

IRAQUEER

عیراق کویر

عراق کویر

**Security Guide for LGBT+ Individuals in
Iraq / Kurdistan Region**

INTRODUCTION

The LGBT+ community in Iraq / Kurdistan Region faces extreme danger from the government, the society, armed groups, and others which makes security the biggest concern every LGBT+ individual in country and even activists working on these issues have.

But one of the biggest sources of threats still remains the daily practices of the LGBT+ individuals themselves which increases the risks of them being exposed and face threats.

This guide will be discussing and presenting information and tips to provide resources for the local LGBT+ community to help them increase their physical and digital security.



PHYSICAL SECURITY

Physical security of the LGBT+ individuals remains greatly threatened. With different killing campaigns being organised, random attacks from individuals and groups who are against the LGBT+ community, and the absence of legal protection from a government that often commits the violations, there is only advice that can be given to reduce the chances of facing these threats.

- Change your daily route when going to school, work, or other places
- Surround yourself with individuals you trust in your social circle.
- Identify allies that can support you in case of an emergency.
- Avoid public display of affection even when you think there isn't anyone around.
- Do not meet people you talk to on dating apps and websites before confirming their identities.
- Physical security requires attention to mental security. You can get more help on this in the sexual health guide which can be found on our website.
- Learn self defence techniques if possible.
- Stick to following all the digital safety tips that are provided in this guide which will also protect your physical security.
- Always be aware of your surroundings when talking about certain things that could be considered sensitive.

DIGITAL SECURITY

Given that a large part of the lives of the LGBT+ individuals in Iraq takes place online, ensuring our personal digital securities hold very high importance. The good news is that unlike physical security, there is a lot that can be done to increase our safety measures.

- Protect your login information. Do not share your credentials over emails and always be suspicious of emails asking for personal information.
- Be careful when using public wifi connections. Attackers on the same wifi connection may try to steal your personal information. You can use VPN solutions if you need to use the internet it will help in protecting your information on the public wifi.
- Log out of your accounts after every time you log in.
- Always have a backup way to restore your account which usually can be done by providing another email address, or a phone number.
- Do not sign up for new accounts by using your social media accounts.
- Do not open links that you received from anonymous people or that looks suspicious.
- Delete chat/email/call history that can put you at risk.
- Make sure to clear your browser cache, which can be used to track your navigation history, your navigation preferences and websites accounts.

YOUR DEVICES



Before thinking of any of your accounts, you have to start thinking of securing your devices. They are the main way for you to access your accounts, but they can also be the main reason why you could lose access to these accounts.

- Do not lose sight of your devices. Keep them always with you or in a secure place.
- Disable your location on your devices. Enabling your location makes it easier for others to track you even if you don't share it with them.
- Protect your devices with passwords/pass codes.
- Avoid sharing devices with other people as much as possible.
- Always create a backup for your device's content either by having it on an external hard drive that you can store safely, or by having an online storage account like DropBox.
- Instal antivirus to your computer.
- Do not save files, pictures, or videos that can be used to compromise your safety on your laptop or phone number.

PASSWORD



Having a strong password is one of the most important aspects of securing your digital presence, because the uniqueness and strength of your password determines how easy/difficult it will be for others to have access to your account. The points below are some useful tips that you should keep in mind when choosing your password

- Choose a password that is at least 12 characters.
- Includes caps, symbols, and numbers in your password.
- Use a different password for each account. Using the same password for all makes it easy to get access to all your accounts.
- Don't use personal information like birth date, family names, and others as your passwords.
- Change your passwords frequently. (Every 6 months)

Password Example

Weak
love2omar

Strong
L0v3tw00m@r 321

TWO STEP VERIFICATION



Two Step Verification adds an extra layer of protection to your account. This feature is available in almost all social media and email accounts. In addition to having a strong password, you can turn this feature on which enables your account to send you a text to your phone with a code when you log into your account.

It's important to know that even though it increases the safety measures of your accounts, you still have to make sure that others don't have access to your phones or texts.



