



# Online Safety Guide

*for the* LGBTQ+ **Community in Uganda**



[www.lwuga.org](http://www.lwuga.org) 🔍



Reach us freely on  
**+256-800322224**



# Introduction:

In today's digital age, the use of dating apps and online platforms has become increasingly popular, offering avenues for individuals to connect and build relationships. However, amidst this convenience lies a growing danger, particularly for the LGBTQ+ community in Uganda. Cases of blackmail, extortion, and violence targeting queer individuals through queer dating apps have been on the rise, leading to grave consequences.

At Let's Walk Uganda, we recognize the urgent need to address this alarming trend and empower the community with the knowledge and tools to stay safe in the online realm. Our Online Safety Guide is designed to raise awareness about the risks faced by queer individuals on dating apps and provide essential guidance on how to navigate these platforms securely.



Through this guide, we aim to shed light on the tactics employed by perpetrators, such as fake accounts, entrapment, and extortion, to target and harm queer individuals. We will offer practical tips, best practices, and resources to help you protect yourself, recognize warning signs, and respond effectively to potential threats.

It is crucial to remember that everyone has the right to safety, respect, and dignity, both online and offline. By equipping yourself with knowledge and awareness, you can reduce the risks associated with online interactions and safeguard your well-being.

Join us in taking a stand against online exploitation and violence. Let us work together to create a safer and more inclusive digital space for all members of the LGBTQ+ community in Uganda. Together, we can build a future where every individual can express themselves freely and authentically without fear or discrimination.



# Problem Description:

In Uganda, the use of dating apps and online platforms by the queer community has become increasingly dangerous due to the rising cases of blackmail and entrapment orchestrated by perpetrators working in collusion with the police. Perpetrators employ deceptive tactics by creating fake accounts on well-known queer dating apps like Romeo, Grindr, and Tinder using false identities, including fake names, ages, and pictures. These fake accounts are used to initiate conversations with queer individuals on the app to entrap them.

Once a queer individual falls victim to the scheme and agrees to meet the person from the fake account, they are subjected to a vicious cycle of violence, blackmail, and extortion. Perpetrators often work in groups, collaborating closely with law enforcement officials to orchestrate these entrapment operations. Upon meeting the individuals, the queer person is ganged up on, physically assaulted, and subsequently arrested by the police, or other security agencies.

The victims are denied their basic rights, including legal representation, and are coerced into paying bribes to the police in exchange for their release. This pattern of abuse and extortion not only violates the rights of queer individuals but also perpetuates a climate of fear and intimidation within the community.

To address this growing problem, Let's Walk Uganda recognizes the urgent need to develop an online safety guide to raise awareness and educate the community on how to identify and avoid falling victim to these malicious schemes. The guide will provide crucial information on recognizing red flags, verifying identities on dating apps, and taking precautions to ensure personal safety while engaging with online platforms. By empowering individuals with the knowledge and tools to protect themselves, Let's Walk Uganda aims to combat the exploitation and violence perpetrated against the queer community in Uganda.

# Definition of terms

**Extortion:** The act of obtaining something, typically money, through force, threats, or intimidation. In this context, it refers to the police or others demanding payment or favours from queer individuals in exchange for their release or other rights.

**Two-Factor Authentication (2FA):** A security process that requires users to provide two different authentication factors to verify their identity before gaining access to an online account. It helps to enhance account security by adding an extra layer of protection.

**Mob-Justice:** Vigilante justice carried out by a group of people without legal authority. In this case, it refers to queer individuals being targeted, beaten, and arrested by a group of people acting outside the law.

**Sexual Harassment:**

Unwanted or unwelcome behavior of a sexual nature that makes a person feel uncomfortable, intimidated, or offended. Queer individuals may face sexual harassment in various forms, including online interactions.

**Torture:**

The act of inflicting severe physical or psychological pain or suffering on someone as a form of punishment or to extract information. In this context, it could refer to the mistreatment of queer individuals by the police or others.





**Forced anal examination:** A medically unnecessary and invasive procedure in which a person's anus is examined without their consent, often used to "prove" or determine a person's sexual orientation. It is a violation of human rights and is not supported by medical evidence.

**Forced Nudity:** The act of being made to undress against one's will, often used as a form of humiliation, control, or abuse. Queer individuals may be subjected to forced nudity as a means of intimidation or coercion.

