Defensive Social Media: How you can put safety first in your election campaign

A training webinar for members of AILG

Kelly Fincham, PhD

OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

SAFETY FIRST

Sharing research with the wider community

Agenda

SAFETY FIRST

* About me and my research

* Key findings from AILG Survey

* 3 focus areas for today

  1. Doxxing (private information)
  2. Malicious campaigns
  3. Mitigating online abuse

* Q&A

Research on social media in politics and/or journalism

Mitigating online harm in politics. *Political Studies Association of Ireland Annual Conference*, Queens University Belfast, October 2023

Exploring corporate social responsibility in news organisation policies. *Future of Journalism Conference*, Cardiff University, September 2023

Lineker-BBC row: survey shows how different outlets approach their staff's social media presence. The Conversation March 2023

Business as Usual: How Journalism's Professional Logics Continue to Shape News Organization Policies Around Social Media Audiences, Journalism Practice, DOI: 10.1080/17512786.2021.1991437 January 2022

Politics as usual? A case study of candidates on Twitter in the Dublin Bay South by-election. *Political Studies Association of Ireland National Conference*. UCD, Ireland, October 2021

Exploring political journalism homophily on Twitter: A comparative analysis of US and UK elections in 2016 and 2017. *Media and Communication*, 7(1), 213-224. DOI: http://dx.doi.org/10.17645/mac.v7i1.1765 2019

Female political journalists sidelined as 'boys on the bus' dominate Twitter interactions. *Political Studies Association of Ireland National Conference*. Maynooth, Ireland, October 2019

#Twitterfail for news organisations: How newsroom Twitter policies fail to guide journalists on engagement. *International Communication Association Conference*. Washington, DC, 2019

How Did Social Media Change the 2016 Presidential Race? *Kalikow School of Government, Public Policy and International Affairs*, Hofstra, 2017

Journalism and politics in the 2016 Irish general election, *Political Studies Association of Ireland National Conference*, Belfast, Ireland, October 2016

These views are my own. The private and public self in the digital media sphere. In Zion L, Craig, D, Ethics for Digital Journalists: Emerging Best Practices. New

About me and my research

Started researching Twitter impact on media and politics in 2011

PhD in 2023

Focus on engagement and interaction in journalism

Everyone in politics and media encouraged to be active on platforms for "engagement" pay-off

Relevant findings

The platforms that were supposed to facilitate *conversations* quickly became entry points for attacks

---

Efforts at online "engagement" resulted in repeated attacks by swarms of bots and trolls

Relevant findings

The perceived benefits of online 'engagement' were wildly optimistic and overplayed - all to the benefit of platforms

Social media interactions are now understood to be overwhelmingly negative and in ways not fully captured in the research

Major newsrooms no longer require reporters to be online and in some cases are actively encouraging them to step away

Early adoption/enthusiasm about engagement based on unquestioned assumptions that all interactions would be "good"

Relevant findings

"Abuse is part of the job"

"Abuse comes with the territory"

If it affects you, do yoga, drink wine or seek therapy

OLD WAY
NEW WAY

Attitudes to abuse are changing too.

Newsrooms now recognise that the scale of the abuse demands a system-wide response rather than leaving it on the individual

Relevant findings

"On the Internet, nobody knows you're a dog."

