#CHAPTERTHON2021

#DIGITALINCLUSIONUG

DIGITAL SECURITY TRAINING FOR PEOPLE WITH DISABILITY IN UGANDA

Date: 27th August 2021
Venue: Ministry of ICT Computer Lab

Encrypt
UGANDA

ABOUT ENCRYPT UGANDA

ABOUT ME

- Digital Rights Organization on a mission to empower and equip different groups of people with the knowledge and skills needed to overcome digital security and safety threats
- Based in Kampala (Uganda)

- Gole Andrew
- Digital Security Trainer and Consultant
- Project Manager at Encrypt Uganda

INTRODUCTION TO DIGITAL SECURITY

Digital Security is the protection of one's digital personality, as it represents the physical identity on the network you are operating on or the internet service in use. Digital Security includes the tools which one uses to secure his/her identity, assets, and technology in the online and mobile world.

DIGITAL TRENDS IN UGANDA IN 2020

TOTAL POPULATION	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	MOBILE CONNECTIONS
45.01	**10.67**	**2.50**	**26.83**
MILLION	MILLION	MILLION	MILLION
URBANISATION	PENETRATION	PENETRATION	VS. POPULATION
24%	**24%**	**5.6%**	**60%**

COMMON DIGITAL THREATS FACED BY PERSONS WITH DISABILITY

- CYBER BULLYING
- ONLINE HARASSMENT
- DOXING
- HATE SPEECH

- TROLLING
- INTIMIDATION/ THREATS
- PUBLIC SHAMING

HOW TO KEEP SAFE ON SOCIAL MEDIA

No.