**Catfishing:** This term refers to the act of creating a fake online persona to deceive someone into a relationship, typically for personal gain or malicious intent.



**Blackmail:**

The practice of demanding money or other forms of payment from someone in exchange for not revealing compromising or damaging information about them.

**Entrapment:**

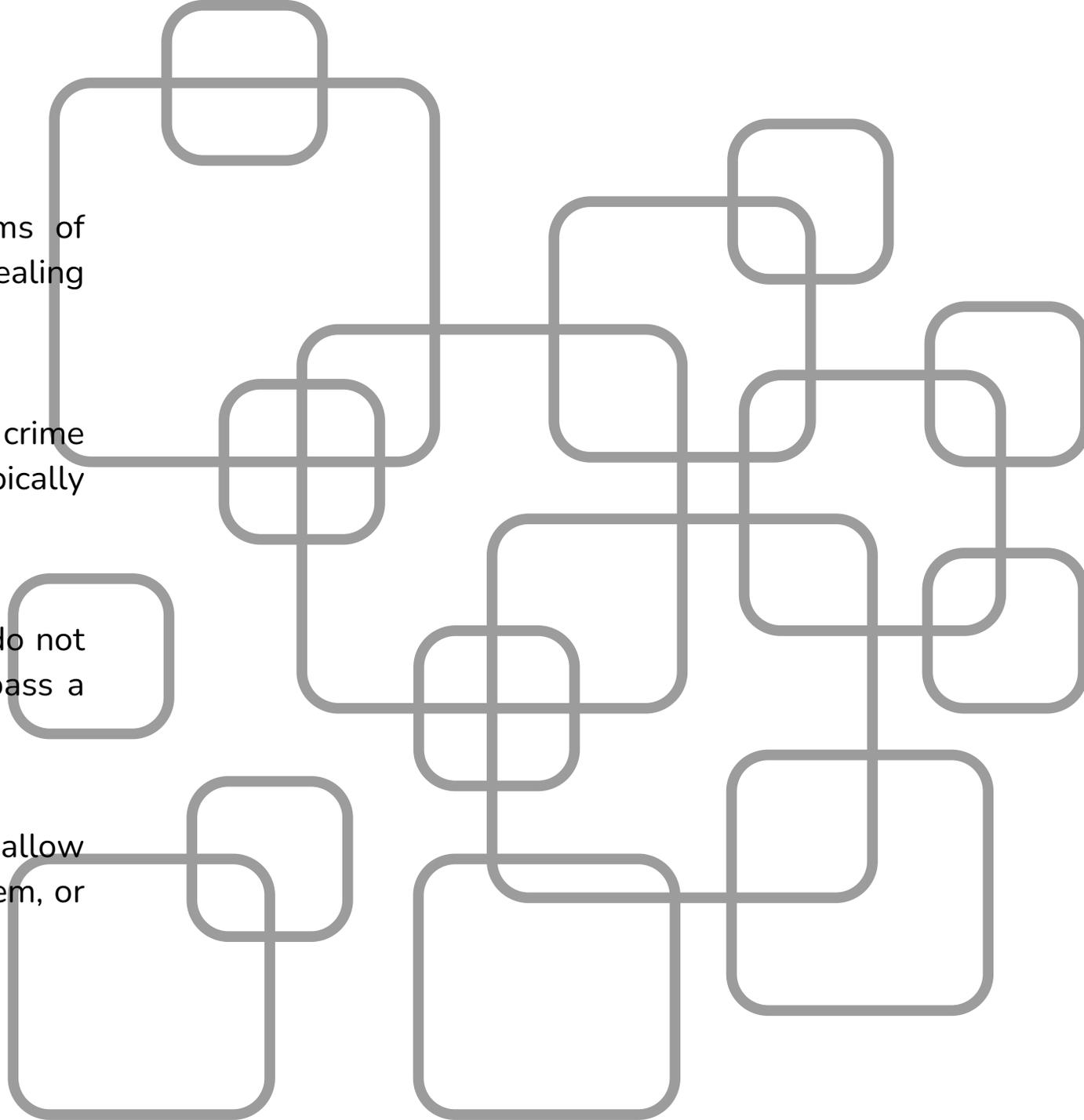
The action of luring an individual into committing a crime they would not have otherwise committed, typically through deceit or coercion.