Journalism is showing us that there is a need to query this underlying assumption that social media matters—and matters quite a lot—because it represents an earnest extension of the public sphere (Quandt, 2022)
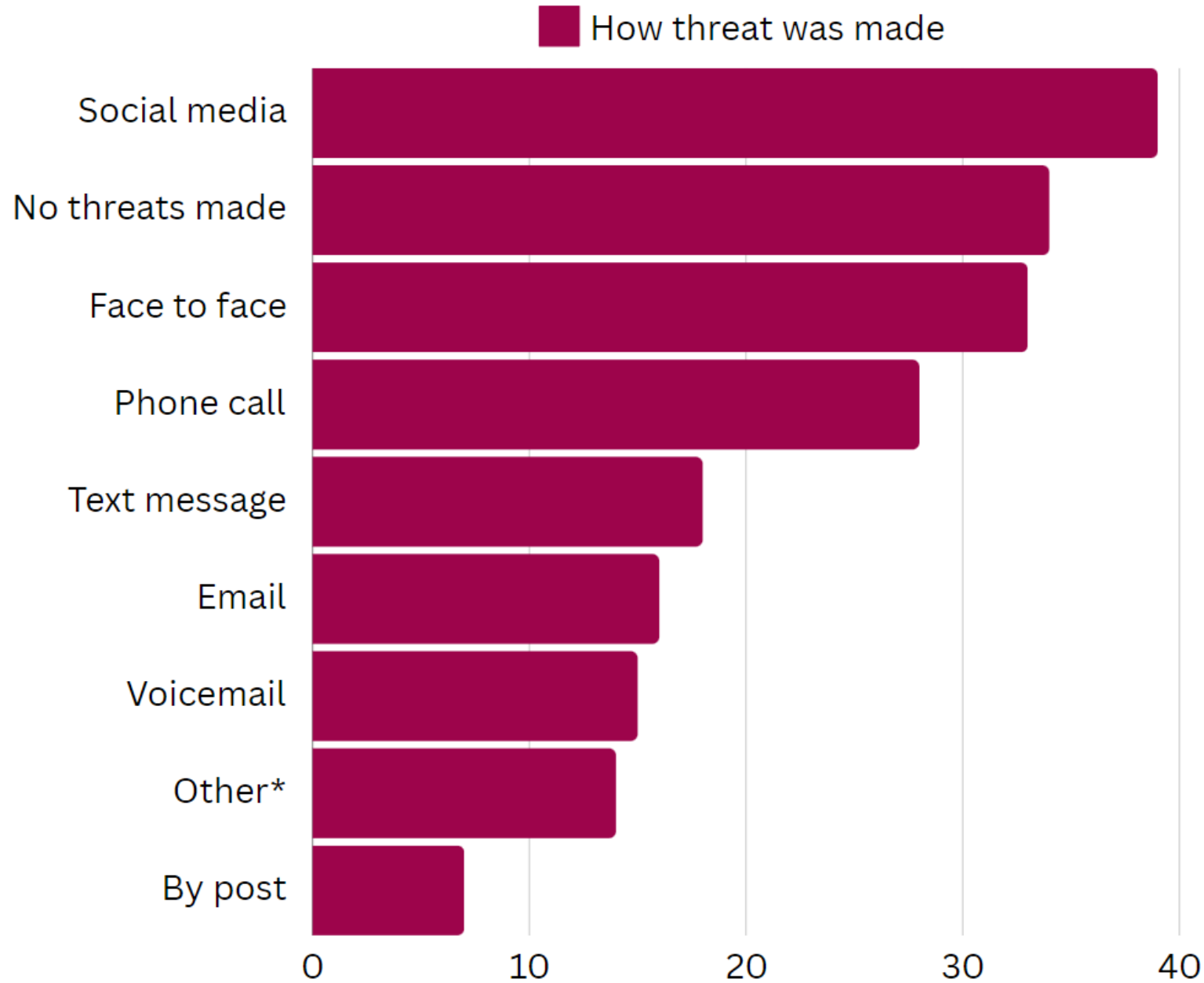
Key Findings

Threats, intimidation and harassment

63%

---

*226 respondents

How threat was made

Key Findings in AILG Survey

Category	Value
Social media	39
No threats made	34
Face to face	33
Phone call	28
Text message	18
Email	16
Voicemail	15
Other*	14
By post	7

**Other includes
- Communicated to another third party
- Online meeting platform
- Communicated to a family member"

Doxxing*
What to do if you are doxxed

*The term derives from "docs" the abbreviation for "documents"

1. Don't blame yourself! This could literally happen to anyone.
2. Report the harassment (this is harassment) through any available tools on the platform where this took place.
3. Screenshot everything
4. Make all your social accounts private and/or pause them
5. Let your friends and family know
6. Let your bank know - request that your credit card details are protected.
7. Report the harassment to the gardai.

