Twitter Thread by [redacted]



[redacted]
@AlFirasah_



Thread:

Recently, doxing of IMT has become a tool to suppress vocal Muslim voices, with rival Sanghis doxing those who hold opposing views. Doxers aim to escalate their conflict with targets from online to the real world, by revealing personal information which includes:1/n

1. Home addresses
2. Workplace details
3. Personal phone numbers
4. Social security numbers
5. Bank account or credit card information
6. Private correspondence
7. Criminal history
8. Personal photos
9. Embarrassing personal details 2/n

Suspension methods used

1. Dig up old tweets to see clues
2. Mark tweets which violate twitter terms and mass report
3. Agent provocateur - Use of trolls to incite to say something that violates twitter policy. 3/n

Doxing methods used:

1. Usage of twitter archive to keep track of a target account. It saves even deleted tweets. After the identity is known, the archived tweets (even if you deleted them) are used to report to goverment, police, employer etc 4/n

2. Social Engineering; Social Engineering is a manipulation technique that exploits human error or friendliness to gain private information. An agent acts as friendly and then lures the unsuspecting person into exposing their own data or their data from someone else. 5/n

a. Send hacking links from fake profile on Direct Message or gaining trust of target using friendly profile. These links look normal but they reveal your location, your device, your mobile provider etc. 6/n

b. Infiltrate IMT groups and social engineer personal info. Get friendly with some accounts & coax them to reveal info about others. 7/n

3. There is a dedicated study team. They try to make a picture of the target person analyzing all kind of data gathered.
a. Analyze old tweets & old personal connections. Talk to the old connections. If needed study the old connections. 8/n

b. Analyze first follows & tweets & likes & @username change history.
c. Analyze Regional news followed, food preferences mentioned, username etc 9/n

d. Analyze posts:
eg; if any screenshots shared, analyze it to know timezone, carrier provider, mobile operating system (android which version, ios which version), analyze pictures clicked and uploaded for metadata. Sometimes posts share your location automatically. 10/n

e. Match target profile personality with other social media profiles personalities
eg: matching bio, @userame, fav movie, fav food, fav colour, political party, writing style, posts written etc on real profile and fake profile, across different platforms (twitter, fb, insta) 11/n

Remedies & NECESSARY precautions

DOs:

1. Imagine a parallel identity - Whose personna is very different than your own 12/n

a. Make your personna with complex detail, personal choices, location & writing style. Therapists say- If you imagine something, your brain doesnt distinguish between real & fake. If you can fool your brain, you can fool others 13/n

b. Deleting previous personal identity tweets doest work! Theres traces remain. Even if you talked with people you personally knew - your replies and messaging exists on twitter - these can be tracked even if you change @userame and everything. 14/n

c. What? Did you say 'Messaging is private'? You have no idea about sanghi twitter infiltration 15/n

2. Have a unique email/password and @username+bio which you havn't EVER USED BEFORE on same platform (twitter) or even other platforms (fb, insta). 16/n

3. use https://t.co/JYFGL7h9jR for email - your general email/password combination you have always used on websites are hacked from a website and available freely on internet with basic hacking tools. 17/n

4. Talk, speak, breath like your personna. Follow news/accounts which match according to the imagined personna.
If you are Bengali & your personna is Tamil - Behave like a Tamil. 18/n

Don't follow Bengali politicians, news, food recipes, activists etc. Dont like any bengali tweet. Translate tamil and like some tamil tweets. 19/n

Add appropriate security settings:
- Turn off location shared with posts
- Check the apps you have given permission to. Remove the ones not actively used. Re-consider if you really have to use the others.
- Doublecheck before uploading images 20/n

DON'T DOs:

1. DON'T - Never share personal info with anyone or poison pilled them.

If you really really have to. Make sure you have
a) met the person personally &
b) align with them ideologically & religiously. 21/n

Never share your info with non muslims. One tweet someday on an ethical value - that doesn't align with them and they will dump you. This will happen in future, even if you think it's not happening today. 22/n

2. DON'T - Never explicitly/directly speak illegal things.
You can always be indirect. It can help against suspension and explaining differently if your identity is exposed. Explicit boldness will get you suspended. 23/n

Explicit boldness will get you suspended. But it's needed. For explicit boldness, you need a 'shahadah' profile, where you speak without restriction until you are 'suspended'. 24/n

Remember -
you need same level of anonymity for shahadah profile
it needs to be on different device and preferrably different network/vpn etc. 25/n

3. DON'T - Never become over friendly and expose private info.
Your identity is the common identity of the group you belong to. You are working for social cause. 26/n

Personal identities are not important. What is important is to work on common cause - even with strangers - even if those strangers are potentially fakes and intruders. 27/n

As long as the strangers are supporting the cause - you work with them - A.N.O.N.Y.M.O.U.S.L.Y. Never become over friendly and expose private info 28/n

4. DON'T - Never click links on private message
if you have to click, then download a vpn app, activate it - and then click 29/n

5. DONT - Never mix your personality into the profile
Describing your favourite movies, colour, dress, festival, dialogue, profession, event, family size, education, marital status, delicacy, aspirations, talking style, etc.. n/n