**Queer**

An umbrella term used to describe individuals who do not identify as heterosexual or cisgender. It can encompass a range of sexual orientations and gender identities.

**Privacy Settings:**

Tools and features offered by online platforms that allow users to control who can see their profile, contact them, or access their personal information.





### **Red Flags:**

Warning signs or indicators that suggest a potential threat or danger, such as inconsistencies in someone's online profile, requests for money, or pressure to meet in person quickly.

### **Consent:**

The principle of giving permission or agreement for something to happen, especially in the context of online interactions, meetings, or sharing personal information.

### **Cybersecurity:**

Measures taken to protect electronic devices, networks, and data from unauthorized access, cyberattacks, or data breaches.

### **Reporting Mechanisms:**

Procedures and channels available for reporting suspicious or abusive behavior on online platforms to platform administrators.



# THE RISKS AND POTENTIAL CONSEQUENCES OF FALLING VICTIM TO THESE SCHEMES:

## **Exposure to Mob Justice:**

The victims in most cases are exposed to Mob justice, especially in cases of meeting in busy areas or when the victim resists the malicious acts of the perpetrator

## **Physical Harm and Violence:**

Victims have been exposed to physical harm, beatings, and serious injuries.

## **Theft of Personal Property:**

The Victims are often vulnerable to theft of personal belongings, such as phones, cash and other valuables.

### **Public Sexual Harassment:**

Some Victims have faced public sexual harassment like forced Nudity and genital checks in public and most cases in the presence of Cameras.

### **Arrest and Detainment:**

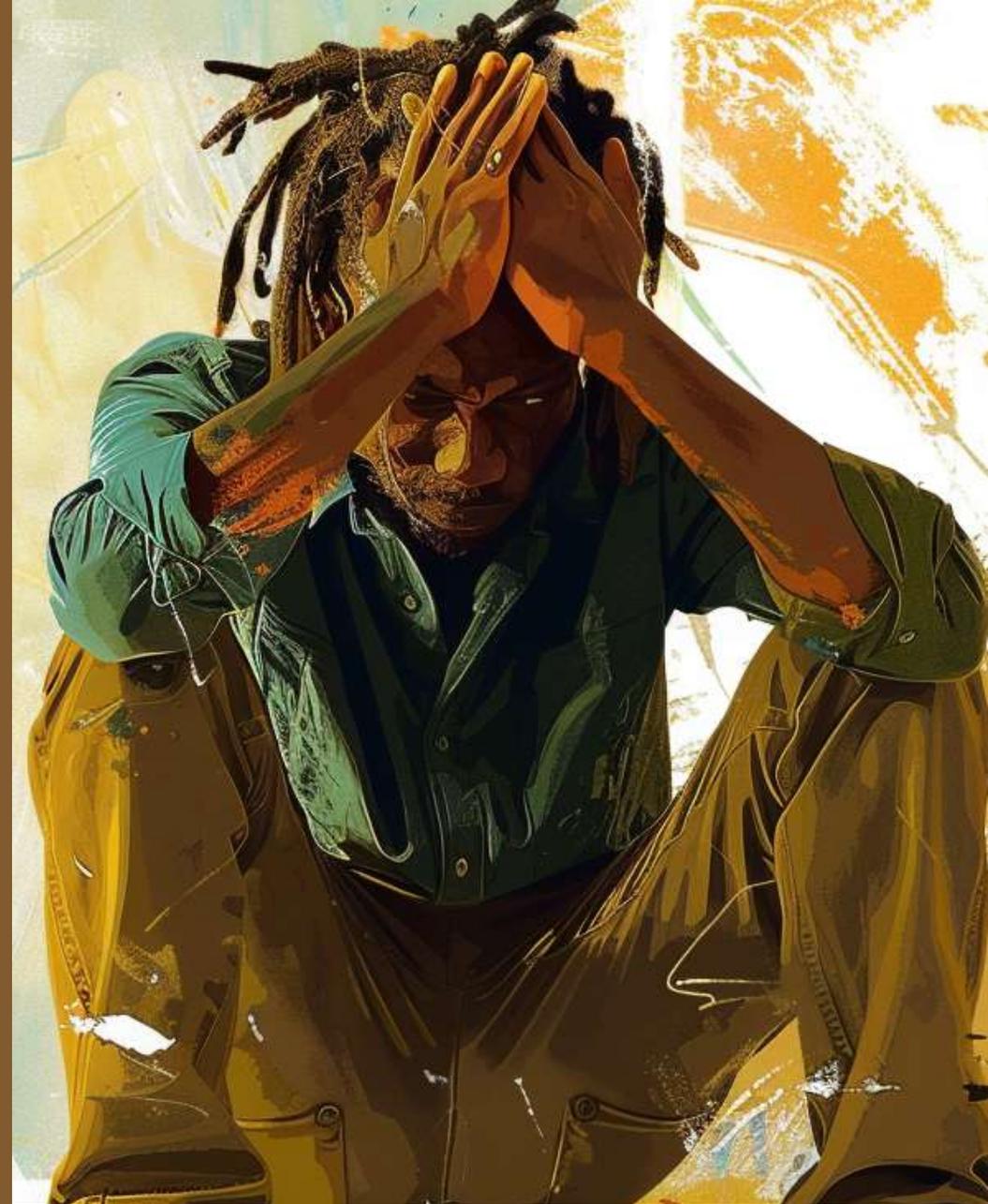
The perpetrators work with law enforcement like police hence the victims are likely to face unjust arrest, detention, and legal complications.

