls
Receive regular incoming calls with Viber when possible
Learn More ☑

Email message history

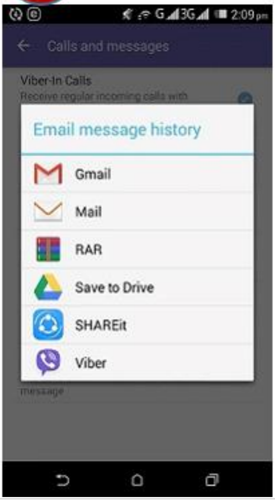
Clear message history

Video calls ☑

Use device proximity sensor
Screen will remain active during Viber calls
Learn More ○

Press enter to send
The send button will be used to send a message ○

4



2:09 pm

Calls and messages

Email message history

- Gmail
- Mail
- RAR
- Save to Drive
- SHAREit
- Viber

7.3.4 How to deactivate a Viber account?

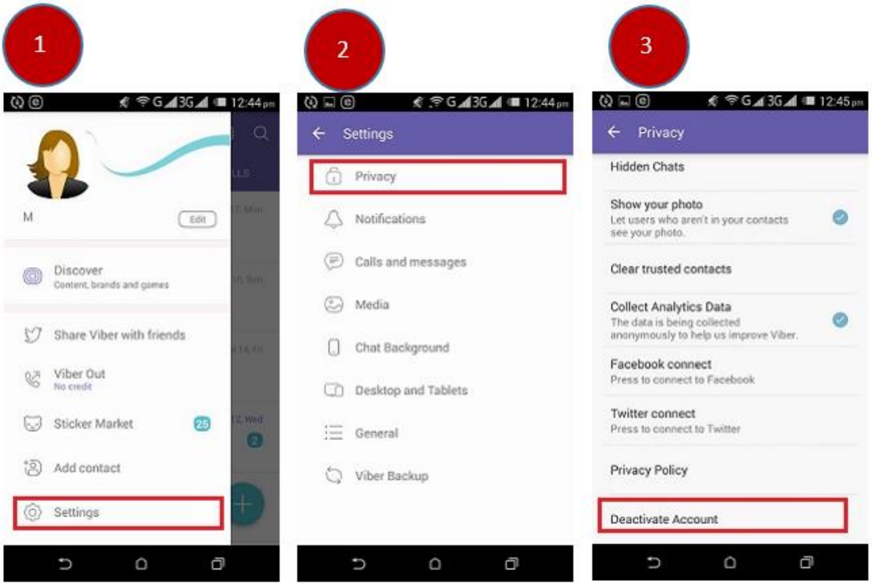
Once your account is deactivated, there is no way to restore any of your user data. Viber does not store any of your message history and is unable to retrieve lost data. Re-registering to Viber with the same mobile phone number will not restore the previous account history.

Create a backup of your Viber chats for safekeeping prior to deactivating your account before deactivating.

Launch the Viber account on your mobile, Select **Settings** option to access options. Then choose the Privacy Option and deactivate the account.

Select **Settings**→ **Privacy** → **Deactivate Account**

7.3.5 Step to deactivate Viber account



7.4 IMO

IMO is a popular free social networking mobile app that allows users to create an account, send photos and video, messages and keep in touch with friends, family and colleagues.

7.4.1 How to delete an IMO account?

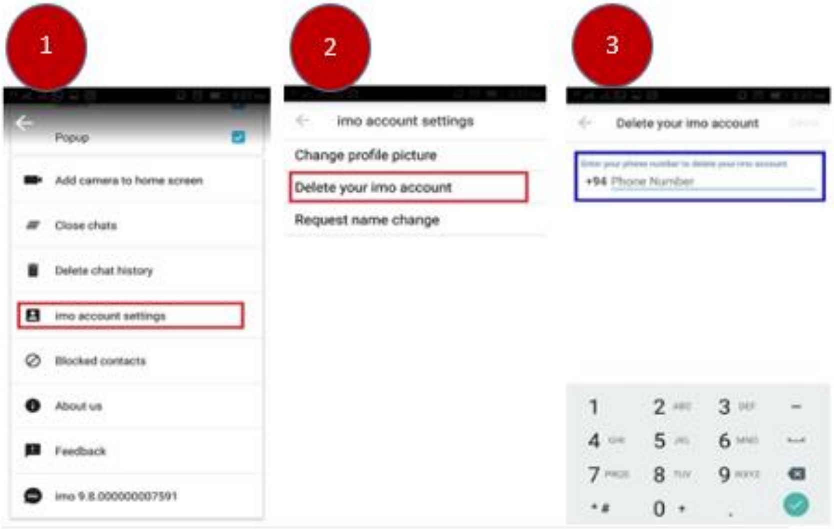
a. Once you open your IMO account from your phone. Tap on the **menu link** located at the bottom left corner of the app. Then, open your **profile** (you can do this by tapping either on your profile name or picture).

b. Select **IMO Account Settings** from the options that appears

c. Select **'Delete your IMO account'** from the options that appears next.

d. Enter the phone number you used in opening your IMO account and tap on **'Delete'** to delete your IMO account. Then confirm the delete process by selecting **'Yes'** and your account will be removed from IMO database.