Doxxing prevention

It's impossible to hide all your personal information that is already in the public domain but if you make it more difficult to find then that might be enough to deter a doxxing attempt.

Change your passwords!

- Long - 12 characters or longer.
- Unique - Do not reuse a password in multiple accounts.
- Easy for you to remember but hard to guess - We recommend choosing a long passphrase over random passwords. For example, using a sentence like "The blue horse likes to eat chocolate" is a memorable password that is hard for others to guess. To meet password requirements, you can add punctuation and numbers to create "The b1ue horse likes to eat ch0c0late".

- Clean up your social media accounts
- Don't share any (more) personal information online.
- Even your photographs can be used to locate your home address
- Use two-factor (or multifactor) authentication (2FA, MFA) in all your accounts.
- Make sure your Zooms/Teams and other calls are private and encrypted.
- Don't open any links sent online before checking the person intended sending them (yes this feels weird but better than launching malware).
- If you don't even know the person ignore them.

Doxxing guide

The New York Times offers a free resource on doxxing which includes a step-by-step guide to doxxing yourself so you can check and see how much information there is already available on you. Use this link to access

How to Dox Yourself on the Internet

A step-by-step guide to finding and removing your personal information from the internet.

The NYT Open Team · Follow
Published in NYT Open · 5 min read · Feb 27, 2020

- **Doxxing Guide**: This guide details steps that you can walk through on your own or with a group to begin cleaning up your online footprint. It includes a list of data broker websites that offer opt-out options, targeted techniques for search engines and tips for locking down your social media accounts.
- **Social Media Security and Privacy Checklist**: This guide includes checklists of recommended security and privacy settings for several popular social media websites that will ensure your profiles are locked down and that you're only sharing information that you're comfortable sharing.
- **Doxxing Curriculum Outline**: A high-level overview of the curriculum we used when running doxxing workshops at The New York Times. If you'd like to bring a version of this program to your newsroom or organization, or to a group you work with, this resource will help you build out a formal training session.

Malicious campaigns

1. Comments posted on a Facebook page included sexist and misogynistic terms and also racist and xenophobic language
2. The page was reported to Facebook/Meta but the platform considered this allowable discourse, not abuse
3. "This is a community group in which members are sharing their concerns about local issues. We don't allow bullying or harassment on Facebook and will remove it when it is reported to us. We have reviewed the group and determined that the content does not violate our policies."

The lack of regulation for social media platforms means that there are very few avenues available for people being attacked on those platforms.

- Report the harassment to the platform and gardai.
- Screenshot everything
- Make all your social accounts private and/or pause them
- Let your friends and family know
- Where it is possible, ask a trusted friend or family member to monitor the page.
- Discourage "bystander intervention" Newer research is showing that posting positive "mentions" that show up in the feed of the person being attacked may actually instead be adding to the feelings of overwhelm and unintentionally contributing to harm.

Mitigating online abuse

Disengage from engagement

The best way to avoid online abuse is to change your use of social media from a networked tool to a broadcast tool

Use all the platform affordances to turn off or restrict conversations and comments.

"Our data suggest that social media campaign effects are achieved through using Twitter as a *broadcast* mechanism. Despite much literature encouraging politicians to engage with social platforms in an interactive fashion, *we find no evidence that this style of communication improves electoral outcomes*" (Bright et al, 2020)

Mitigating online abuse

Don't feed the trolls

Facebook: Create posts with comments only for people mentioned (don't mention anyone!)