1

Protection from Hate speech

No. **3**

Protection from harassment

[DISCUSS] 15 mins

1. Have you experienced any abusive content on Social Media?
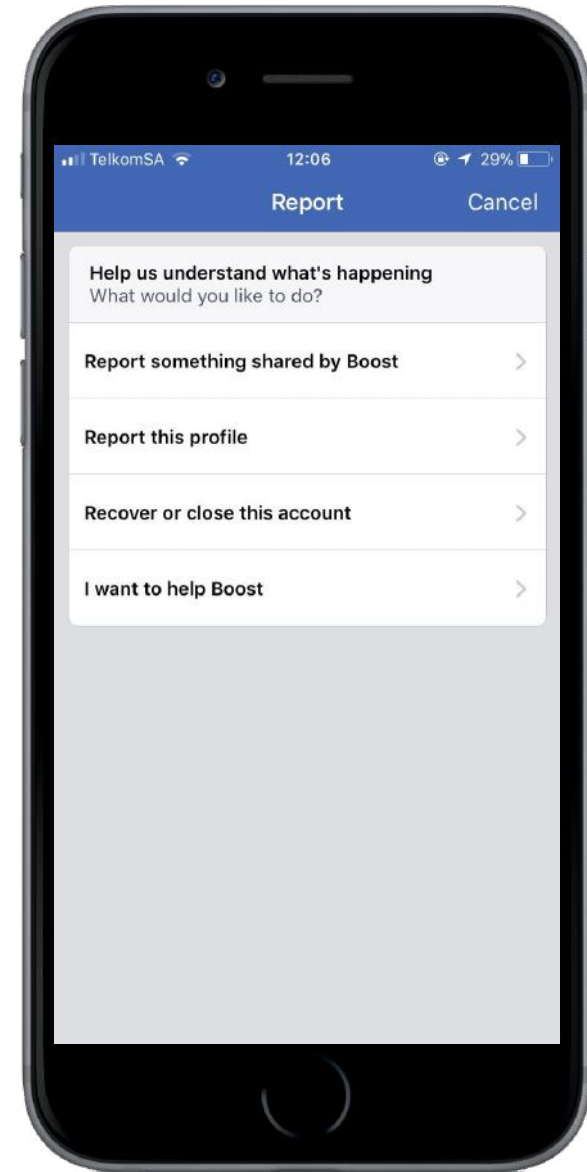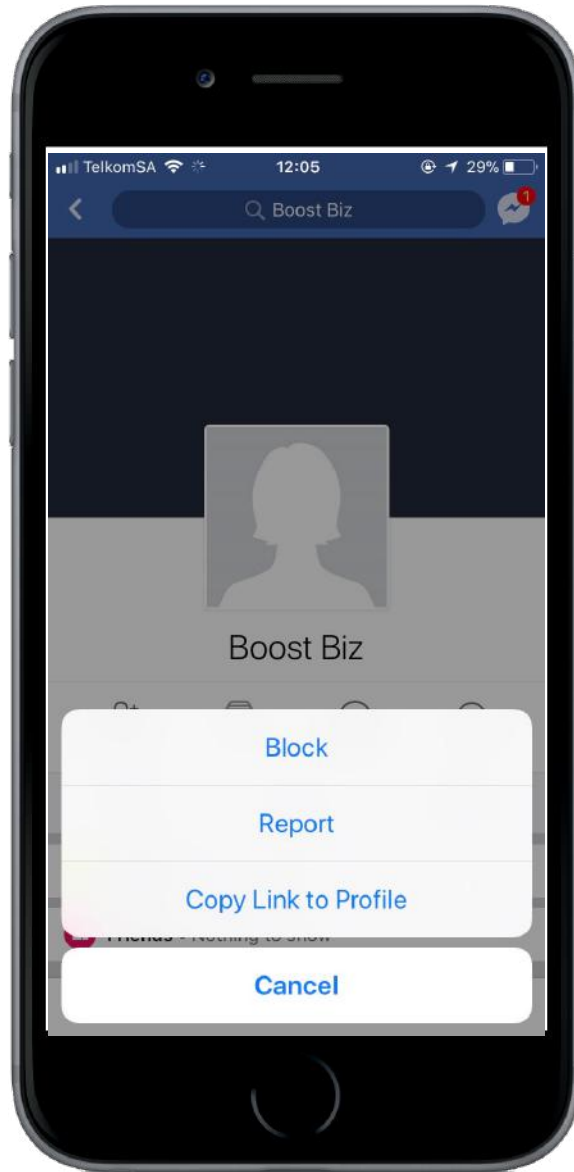2. What did you do when you experienced this?
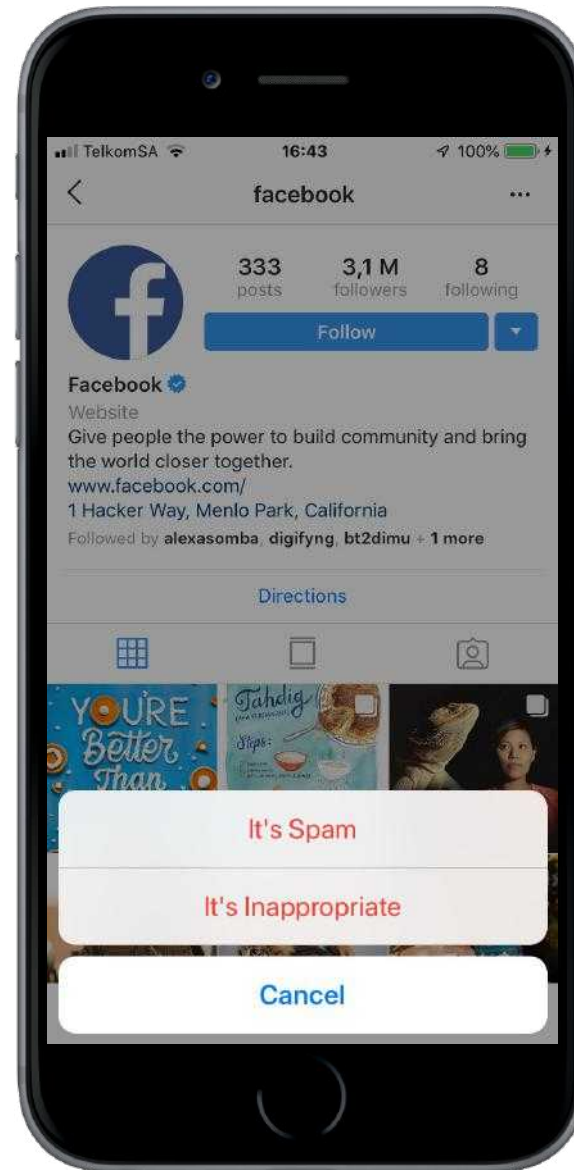