### **Torture and Forced Examinations:**

The victim will likely be tortured, and taken through forced anal examinations, and other violations of human rights.

### **Denial of Rights and Access to Legal Representation:**

Victims may be denied their rights, including access to legal representation and due process, leading to further exploitation and abuse.

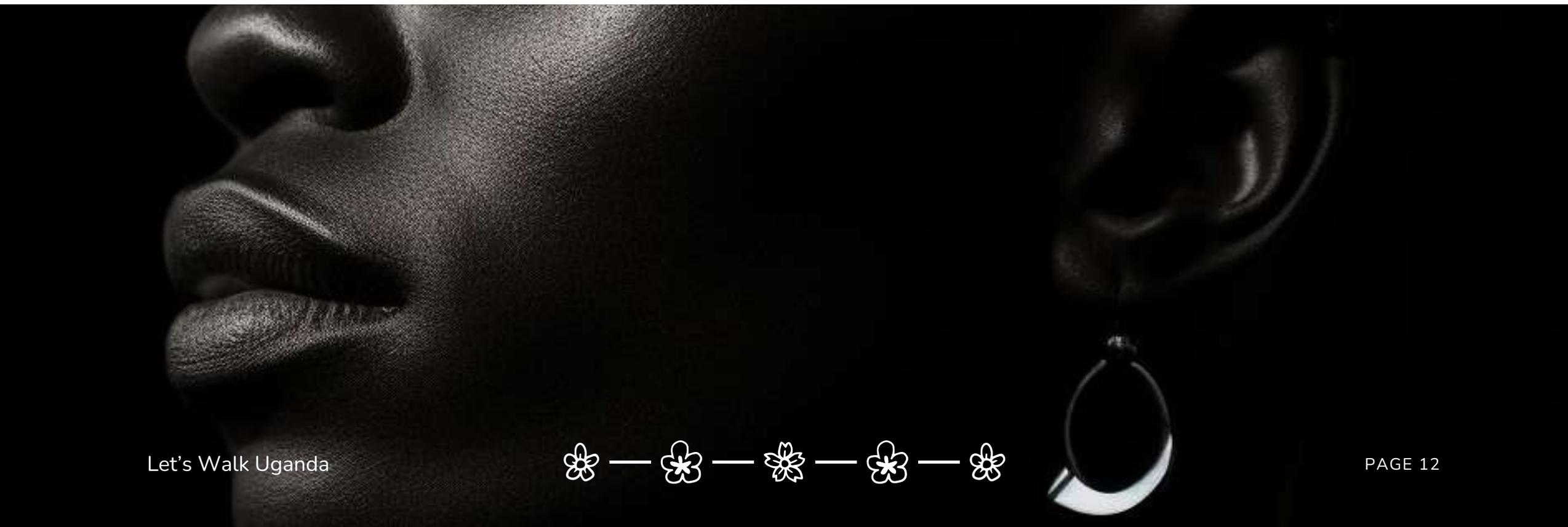


**Extortion:**

Perpetrators may extort money or other valuables from the victim in exchange for release or safety.

