HUMAN RIGHTS WATCH

secure our SOCIALS
نحو منصّات آمنة

LGBT People Should Feel Secure Online **Awareness Tips**

Government officials across the Middle East and North Africa (MENA) region are targeting lesbian, gay, bisexual, and transgender (LGBT) people based on their online activity on social media. Security forces and private individuals use social media posts to identify and target LGBT people and activists for harassment, blackmail, threats, and censorship. Security forces have entrapped LGBT people on social media, subjected them to online extortion, online harassment, and outing, and have forced access to their mobile devices and social media accounts and relied on illegitimately obtained digital photos, chats, and similar information in prosecutions.

To learn more about online targeting and its offline consequences read the full report and watch the videos by Human Rights Watch (HRW).

Social media companies should do more to protect users from online attacks, including LGBT people in the MENA region. While the responsibility for better digital security falls on companies, there are some steps you can take to better protect yourself online. It is important to note that people's threat models are different and vary based on several factors, including age, location, race, gender, socioeconomic background, as well as sexual orientation and gender identity.

While not intended to be a comprehensive list, here are some steps to consider for your privacy and safety based on HRW's investigation findings and recommendations. These awareness tips have three parts:

1. Signs of a Potentially Malicious Account or Activity
2. Mitigating the Consequences of Digital Targeting
3. Resources

01 Signs of a Potentially Malicious Account or Activity: **Am I Being Digitally Targeted?**

We outline below some indicators and awareness tips that may allow you to establish a baseline for assessing whether you might be targeted digitally. While the behavior outlined below may not be malicious and does not always indicate you are being targeted, our research pertaining to LGBT people's online experiences in the MENA region identifies some of the following patterns as common practices preceding to digital targeting:

Their Profile

- Their profile is freshly created, and its details are ambiguous or scarce. Some platforms such as Facebook and Instagram allow you to see when an account was created.
- A profile claiming to be a friend is asking you questions the friend should already know, such as identifying information, residence location, and sexual orientation or gender identity.

Personal Information

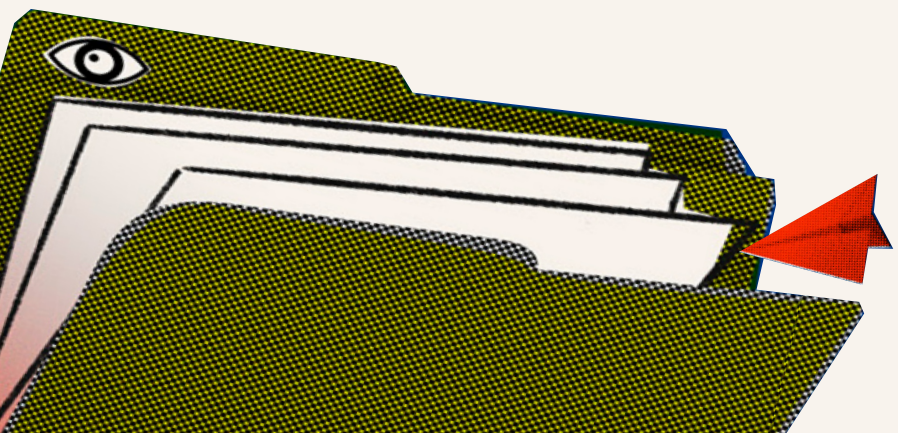
- You are immediately told highly personal information and asked to share the same.
- You are not currently engaging in sex work, but they ask you how much you charge in exchange for sex.
- You are not currently engaging in drug use, but they ask you if you use or have drugs.
- They ask for your phone number before you are sure of their identity.

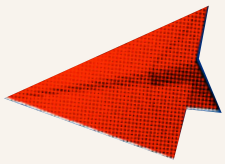
Photo and Video

- You are immediately asked to send photos, including nude images of yourself or others.
- You are immediately asked to have "cybersex."

Meeting Location

- They ask you to meet in a new or unfamiliar location, such as a private residence.
- You meet in a public place, and they insist on a public display of affection, including touching or kissing, after you have expressed discomfort.
- There are other unexpected people at the meeting.





02 Mitigating the Consequences of Digital Targeting: **What Can I Do?**

Here are some steps you can take to protect your online account and reduce the risks and impact of being digitally targeted:

Photo and Video

- Ask them to share a picture with you and then check it via reverse image search.
- Ask them to send you a 5 second video or video call so you can see their face.
- Avoid sending photos that show your face or other identifiable features, including identifying landmarks visible in the background, on or through pseudonymous profiles to profiles you don't know or trust.
- Delete photos and videos from your personal phones after sharing them.
- If you are using WhatsApp to send photos, use the *view once* option. This will prevent others from taking a screenshot of your photo.