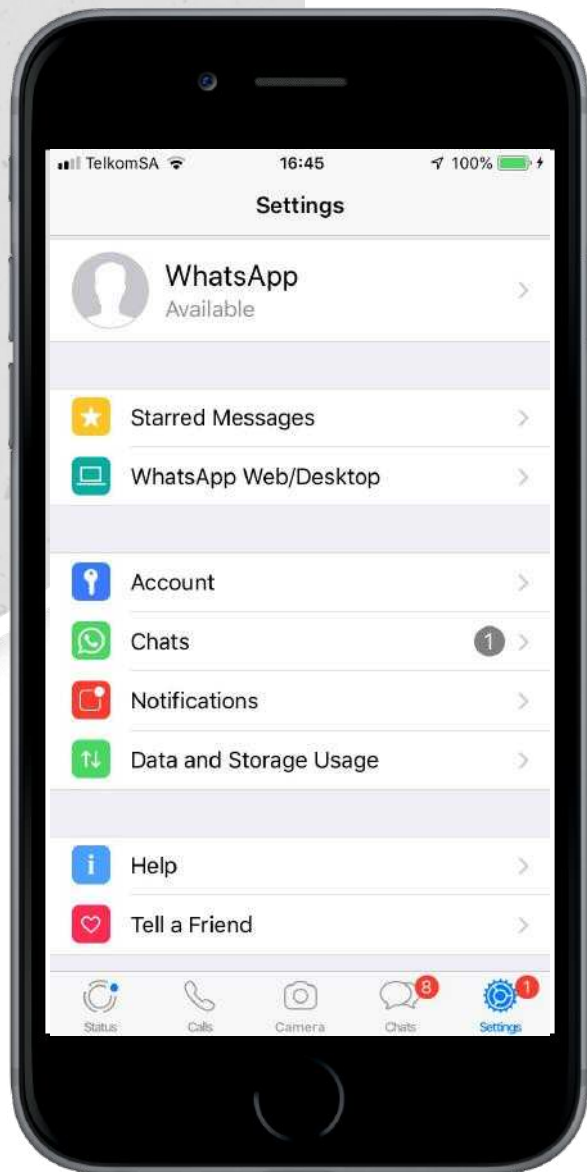Harassment and Reporting on Facebook, Instagram and WhatsApp
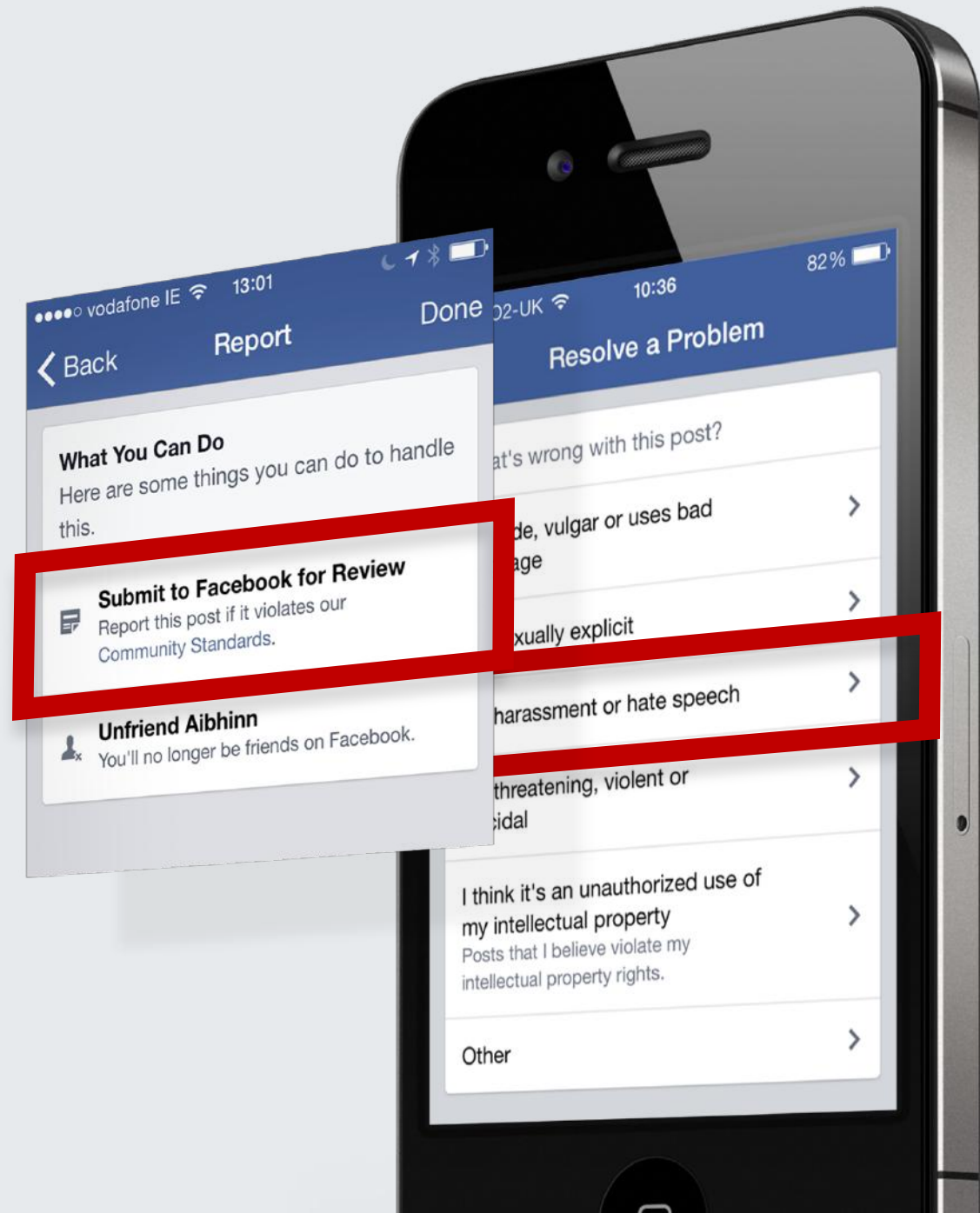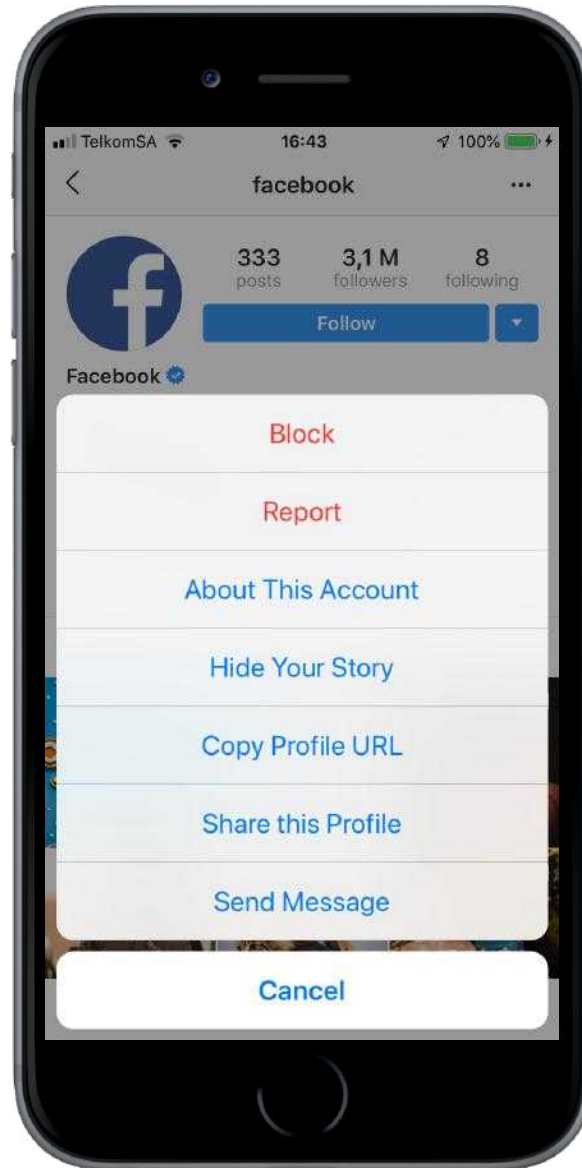
Banning and Removing on Facebook
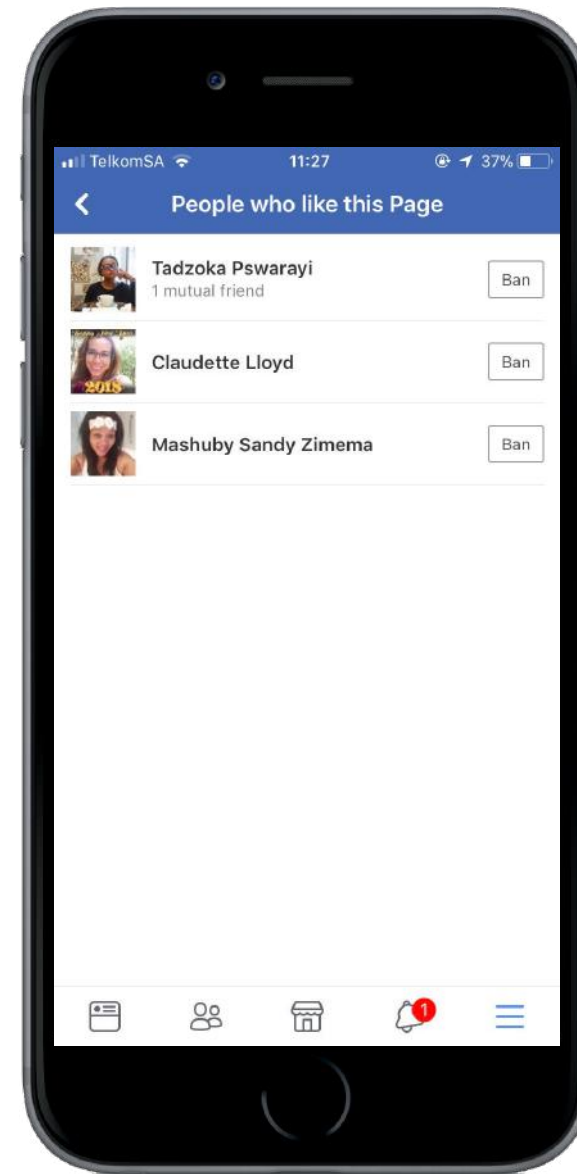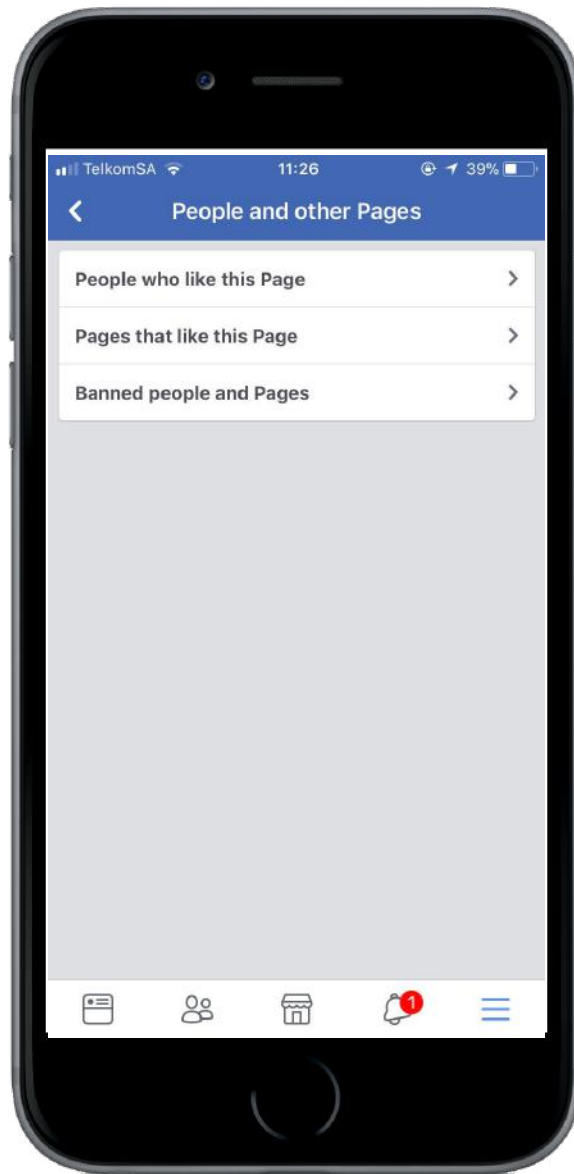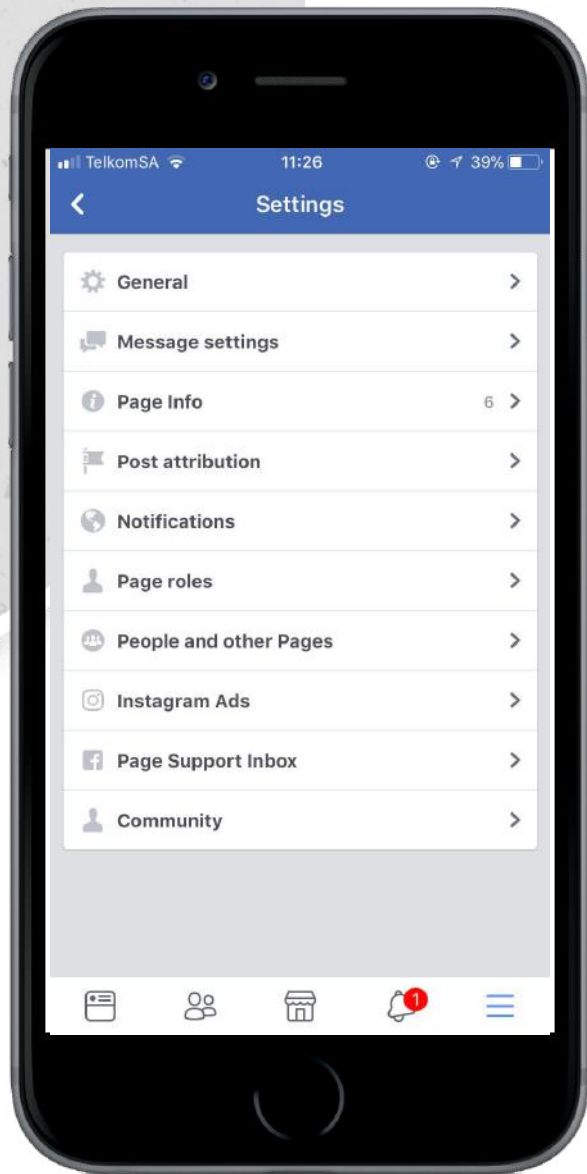
Reporting a profile on Facebook