**Long-Term Effects and Trauma:**

Experiencing such traumatic events can have long-lasting effects, including post-traumatic stress disorder (PTSD) and emotional distress.



# Safety tips for using dating apps:

- Interact with verified accounts: Look for dating profiles with verification badges or accounts that have been confirmed by the platform.
- Avoid accounts with limited information: Be cautious of profiles that have very little information or only a few pictures. Genuine users typically provide more details about themselves.
- Verify photos through video calls: Before meeting someone in person, consider having a video call to confirm their identity and ensure they match their photos.
- Chat for a longer time before meeting: Take the time to get to know the person through conversations before deciding to meet them in real life.
- Avoid sharing sensitive information: Refrain from sharing personal details like your address, financial information, or other sensitive data with someone you've just met online.

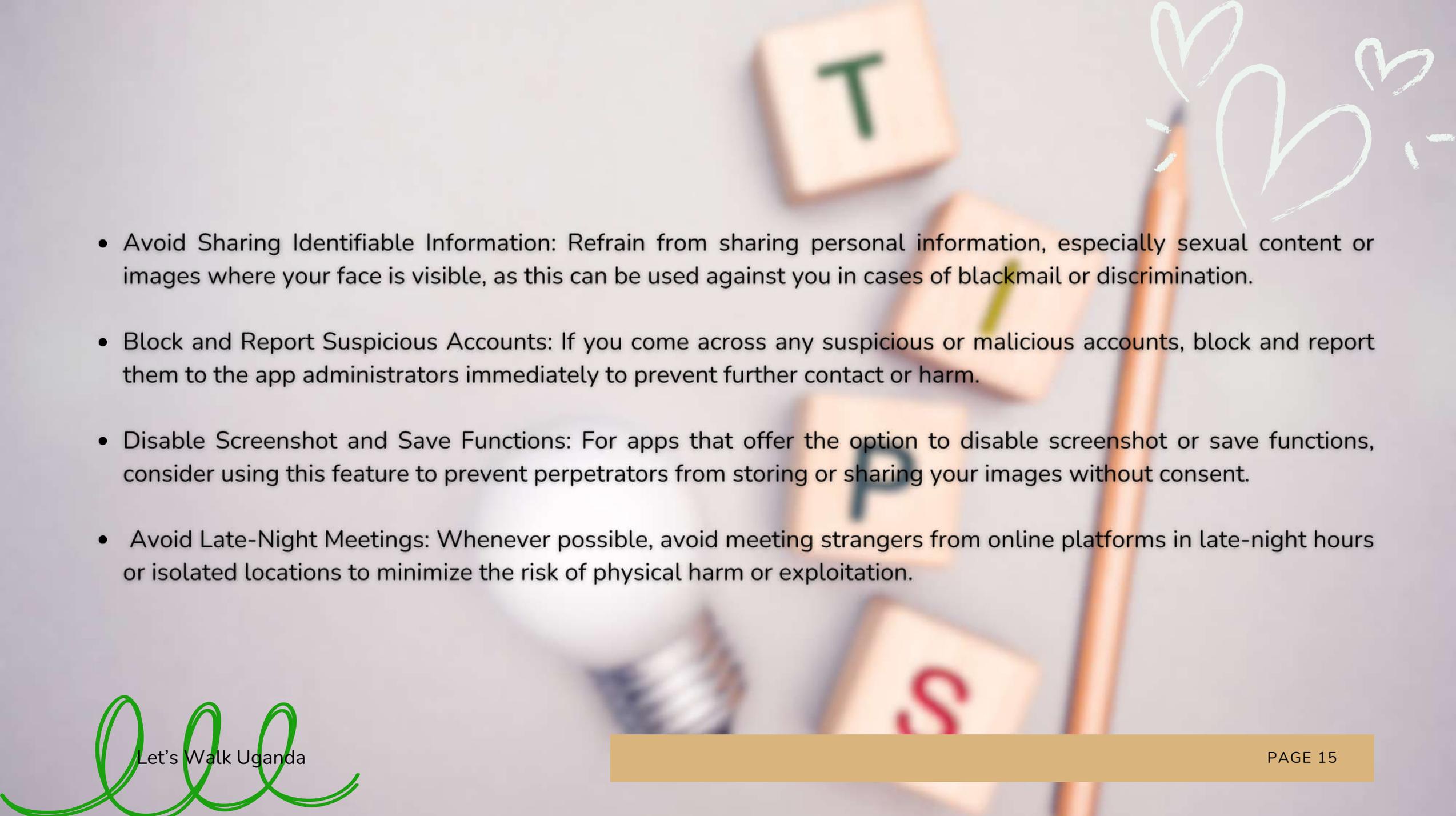




Let's Walk Uganda

- Inform a friend before meeting: Let a trusted friend or family member know about your plans to meet someone from a dating app. Share the person's profile and location details.
- Meet in secure public places: Choose meeting spots that are well-lit, populated, and secure, such as cafes, restaurants, or public parks. Avoid isolated or secluded locations.
- Arrive early and observe the situation: Arrive at the meeting place slightly earlier than the agreed time to scope out the surroundings and ensure your safety before the other person arrives.
- Trust your instincts: If something feels off or uncomfortable during your interactions with someone online, trust your gut feeling and consider ending the communication or meeting.
- Report suspicious activities: If you encounter any suspicious behavior or feel threatened while using a dating app, report it to the platform's support team.
- Read and Understand Community Guidelines: Take the time to read and understand the community guidelines and warnings issued by app developers regarding potential risks in specific countries or regions, including Uganda.



- 
- **Avoid Sharing Identifiable Information:** Refrain from sharing personal information, especially sexual content or images where your face is visible, as this can be used against you in cases of blackmail or discrimination.
  - **Block and Report Suspicious Accounts:** If you come across any suspicious or malicious accounts, block and report them to the app administrators immediately to prevent further contact or harm.
