VTuber Social Media Information Security Behavioral Guidelines

By Joseph Binette, Caleb Corlett

Impersonation

Impersonation can lead to false accusations and a loss in reputation. It can also cause fans to potentially fall for scams thinking they are interacting with you.

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 [2].

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 [2].

Watermark your images with a reference or link to your original account [2].

Brand Impersonation

Double check the handle of any brands that reach out to you, check for anything strange or any abnormalities before sharing anything personal information or following any links.

> Brand impersonators can also obtain verification badges. Do not assume a verification badge indicates a real, affiliated brand account, especially on sites where verification is subscription-based [3].

Make sure any brand account that reaches out to you is actually affiliated with the brand they claim to represent [3].

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) 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.

Whenever possible, do not let others post images of your face to social media.

If you can have control over all of the spaces where you can be identified, you will

have an easier time protecting yourself from malicious aggressors.

Phishing

Trust your gut and don't proceed if something feels off [1].

Use an anti-phishing browser extension that utilizes AI for anomaly detection and context Analysis [1].

Ex. No Phishing!, Slashnext, or Netcraft

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) [2].

Follow online safety learning sources for other ways to protect your information security [2].

For example, r/privacy (https://www.reddit.com/r/privacy/), commonsense.org's section about privacy (https://privacy.commonsense.org/) are good places to start.

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.

References

[1] M. S. Liaqat, G. Mumtaz, N. Rasheed, and Z. Mubeen, “Exploring Phishing Attacks in the AI Age: A Comprehensive Literature Review,” *Journal of Computing & Biomedical Informatics*, vol. 7, no. 02, Art. no. 02, Sep. 2024, Accessed: Dec. 07, 2024. [Online]. Available: https://jcbi.org/index.php/Main/article/view/567

[2] A. Soneji, V. Hamilton, A. Doupé, A. McDonald, and E. M. Redmiles, “‘I feel physically safe but not politically safe’: Understanding the Digital Threats and Safety Practices of {OnlyFans} Creators,” presented at the 33rd USENIX Security Symposium (USENIX Security 24), 2024, pp. 1–18. Accessed: Nov. 11, 2024. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/soneji

[3] B. Acharya *et al.*, “The Imitation Game: Exploring Brand Impersonation Attacks on Social Media Platforms,” presented at the 33rd USENIX Security Symposium (USENIX Security 24), 2024, pp. 4427–4444. Accessed: Dec. 07, 2024. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/acharya