Reporting a profile on Instagram

Reporting on WhatsApp
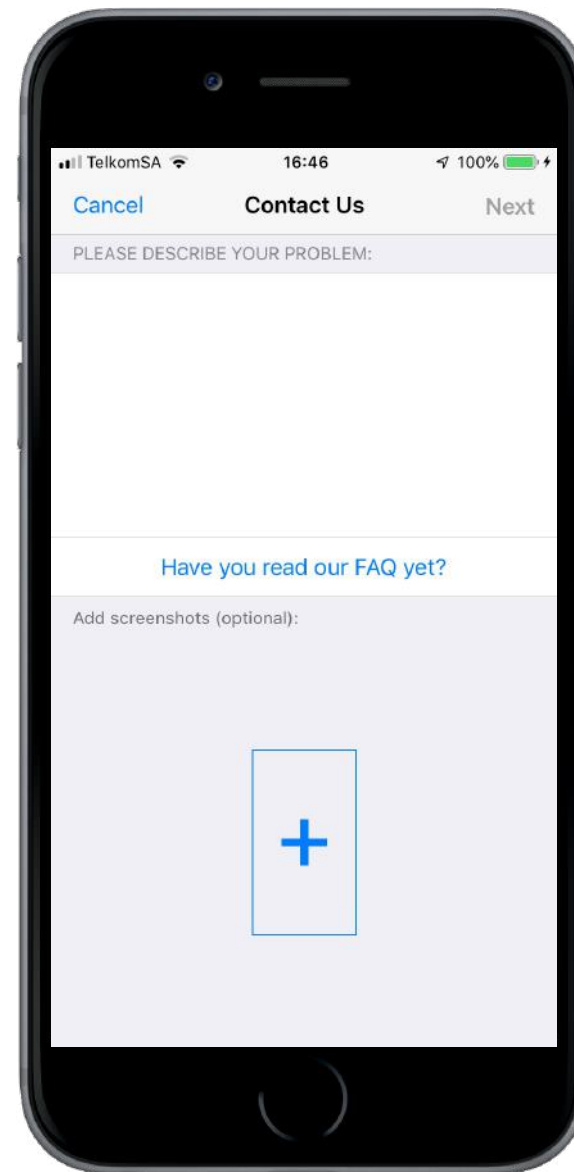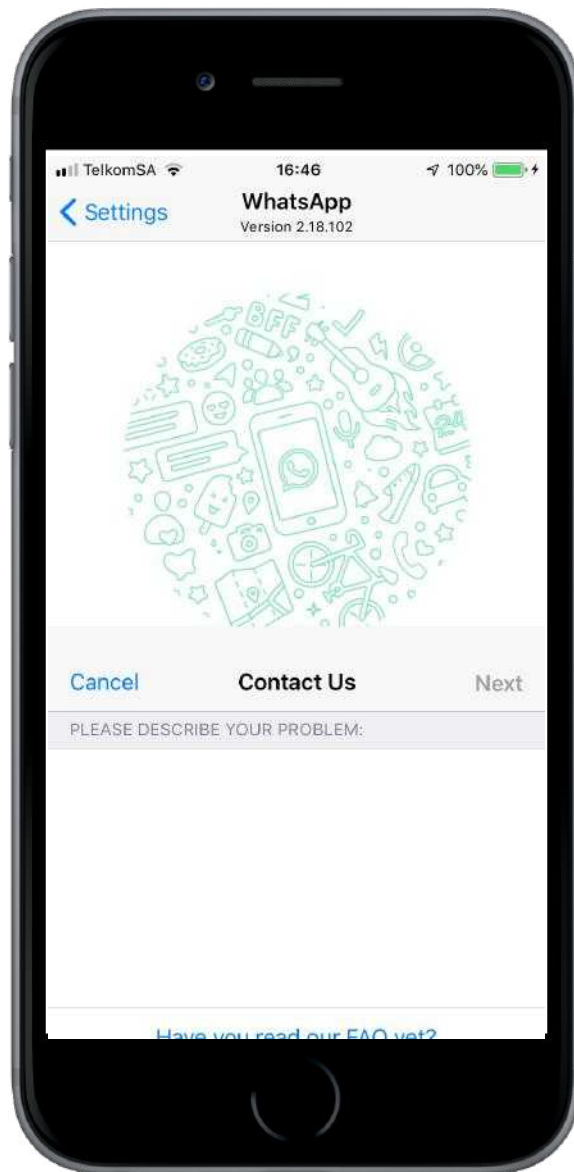
Unfollowing and Blocking
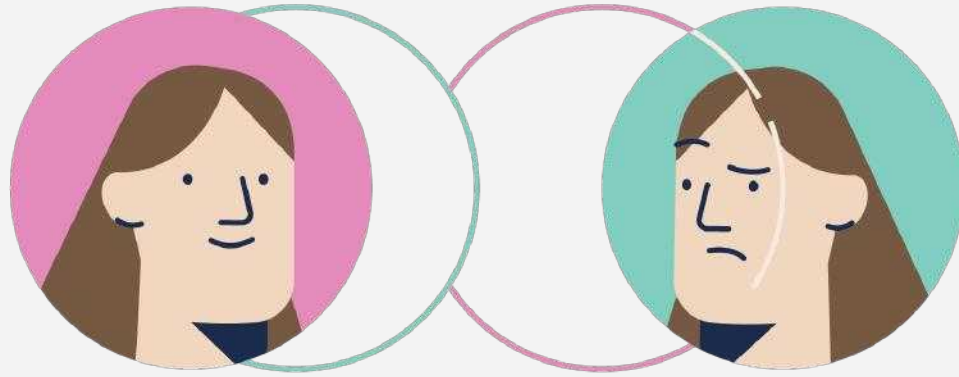
Blocking words from appearing on your page

Managing Online Harassment

Preventing Harassment

1 | Preventing Unwanted Contact

2 | Ignoring Messages
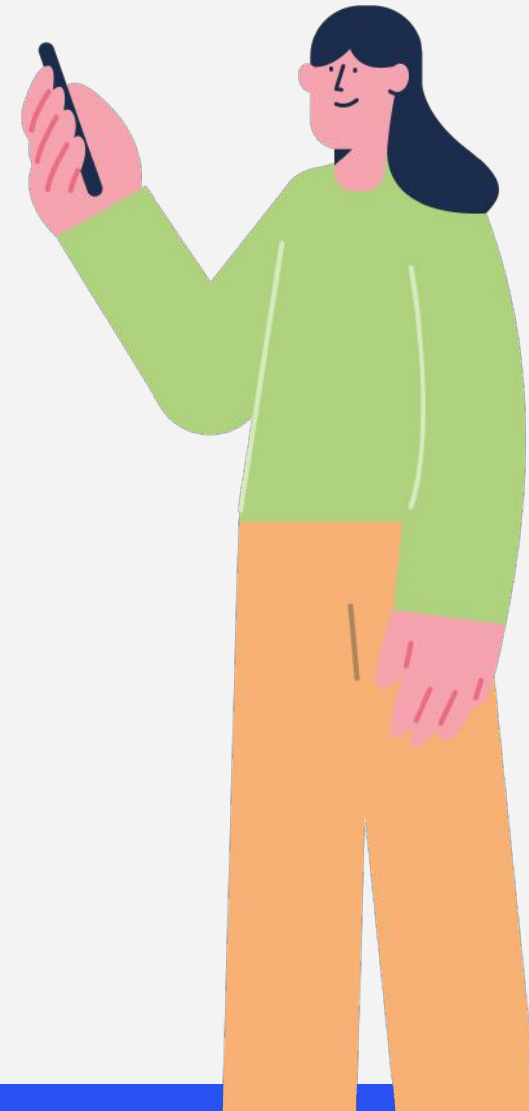
Blocking
on Profile

