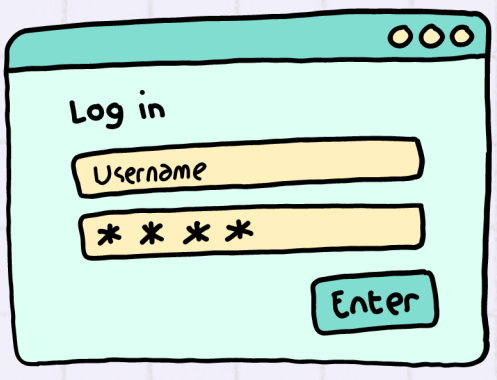
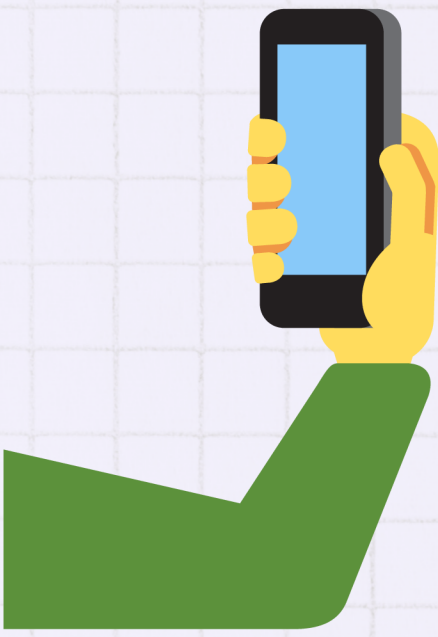
Social Media Security Guide

01 Account Security

- Use Multifactor Authentication (MFA)/2 Factor Authentication (2FA) to secure your accounts
- Do not use social media accounts to log into other services/do not allow 3rd party access
- Have separate accounts for specific purposes (i.e. personal and professional)

<u>Use blocklists to your advantage, regularly go through and clean your social media posts, and block at your discretion</u>





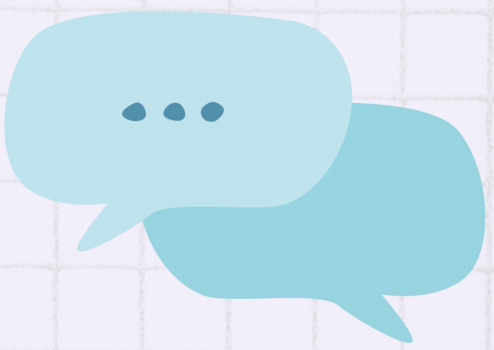
02 Photos/Selfies

- Ask before taking pictures that include others
- Check for anything identifiable in photos you take (i.e. license plates, reflections, mail, keys)
- Try not to post while at an event (wait at least 30 minutes after) or within 5 miles of your home.

<u>If posting at/about a location don't post an exact address, use the nearest large city or venue</u>

03 Messaging

- Know who you're talking to. Anyone can be an "expert"(tm) on the internet.
- Social media is not a secure messaging platform. For sensitive conversations use a secure messaging app such as Signal
- Watch out for bots or accounts that ask for money or personal information



04 More Info

- **RAINN:** https://rainn.org/safe-media
- **National Cybersecurity Centre: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely**

Sources

CISA Staying Safe on Social Networking:
https://www.cisa.gov/news-events/news/staying-safe-social-networking-sites

National Cybersecurity Alliance:
https://www.staysafeonline.org/articles/share-with-care-staying-safe-on-social-media

@radicalKjax

Made by Zoe/Echo419 with support from DC916