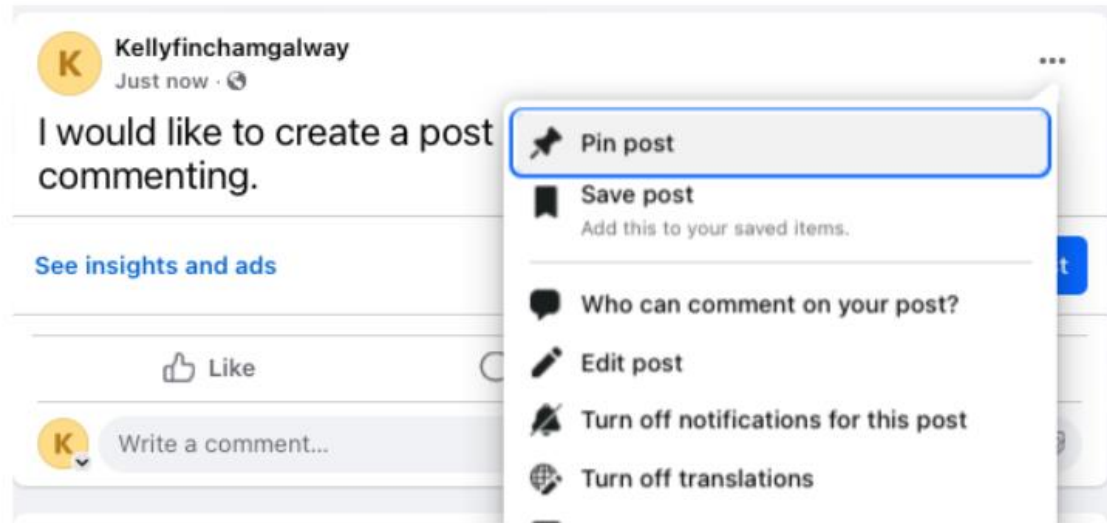**Twitter:** Start by blocking and muting. Restrict replies to tweets

Instagram: Disable comments on your post
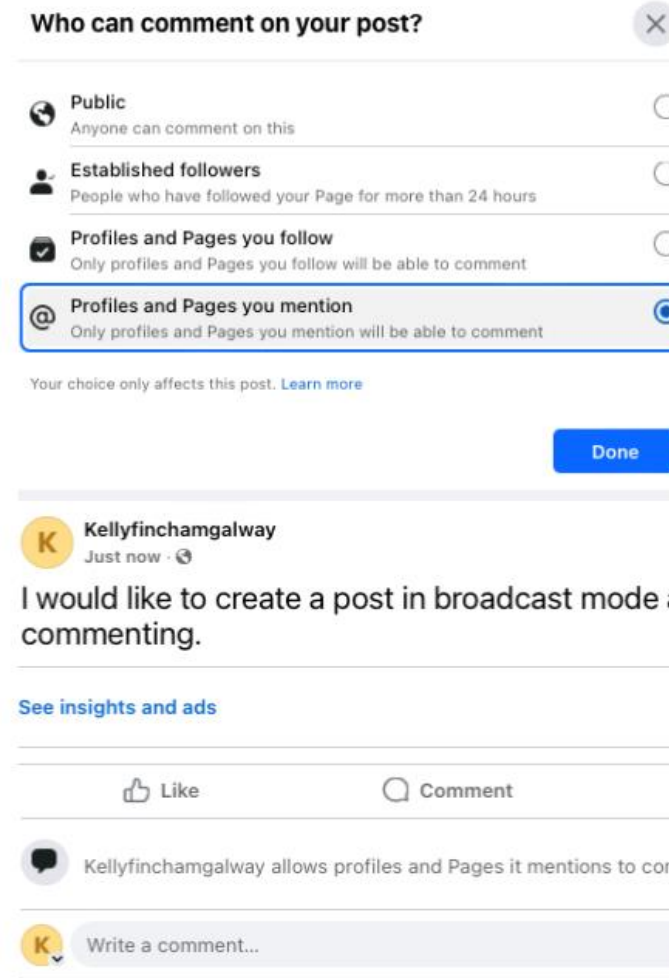
TikTok: Disable comments on video