Blocking on Messenger

Blocking on Messenger
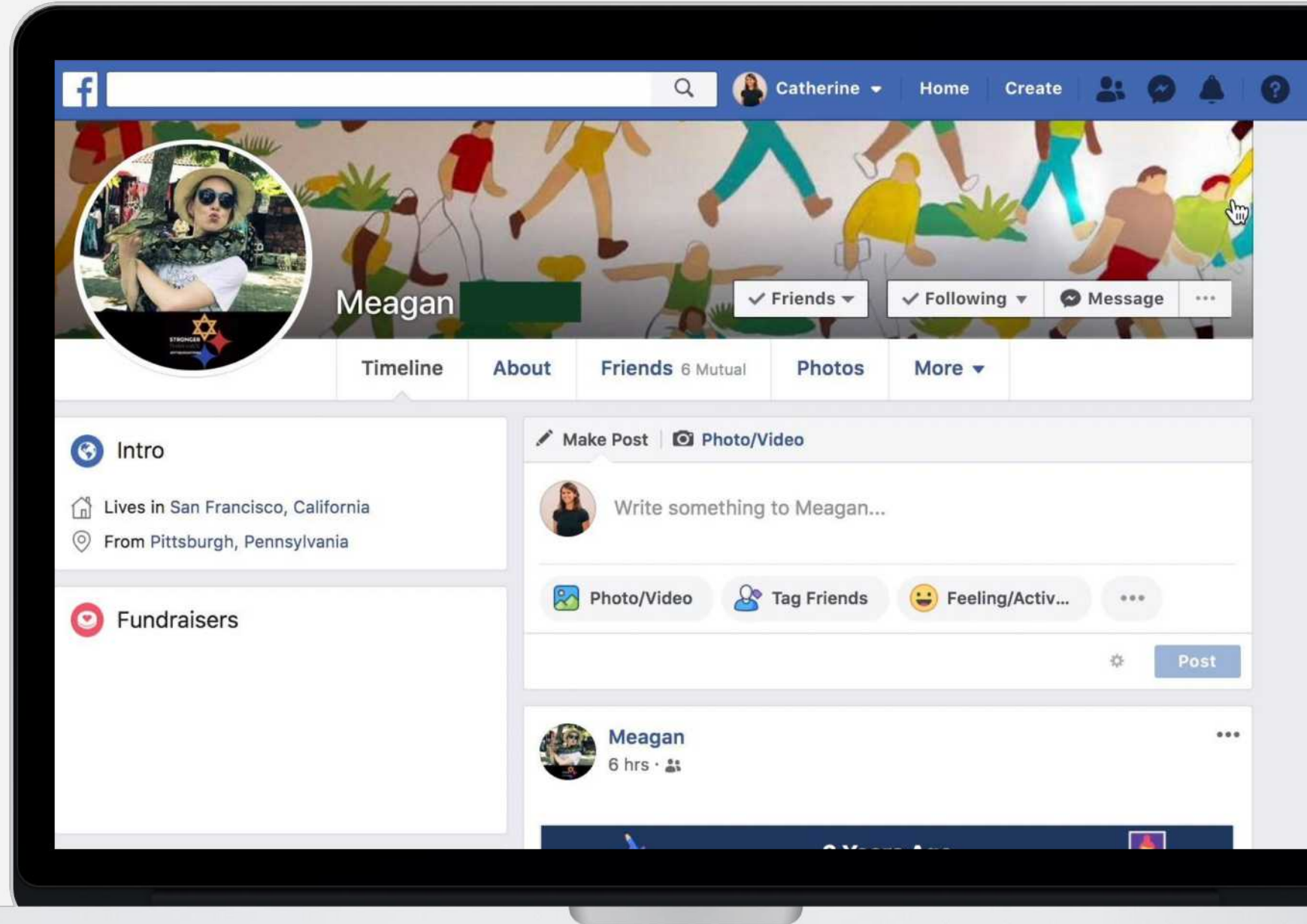
MANAGING ONLINE HARASSMENT

Blocking on Mobile Messenger
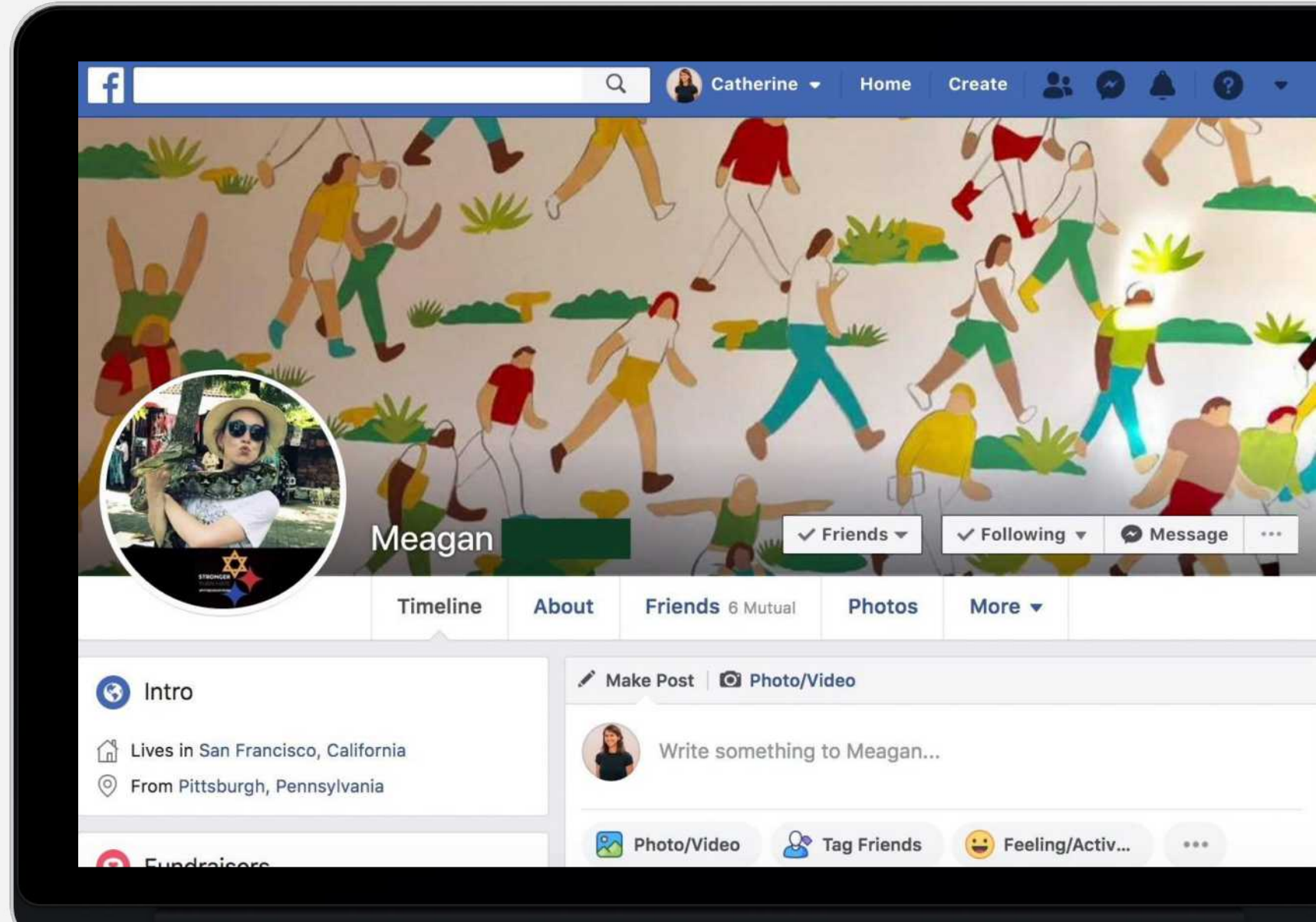
Reporting Harassment

