Twitter Thread by Dusk @ it's 2021



Dusk @ it's 2021
@nekoromancy



I am seeing a ton of confusion about protecting yourself on the Internet. So as a retired bastard genius kid, I wanted to share my own experiences and knowledge in this.

DOXXING, PERSONAL CYBERSECURITY, ANONYMITY for the average revolutionary. A thread:

If you're a regular user of huge Internet services like Amazon, Google, Twitter, Facebook, etc., as well as over the age of 18, it's wise to assume that your personally identifiable information IS attainable and IS out there. These services all collect and save info --

to varying degrees, and to varying levels of security. And this information is VALUABLE. Data breaches occur frequently, retroactively, and unknowingly, and the data from said breaches are circulated around and cached in all kinds of easy-to-access places online.

Why does this matter? A (simplified) hypothetical: while someone probably can't find your street address from just your Twitter bio, if your handle is the same as your e-mail, and that e-mail is in a publicly available data breach with a street address attached, you're screwed.

Usually when doxxing happens, a much more elaborate version of said case happens. Doxxing really comes down to investigating all of an individual's available info and digital footprints, and narrowing it down to a single identity.

Things like email, name are major clues, but there are lots of unexpected ways to narrow down a person's identity or info. What I've used in the past: old forum archives. Brands/logos on items in the background of photos. As of late, people are using Amazon wishlists, apparently.

Should you worry? For most of us, no.
On an individual level, most average people are not important enough to try to dox. But if you're hiding from a tyrant govt, a high-profile YouTuber with bad opinions, hiding from white supremacists, or an active BLM protestor? Be concerned.

You may be reading this and thinking "shit, it's too late for me, I'm screwed!" Well, truthfully, nobody -- yes, NO ONE -- is truly safe from being hacked/doxxed, especially if you've been using the Web for a while. That's why taking measures NOW is the best thing you can do.

I don't want to go into every single cybersecurity method for keeping yourself safe as it's too broad of a topic. So instead here are some tips in Q&A format:

Q: What is the #1 best way to prevent myself from being hacked?
A: STRONG passwords changed regularly. NEVER use the same PW between sites. PW managers/generators help immensely. Combined with two-factor authentication (2FA) on all services, this is enough for most average users.

Adding to this, general safe surfing: avoiding shady links and downloads. Understanding HTTPS and why it matters (most browsers are built-in now to warn or prevent you from entering information on non-certified or non-HTTPS websites). Keeping your software updated. All good tips.

Q: Can I be doxxed if I have pronouns, name, age in bio?
A: Possibly, but probably not. It can help to narrow down a search for info, but those alone usually aren't enough to find a person online.

Q: Can I be doxxed from a shady link?
A: Yes -- sort of. Do not click strange links without knowing the context. Malicious websites run scripts that do things like IP logging or cookie grabbing. An IP alone does not reveal a physical location, but can be spoofed as your identity.

Q: So should I just not post anything at all?
A: Not necessarily. Many people stay anonymous by operating through multiple identities and being careful about what data is shared where. You are at discretion with how far you want to protect yourself, just like with real life.

Q: Can I erase my personal info off the Internet?
A: Virtually no. Nearly all data ever inputted into the Web has been cached and saved somewhere. You can request people directory sites to take down info of you, but usually with limitations. The best way to deal with it is --

1) figure out exactly how much of your info is out there now by... well, doxxing yourself

2) obfuscating what you found as much as possible. Delete/archive old social media accounts. Request said takedowns. Change your account handles and email addresses. Etc.

Q: I'm anxious now.
A: I know. This stuff is scary. But being equipped with the knowledge is the best thing you can do for yourself. ^^

Gonna end it here now -- I hope this was an informative read. If you're versed in this stuff as IT or cybersec, feel free to correct or add your opinions. To end this thread I'd like to share a few links for further reading.

Some methods used to dox streamers in the past (my citation for Amazon wishlist social engineering):
https://t.co/vQiwAH6fOI

A password manager I like and personally use, KeePass. I am not paid to say this or anything, it's a free and open source software that works seamlessly. https://t.co/liFa0NhisH

An excellent EXIF data (metadata that stores info like geo coordinates, device etc.) scrubber I really like made by @everestpipkin. Works in-browser and has blurring tools for faces. You can also turn off your EXIF data within your Camera apps.

https://t.co/Ht1yLvBGUR

A general guide for keeping yourself anonymous and secure if you go out for demonstrations.
https://t.co/hGm38m94mH

Potential TW //
This is technically not about doxxing but it's an INCREDIBLE independent investigation on geolocating a child abuse case based on photos alone. It's incredible what a photo can tell you, even outside of metadata.

https://t.co/bFGbUSelC2

An aside, btw. This is not an exhaustive guide to protecting yourself. There are many layers and methods to cybersec, and like all of tech, it constantly changes! I invite you to explore this on your own if you intend to use the Internet a lot in your activities.

Some topics you may want to delve into:
Encrypted forms of communication (Telegram, Signal)
Social engineering
Tor Browser/Tor Network/.onion addresses
Hong Kong protests (I can't find articles on it at this moment but their web organizing was INTENSE and worth learning from)

Lastly, please share this thread if you find it helpful. I want to make sure people are educated on this stuff moving forward because politics is only getting worse and worse in this country and tech + the Internet will be key points to our survival and growth. Take care.