# Intro To CyberSecurity – Spring 2023

## Research Project #1: Pre-Proposal

## Due: Monday, March 27th 2022

Highlights

- Expected contribution towards the final score: 1%.
- **You should work on this task individually or in a team of up to 5 members (highly recommended). One submission per team.**
- **Submit your work as a pdf** through the USTC Blackboard

As the first step of your research project (accounting for 20% of the final score), **you need to pre-propose your project and get approval from the instructor before starting to formally propose and work on it.**

The following elements are suggested to be included in your pre-proposal.

- A list of cybersecurity topic candidates (problems) you plan to work on, in the order of your preference. For each topic, **briefly** write a paragraph to *sell* it by answering the following questions**.**
    - The motivations, i.e., why does this problem have its value?
    - The technical challenges of pursuing this research problem
    - How do you plan to address these technical challenges?

**Ping the instructor as a team if you need to discuss potential research ideas.** For example, you can set up a Feishu group to discuss the topic candidates with the instructor.

Below we provide a set of topic candidates for your reference. However, you are not required to select any of them, instead, we encourage you to propose your own.

1. **Fuzzing biological tools (programs)** for security vulnerabilities
2. Get a up-to-date understanding of the arms race between **obfuscation tools** and **de-obfuscation tools**
    - What are the state-of-the-art obfuscation/deobfuscation tools
    - What are their underlying technical mechanisms
    - how well they can work towards their goals
3. Evaluate certificate validation of large-scaled Android apps
    - Adapt the methodologies proposed in this work: On the Complexity of the Web's PKI: Evaluating Certificate Validation of Mobile Browsers
4. Detecting and understanding **misinformation and disinformation** on Chinese public social networks (Weibo, xiaohongshu)
    - Misinformation is false or inaccurate information
5. Detecting and understanding **toxic content** on Chinese public social networks (Weibo, xiaohongshu)
    - Toxic textual content

    - Toxic image/video content
6. Understanding GFW circumvention solutions for websites
    - Example services
        - https://nogfw.org/
        - https://www.zfcdn.xyz/
    - Questions
        - How do they work?
        - What websites are using such services?
        - How effectively can they protect a website from being blocked by GFW?
7. The security/privacy implications of face liveness detection SDKs on Android platform
    - SDK examples
        - ai.advance.liveness
        - com.liveness.dflivenesslibrary
        - com.dfsdk.liveness
        - Com.oliveapp.face
    - Questions
        - How do they SDK works, e.g., whether the liveness detection model is deployed locally on the mobile device or remotely on the server?
        - To what extent do these SDKs get adopted by mobile apps?
        - What are their security and privacy implications?
8. Generating textual description for encrypted network traffic
    - Refer to related works on generating textual description for images
9. Why can free VPNs be free?
10. Detecting and understanding drug trafficking on Chinese social networks