Reporting Harassment on Mobile

Reporting Harassment on Mobile

Reporting Harassment on Mobile

Reporting Harassment on Mobile
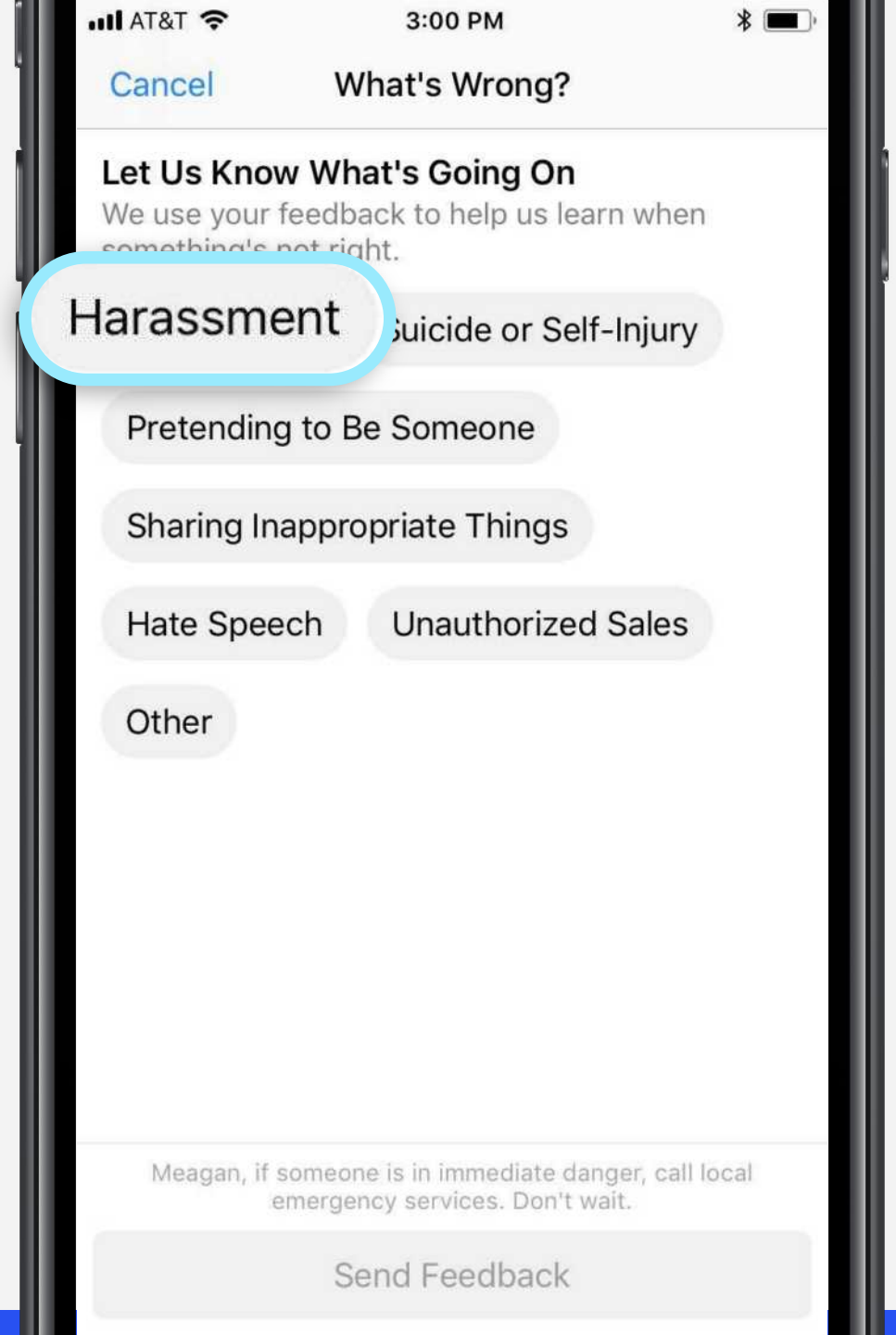
Harassment on Pages
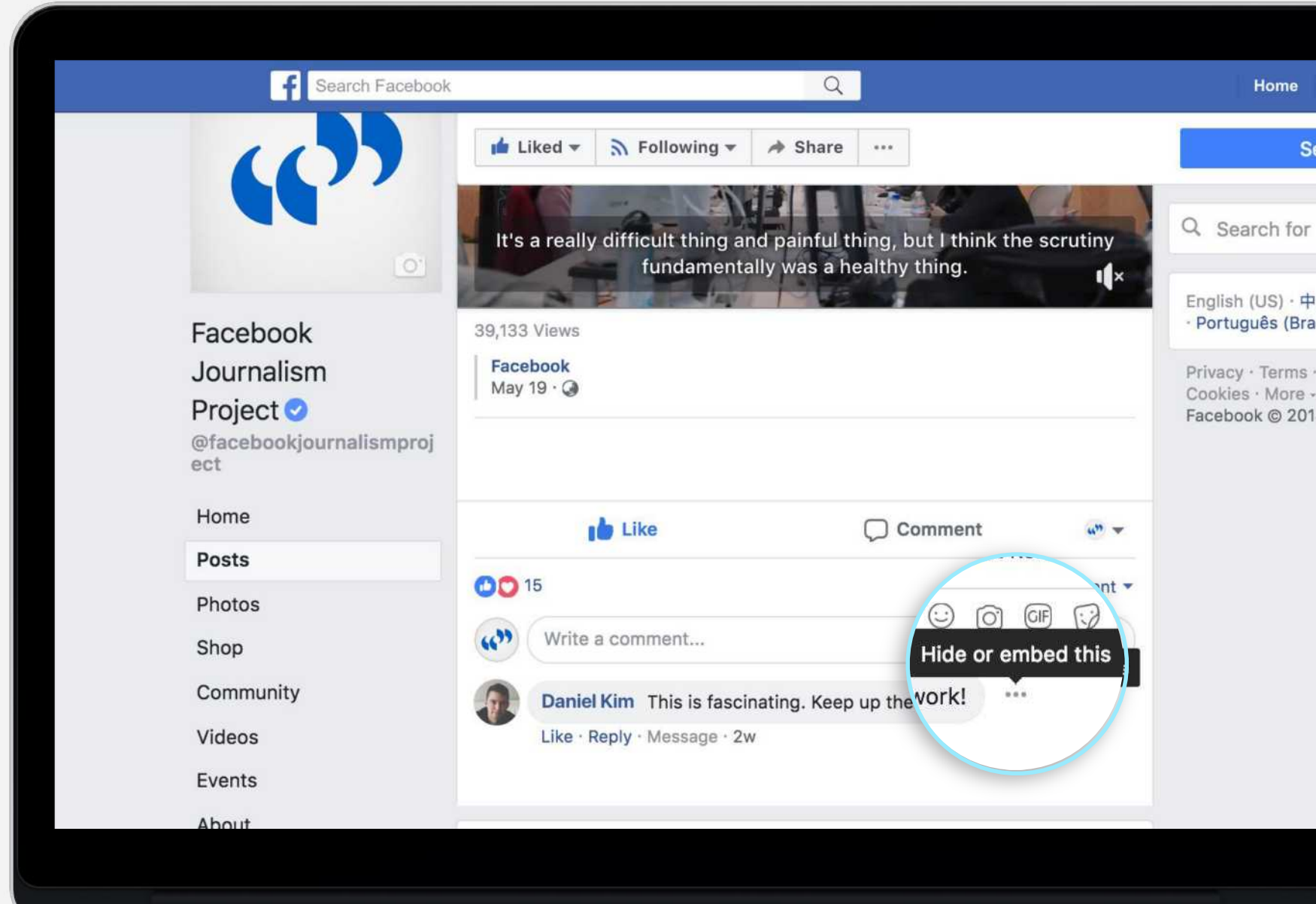
Harassment on Pages
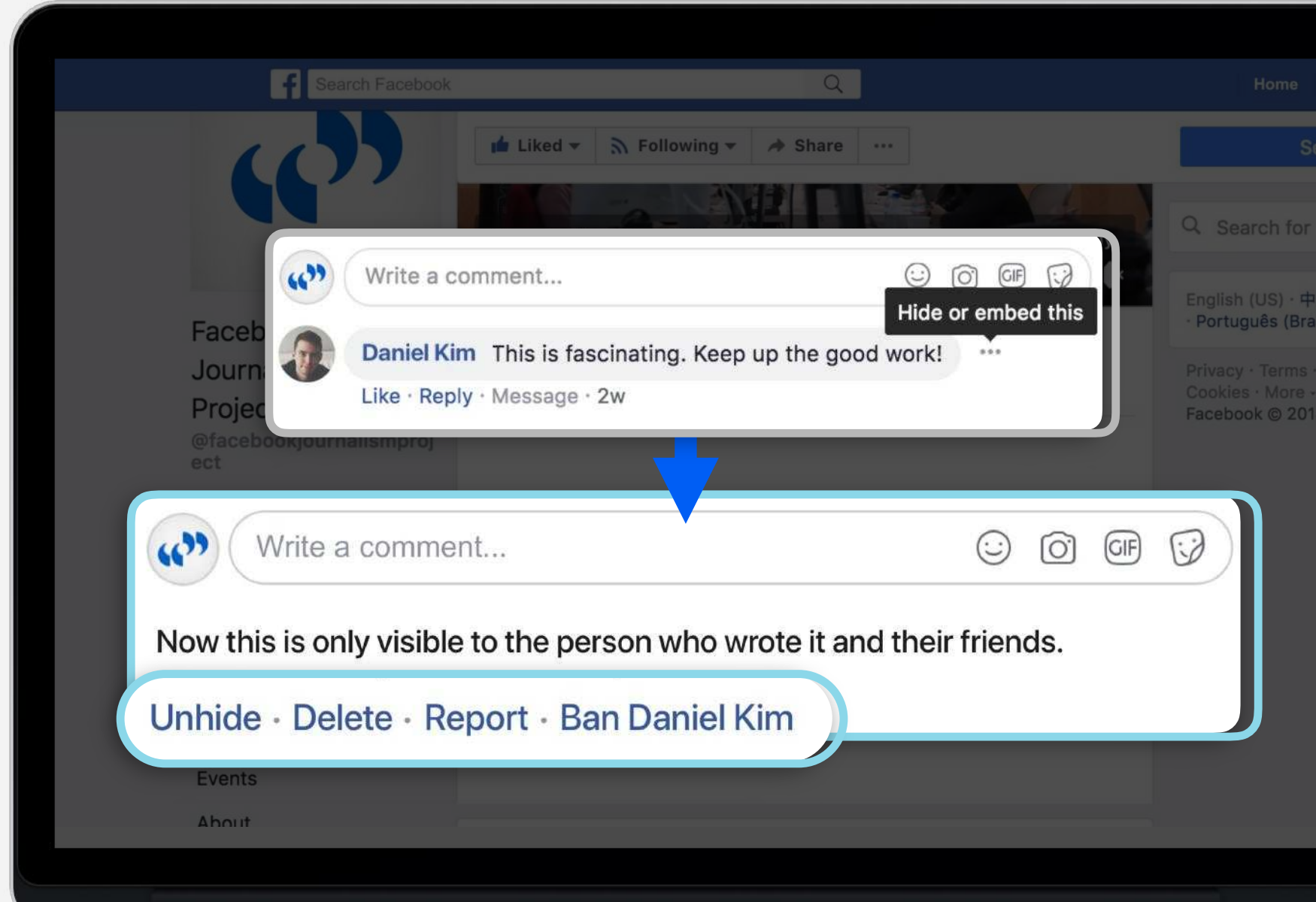
Protecting Your Information on Facebook