Personal Information

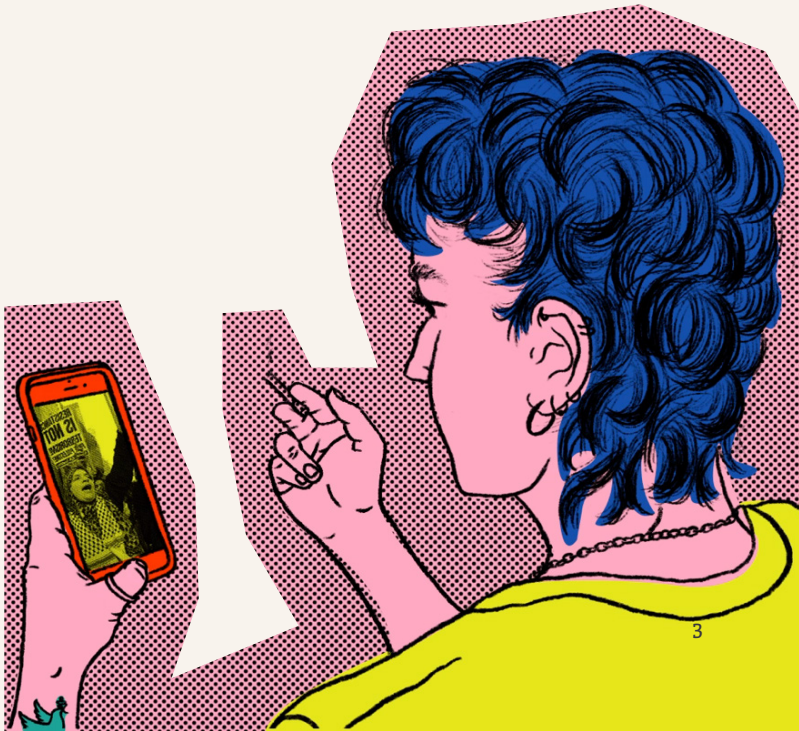
- Avoid sending personal information about your location, workplace, or family.

Profile

- Check their profiles on other social media platforms to verify their identity.
- Consider creating a separate dating application account that does not link to your social media application profiles and does not use your real name for sharing your sexual orientation or gender identity.
- Review your privacy settings so that your social media profiles, posts, and location are only visible to those you want to share them with.

Meeting Location

- Meet them in a neutral public place.



02 Mitigating the Consequences of Digital Targeting: **What Can I Do? Cont.**

Data and Device Security

- Enable two-factor authentication for all your accounts.
- Use strong passwords or passphrases and a secure password manager.
- Disable face and fingerprint logins.
- Disable screen notifications for apps that might contain sensitive information (dating apps, chat apps, etc.).
- Utilize features that allow you to disguise or cloak certain applications on your phone, such as this feature from Grindr which makes your app icons discreet.
- Use messaging apps with end-to-end encryption such as Signal and WhatsApp.
- Use disappearing messages, the *view once* option or set your messages to auto-delete.
- Use a reputable VPN, especially when using a public Wi-Fi hotspot such as at coffee shops or airports.

First Responses to Digital Targeting

- If you experience entrapment, which includes law enforcement's impersonation of LGBT people on social media and dating applications to meet and arrest unsuspecting LGBT users, by someone you've met online, take a screenshot to preserve evidence, then block the account and report the incident directly to the relevant platform.
- Seek immediate psychosocial support, if it is available, through trusted individuals or groups.
- After you take a screenshot to preserve evidence, archive it elsewhere, and delete all records of interaction with the person, including photos and chats on your device.
- If targeted on social media, deactivate all social media accounts.
- If you are at risk of arrest as a result of digital targeting, leave your phone in a safe place, if possible.
- Report immediately to a relevant helpline (see Resources).

What Can I Ask Social Media Companies to do to Help Secure Accounts Online?

The #SecureOurSocials campaign is calling on Meta platforms, Facebook and Instagram, to be more accountable and transparent on user safety by publishing meaningful data on its investment in user safety, including content moderation. You can join the call by emailing Meta executives directly on www.hrw.org/SecureOurSocials

03 Resources
Want to learn more?

There are some excellent guides that provide comprehensive tips for steps you can take to protect your privacy and security online. There are also some helplines operated by civil society groups in Arabic, English, and French, that you can reach out to if you require more guided support. See:

Guides

- EFF
  - https://ssd.eff.org/
- Data Detox Kit
- Wirecutter
- Grindr's Holistic Security Guide
- Glitch Charity Documentation Guide
- GLAAD Digital Safety Guide
- Online Harassment Field Manual

Help Lines

- Access Now Helpline
- Social Media Exchange (SMEX) Helpline
- Helem Helpline