### Only keep record of citation if guideline originated from academic article or news article. Avoid associating individuals with vulnerabilities!! -Caleb

\*I’ve been putting the categories in alphabetical order btw. -Caleb

**Impersonation**

Impersonation can lead to false accusations and a loss in reputation. It can also cause fans to potentially fall for scams.

To remain safer from impersonation, make sure to get any possible account verified. Additionally, be vigilant about any potential scams being spread using your name. Warn your audience, and take necessary actions to eliminate impostors, whether it be through reporting, blacklisting users, or blacklisting keywords.

You may be able to use DMCA takedown services to remove the impersonated content.

I feel physically safe but not politically safe

If possible, claim your username as soon as possible on platforms you are considering using in order to prevent impersonators from claiming it before you.

I feel physically safe but not politically safe

Watermark your images with a reference or link to your original account

I feel physically safe but not politically safe

**Mail**

If P.O. boxes are available in your area, get one and have fans send mail to it.

Open your packages at the Post Office, do not take them home without checking for air

tags / tracking devices.

**Password Protection**

Always enable Two Factor Authentication

Use a service like haveibeenpwned ([https://haveibeenpwned.com](https://haveibeenpwned.com/Passwords)) to see if your email

address or passwords were leaked in a data breach.

Change your leaked password **EVERYWHERE** it is used.

Use a password manager to easily generate strong random passwords and keep track of them.

Protect your master password and don’t use a password that has previously

been included in a data breach.

**Personal Identifying Information**

Treat your full name like it is your address, job, family members’ names, family

members’ addresses, family members’ jobs, etc.

You can use a service like Incogni (<https://incogni.com/>) to delete your data from

people finding sites to reduce the amount of possible information to be leaked

from a doxxing attack.

Treat your face like it is your full name.

**Phishing**

Trust your gut and don’t proceed if something feels off

Explaining phishing attacks in AI age

Use an anti-phishing browser extension that utilizes AI for anomaly detection and context

analysis

Ex. Netcraft (works on Chrome, Firefox, Edge, and Opera)

Explaining phishing attacks in AI age

**Proactive Doxxing Prevention**

If you live in a state where your voter registration information is public to anyone, consider looking into any services to scrub your information / certain parts of your information (like your address)

I feel physically safe but not politically safe

Follow online safety learning sources for other ways to protect your information security

Give example, could be youtube channel, sns account, etc.

I feel physically safe but not politically safe

Also check out the section titled **Personal Identifying Information**

**Stalkers**

Avoid posting details about your plans on social media.

Posting fake information is an option.

Keep your location a secret. If where you live is public knowledge, then avoid posting

anything that might detail where you are going to be in the future (any plans, routines, etc.)

Avoid posting any details about your floorplans or room layout and where you keep things.

Get data removed from data broker sites.

**Swatting**

Inform your local police department that you are a streamer and that swatting at your

address might be a possibility.

This might involve you showing your stream to the police.