1. Replying to messages, retweeting, or engaging directly with the public is not a vote winner
2. Individual interactions are by definition small scale
3. The lack of any evidence that engaging in interactive campaigning improves vote outcomes is striking.
4. Fun fact: Facebook used to consider "likes", "shares" and "comments" as having equal weight.
5. Number of Facebook likes and the number of Twitter followers are associated with positive outcomes

How to disable comments on Facebook

Restrict comments to profiles and pages you mention
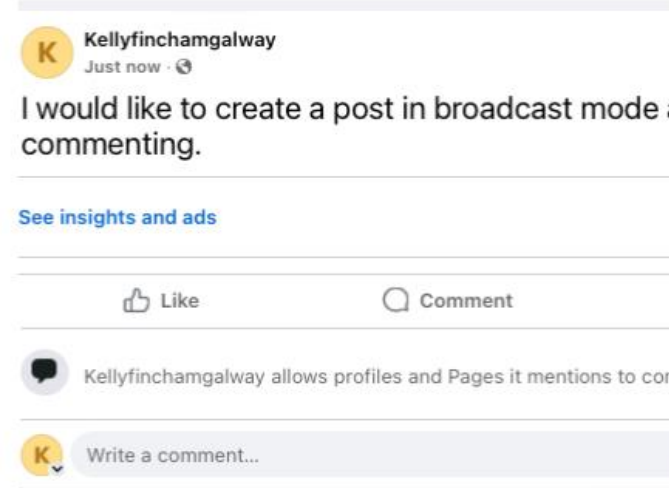
The post now only accepts Likes and Shares

Likes and Shares are still valuable!
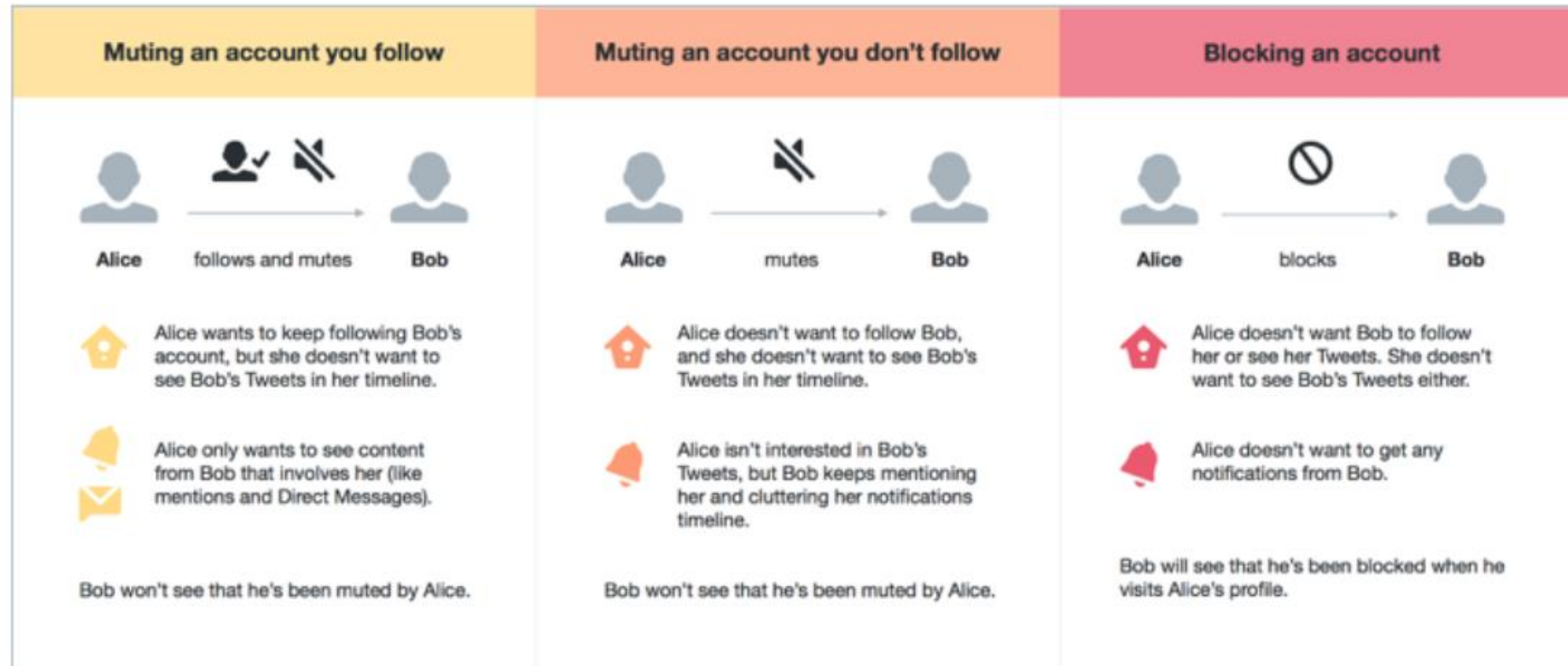
Create your page post first, publish it and and then hit the three dots and select "who can comment on your post"