[SCENARIOS]

My account has just been stolen by a stranger. How do I recover my account and report this to Facebook?

OR

Hackers have created a fake account with my name and pictures what should I do?

Your account could be hacked if:

1. Your email or password have changed
2. Your name or birthday have changed
3. Friend requests have been sent to people you don't know
4. Messages have been sent that you didn't write
5. Posts have been made that you didn't create

To report visit: www.facebook.com/hacked

If you're worried about the security of your account, we can help you.

First, can you tell us what's happening?

○ I found a post, message or event that I didn't create

◉ Someone else got into my account without my permission

○ I found an account which uses my name or photos

○ People can see things that I thought were private

○ I don't see the right option on this list

Cancel   Continue

Securing your accounts on Facebook

There are two main ways for you to secure your account on Facebook:

1. Two Factor Authentication
2. Login Alerts

To turn on or manage two-factor authentication

- Go to your Security and Login Settings by clicking in the top-right corner of Facebook and clicking Settings > Security and Login.
- Scroll down to Use two-factor authentication and click Edit
- Choose the authentication method you want to add and follow the on-screen instructions
- Click Enable once you've selected and turned on an authentication method

Two Factor Authenticatio n (2FA)
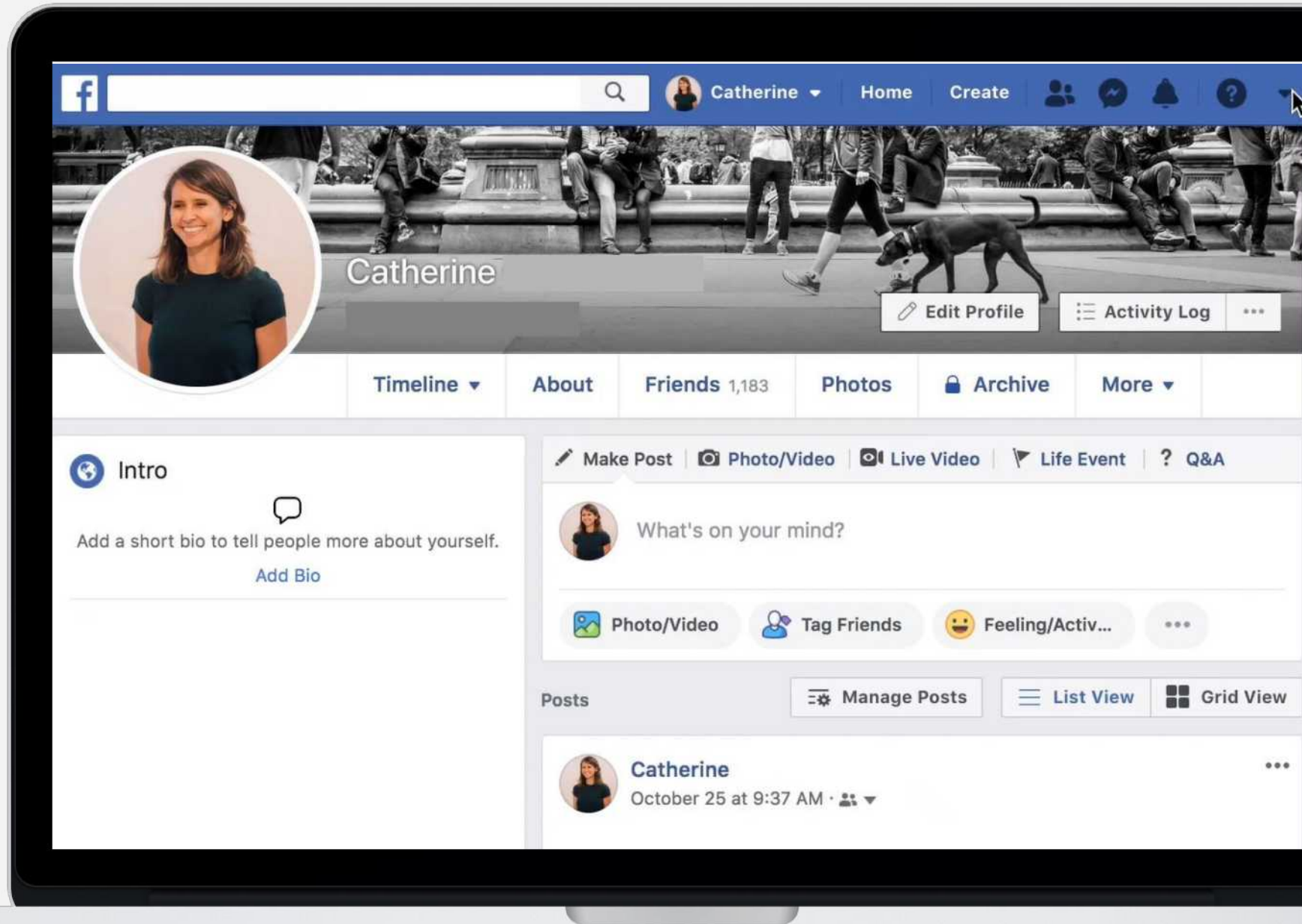
Two Factor Authenticatio n (2FA)