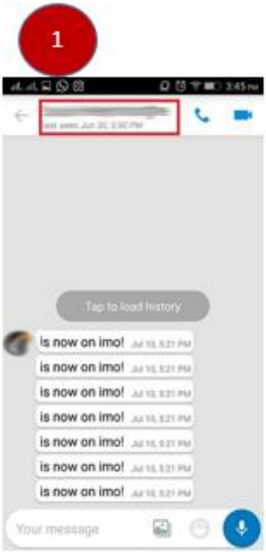
7.4.2 Steps to delete an IMO account



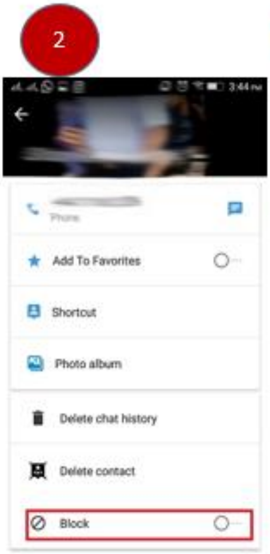
7.4.3 How to Block an IMO chat?

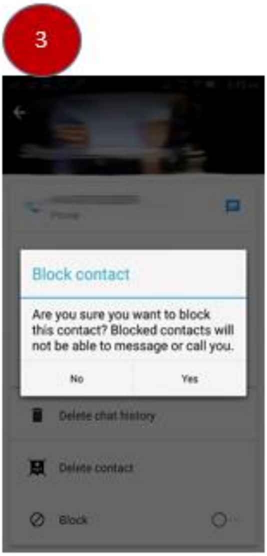
a. Once a **user profile is open** on IMO. click on his/her name from the top of your screen.
b. Scroll down enable **block option.**
c. Go back to profile and click on the **block button** to block him/her on IMO.

7.4.4 Steps to Block an IMO chat



is now on imo! Jul 10, 5:21 PM
is now on imo! Jul 10, 5:21 PM
is now on imo! Jul 10, 5:21 PM
is now on imo! Jul 10, 5:21 PM
is now on imo! Jul 10, 5:21 PM
is now on imo! Jul 10, 5:21 PM
is now on imo! Jul 10, 5:21 PM





Block contact

Are you sure you want to block this contact? Blocked contacts will not be able to message or call you.

8 Ethical Use of the Internet

- Do not create emails or social media accounts using other individuals' names.
- Never use or post other peoples' pictures or details in social media accounts without their consent.
- Always respect and protect yours and others privacy.
- Never use social media accounts or Internet for harming individuals' or companies' reputation or their personality at all costs.
- Always post the real facts in social media accounts regarding social problems caused by events or circumstances activities such as religious, political, etc.
- Never make, modify or edit others' portraits and publish them on popular social media websites without their consent.
- Do not publish nude pictures or pictures related to illegal drugs or alcohol on social media websites.
- Never take embarrassing pictures of others using your mobile phones because technology has evolved so much that anyone can retrieve deleted images. The risk of exposing these to a third party is high.
- Never try to hack, gain access or misuse other individuals' social media accounts. Even if you lay hands on someone else's account never publish anything embarrassing targeting him/her. Because anyone can take and keep a snapshot or a screenshot of the article you've published.
- Never act, represent or try to simulate as prominent/popular individuals like actors, politicians etc. using their pictures.
- Never publish pictures, documents or articles destroying someone else's reputation using your social media accounts. Because most of the time these articles are written for personal vendetta. Always look back and think how you would react if this happened to you, your friends or your family.
- Think twice before publishing anything using your social medial accounts. Think about the consequences. Because Internet has its own dark side.

Social media accounts and Internet are there to use for good deeds. Therefore it is best practice never to misuse the power of the Internet. As we all know that power comes with great responsibility.

9 Useful contacts

9.1 Contact for technical assistance

SRI LANKA
CERT|CC
Sri Lanka Computer Emergency Rediness Team
Coordination Centre

Sri Lanka CERT
Sri Lanka Computer Emergency Readiness Team| Coordination Center.
4-112, BMICH, Bauddhaloka Mawatha, Colombo 07, Sri Lanka
Tel: +94 112-691692
Email: cert@cert.gov.lk
Web: www.cert.gov.lk

9.2 Contact for incidents related to child abuse

NCPA
National Child Protection Authority,
No. 330, Thalawathugoda Road,
Madiwela, Sri Jayewardenepura, Sri Lanka.
Tel: +94 11 2 778 911 – 4
Emergency Hotline: 1929
Email: ncpa@childprotection.gov.lk
Web: www.childprotection.gov.lk

9.3 Contact for incidents related to women and child protection

Ministry of Women and Child Affairs
Ministry of Women and Child Affairs,
5th Floor, Sethsiripaya Stage II,
Battaramulla, Sri Lanka.
Tel: +94 11 2186055
Emergency Hotline: 1938
Fax: +94 11 2187249

9.4 Other Contacts

Police internet crime complain center:
http://www.police.lk/index.php/child-a-women- bureau/402-internetcrime-complaint-centre

Police Emergency Division: 119

Emergency Information Service: 118

Government Information Centre: 1919

SRI LANKA CERT | CC

ICTA ideas actioned

Ministry of Telecommunication
and Digital Infrastructure

SUPPORTED BY :

British
High Commission
Colombo

Sri Lanka CERT | CC
Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07.
Tel: +94 11 269 1692 / 269 5749 / 267 9888 Fax: +94 11 2691064
E-mail: cert@cert.gov.lk Web: www.cert.gov.lk

Published August 2017