Muting and blocking on Twitter/X

Muting an account you follow	Muting an account you don't follow	Blocking an account
Alice — follows and mutes — Bob	Alice — mutes — Bob	Alice — blocks — Bob
Alice wants to keep following Bob's account, but she doesn't want to see Bob's Tweets in her timeline.	Alice doesn't want to follow Bob, and she doesn't want to see Bob's Tweets in her timeline.	Alice doesn't want Bob to follow her or see her Tweets. She doesn't want to see Bob's Tweets either.
Alice only wants to see content from Bob that involves her (like mentions and Direct Messages).	Alice isn't interested in Bob's Tweets, but Bob keeps mentioning her and cluttering her notifications timeline.	Alice doesn't want to get any notifications from Bob.
Bob won't see that he's been muted by Alice.	Bob won't see that he's been muted by Alice.	Bob will see that he's been blocked when he visits Alice's profile.

Blocking can be an effective way to handle unwanted interactions from accounts you do not want to engage with

How to restrict replies on Twitter/X
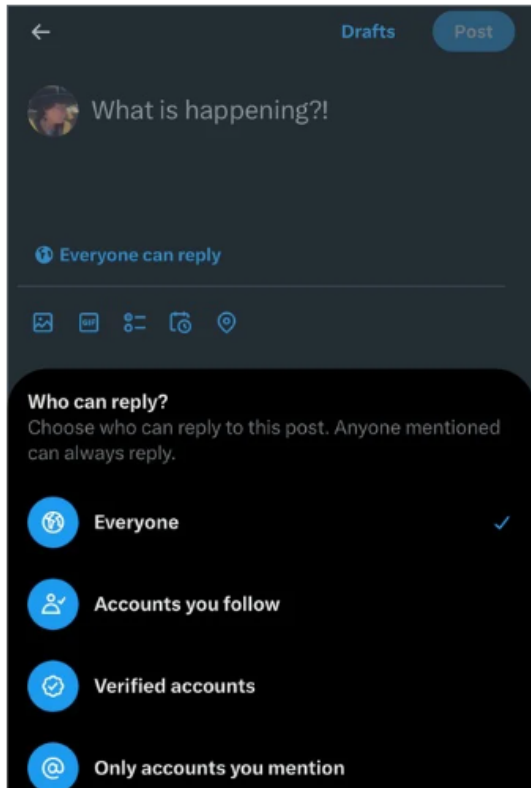
Restricting replies to only people that you want to hear from removes unwanted interactions

Protect yourself by using all available tools from the platforms to reduce unwanted interactions from specific users OR all users

More links to how-tos will be posted on the bit.ly page after the session

SAFETY FIRST

Going forward

Yes! You should be using social !

- But use it as a broadcast media tool
- Share stories about your campaign, use pictures as much as possible BUT
- Disengage from engagement
- Do your own doxxing guide NOW.
- Reduce the amount of publicly available information about you.
- Change those passwords!
- Restrict "reach" efforts to liking and sharing
- Remember Facebook used to accord them equal value until the platforms saw more value for themselves in the comments