Strong Password Formula
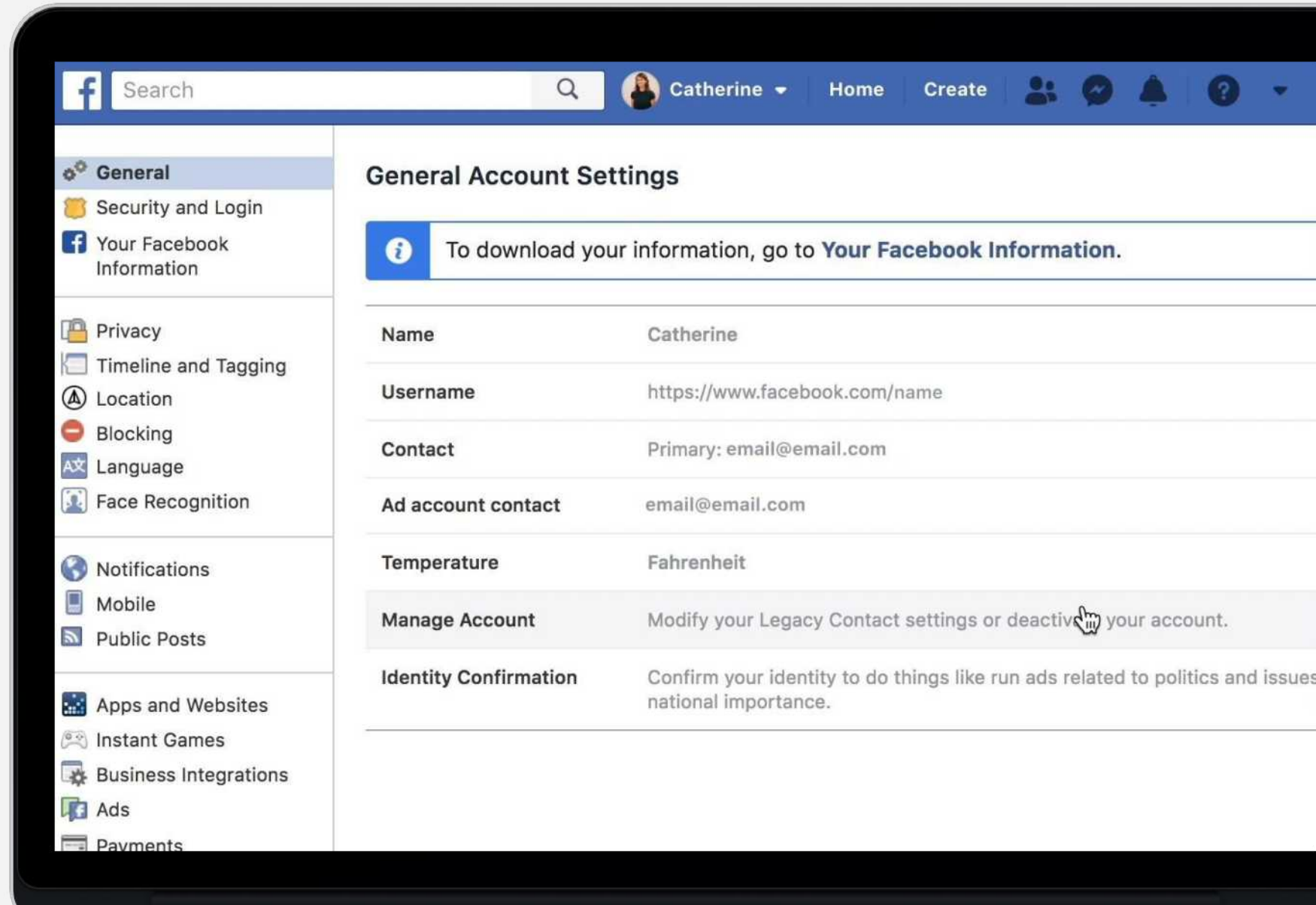

AVOID PUBLIC INFORMATION LIKE YOUR NAME

+

A PASSWORD UNIQUE TO FACEBOOK

+

DON'T SHARE YOUR PASSWORD

Keeping your accounts safe from hackers

1 Enable login notifications

2 Check active sessions on Facebook

3 Pick a strong Password

4 Change you password regularly and never give it to someone you do not know and trust

Keeping your accounts safe from hackers
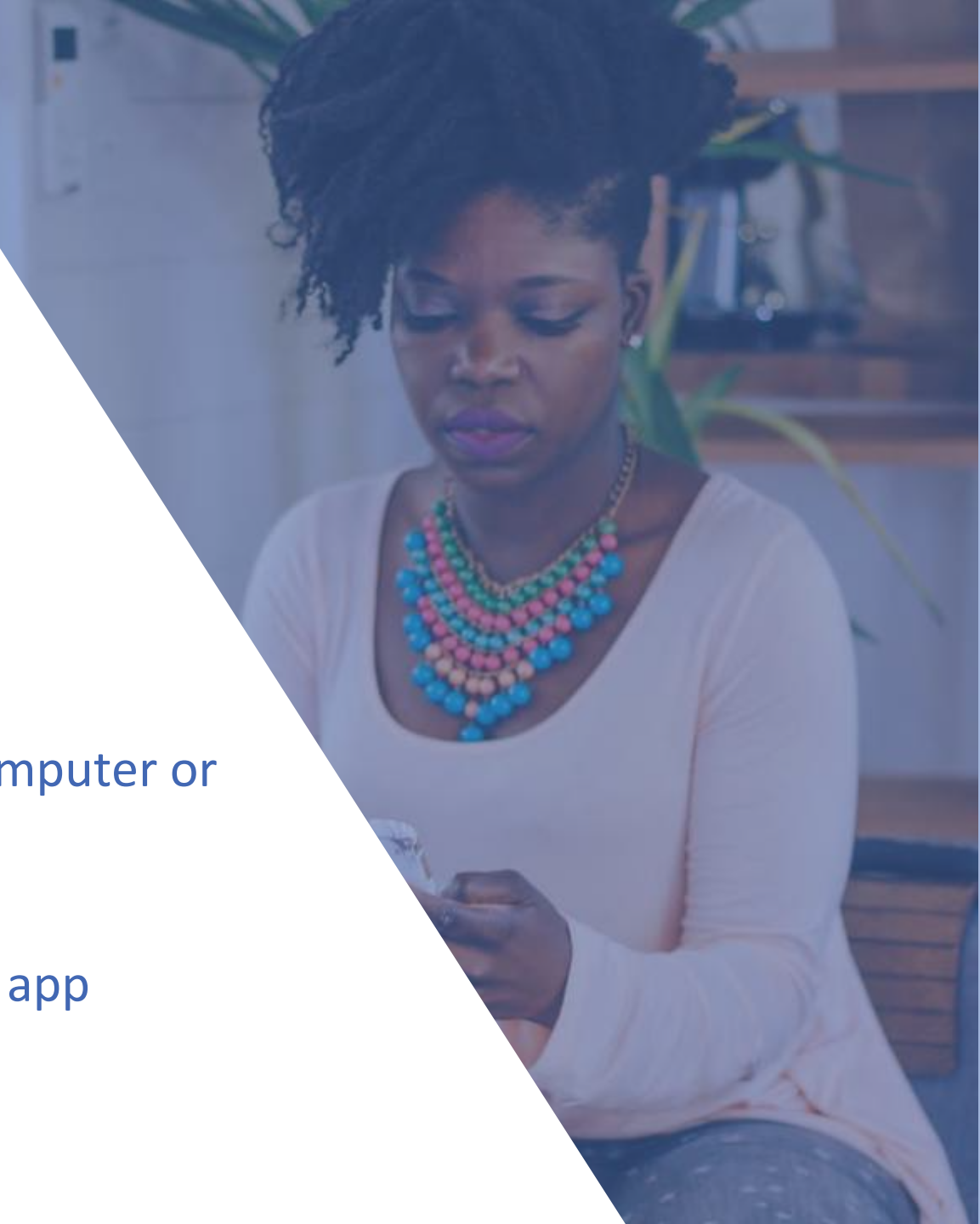
5   Turn on two-factor authentication

6   Make sure your email account is secure

7   Log out of Instagram when you use a computer or phone you share with other people

8   Think before you authorize a third party app

Security
Checkup

facebook.com/help/securitycheckup