There are several email service providers around the world, but gmail remains one of the largest. Protecting your email account is crucial especially because almost all of your other accounts are based on this. The safety measures in gmail are improving each year. To make sure that your email account is protected, keep the following points in mind:

- Create a strong and unique password.
- Activate **Two Step Verification** [here](#).

Other Email Service Providers | Yahoo, Hotmail, others |

While both Yahoo and Hotmail are okay to use, they are still slower in making updates and improving their safety measures comparing to gmail. But both Yahoo and Hotmail also have two step verifications, and if you are using them, you can still follow the digital security measures we recommend in this guide.

facebook

From “**Settings**” you can go to “**Security**” and do the following:

- Activate **Login Alerts** which is a layer of protection that requires access to your phone every time you login into your account from a new device.
- **Code Generator** is a feature that allows you to use your phone to access your account on your other devices.
- **Login Alerts** is a feature that enables you to know whenever any other person tries to access your phone by sending you an email or a text.

Losing access to your phone and/or other devices makes it easier for others to hack your accounts even if you were not logged in into your accounts.

Don't include your location on your profile, and disabled the location to avoid it appearing when posting anything.

When adding content to your page or profile, always check the privacy settings to avoid making public a post that you wanted to share only with trusted friends.

You can hide your email, birthday, and other personal info from your friends and others who visit your profile. This makes it hard for hackers to access your account.



- Don't lose access to your login information (Email + Password).
- Create a unique & strong password.
- Make your account private.
- Activate two step verification [here](#)



- Don't lose access to your login information (Email + Password).
- Create a unique & strong password.
- Make your tweets private / protected
- Verify login requests / TwoStepVerification [here](#)



- Don't lose access to your login information (Email + Password).
- Create a unique & strong password.
- Make your account private.
- Activate login verification [here](#)



Jitsi is a safe and encrypted website/app that can be used to make voice and video calls. It's available for android, OS, and Linux. You can either download it on your device, or use it directly from the website www.jitsi.org. The privacy of users is ensured since using jitsi does not need an account.



Signal is an app that can be used to text, share files and make calls safely. It's safer than most apps. It requires a phone number, but no need for any personal information. Your data and chat are all private, and not accessed by the service provider.



Telegram is a safe and encrypted texting app for windows, android, and OS devices. It can be protected even more by activating the passcode lock, two step verification, and creating a secure chat which can destroy the chat history after a specific period of time that you control. You can also activate two step verification [here](#)



Whatsapp is becoming safer, but there are safer options.



We do not recommend viber.



We do not recommend Skype.



Even though Kik doesn't need your number, but it's easy to track your location.



MANJAM

SCRUFF™

Dating apps like Grindr, Tinder, Scruff, Hornet and others are widely spread and used in Iraq/KurdistanRegion. Even though it represent a good way to express sexuality and communicate with others who know what we go through and look for, it is also used by other groups that take advantage of the app to target LGBT+ individuals with violent attacks.

manjam.com is also one of the most popular dating websites for LGBT+ individuals in Iraq. It's also heavily used to target members of the queer community.

When using this app or websites, it's crucial to verify the identity of the person(s) you talk to before you meet them. Do not activate your location, and share as little information as possible.

You should also make sure you don't lose access to your login information, and that you have a strong password.

When meeting new people, try to meet them in a public location in the beginning to establish a sense of what kind of person you're meeting.

IRAQUEER

عراق كوير

عراق كوير

About IraQueer

IraQueer is a registered human rights nonprofit that focuses on the LGBT+ community in Iraq/KurdistanRegion. IraQueer envisions an Iraq where the LGBT+ community is recognised and enjoy equal rights and responsibilities to the ones other individuals have. IraQueer's mission is to empower the LGBT+ community in Iraq/KurdistanRegion through raising awareness and capacity building, and strengthen the LGBT+ community to lead the first queer movement in Iraq/KurdistanRegion's public history.

info@iraqueer.org
+46762383076 | WhatsApp & Viber
www.iraqueer.org

Find IraQueer on
Facebook | Twitter | Instagram |
Snapchat | LinkedIn | Youtube