  - **Disable Screenshot and Save Functions:** For apps that offer the option to disable screenshot or save functions, consider using this feature to prevent perpetrators from storing or sharing your images without consent.
  - **Avoid Late-Night Meetings:** Whenever possible, avoid meeting strangers from online platforms in late-night hours or isolated locations to minimize the risk of physical harm or exploitation.



## DIGITAL SECURITY AND PRIVACY TIPS:

- Use Strong Passwords: Create unique and complex passwords for all your accounts to prevent unauthorized access. Use a mix of letters, numbers, and special characters.
- Enable Two-Factor Authentication: Add an extra layer of security to your accounts by enabling two-factor authentication (2FA) where available. This will require a second form of verification, such as a code sent to your phone, in addition to your password.



- **Avoid Unsecure Public Wi-Fi Networks:** Public Wi-Fi networks can be vulnerable to hackers. Avoid accessing sensitive information, such as dating apps, when connected to unsecured public Wi-Fi.
- **Secure Your Devices:** Set strong passwords or use biometric authentication like face or fingerprint recognition to lock your devices. This can help protect your personal data in case your device is lost or stolen.
- **Be Cautious with Password Sharing:** Do not share your passwords with anyone, especially untrusted individuals. Keep your passwords confidential to maintain account security.
- **Keep Software Updated:** Regularly update your devices and apps to ensure you have the latest security patches and protections against vulnerabilities.

- Beware of Phishing Attempts: Be cautious of suspicious emails, messages, or websites that may be phishing attempts to steal your information. Avoid clicking on links or providing personal details to unknown sources.
- Avoid Entering Sensitive Information on Suspicious Websites: Be cautious when entering sensitive information like bank details on websites. Ensure the website is secure (look for "https://" in the URL) and legitimate before providing any personal data.
- Log Out After Using Devices: Always log out of your accounts, especially on shared or public devices, to prevent unauthorized access to your information.





## EMERGENCY CONTACTS AND RESOURCES:

[lwuganda@gmail.com](mailto:lwuganda@gmail.com)

[www.lwuga.org](http://www.lwuga.org)

+256-200902700

+256-800322224



[www.lwuganda.org](http://www.lwuganda.org) 

Let's Walk Uganda

Reach us freely on  
 **+256-800322224**



Let's Walk Uganda

THEEZAQ  
Where Art Meets Design™