

Final Presentation Topics

Adrianna Holden-Gouveia

Website: aholdengouveia.name

: [aholdengouveia](https://github.com/aholdengouveia)

: [aholdengouveia](https://twitter.com/aholdengouveia)

Accessibility Notice

This document is also available in HTML format at:

Link: <https://aholdengouveia.name/InfoSec/labs/finalpresentation-topics.html>

The HTML version provides enhanced accessibility features including keyboard navigation, screen reader support, responsive design, dark mode support, and high contrast options.

How to Pick a Topic

Pick one topic from this list for your final presentation. The full instructions are in the Final Presentation document, linked under Resources.

- Topics are first come, first served. Claim yours by starting a thread in the Final Presentation discussion on Brightspace, as the instructions explain.
- Two students can't present the same topic. If someone has already claimed yours, pick another one.
- You may pick a topic that isn't on this list, but check with me first.

Topics

1. **Passkeys:** how passkeys work, why they're replacing passwords, and how to set one up
2. **Prompt injection and AI chatbot security:** how attackers trick AI chatbots and assistants into ignoring their rules or leaking data
3. **Attacks on AI models:** data poisoning, model theft, and fake AI models, and how companies protect their AI
4. **SIM swapping:** how attackers take over a phone number, and how to protect yours
5. **Scams aimed at college students:** fake jobs, fake rentals, ticket resale scams, and how to spot them
6. **Gaming account security:** account theft, malware hidden in cheats and mods, and in-game trading scams
7. **Payment app scams:** how scammers use Venmo, Zelle, and Cash App, and how to protect your money
8. **Cryptocurrency scams and wallet security:** common crypto scams, and how people protect their wallets
9. **Romance scams and dating app safety:** how romance scams work, and how to stay safe on dating apps
10. **Ransomware as a business:** how ransomware gangs run like companies, with affiliates, help desks, and negotiators
11. **Election security:** how voting machines, voter rolls, and election results are protected
12. **Attacks on critical infrastructure:** attacks on water systems, power grids, and pipelines, and how they're defended
13. **Hospital cybersecurity:** why hospitals are targeted, and what happens to patient care during an attack
14. **Medical device security:** risks to pacemakers, insulin pumps, and other connected medical devices
15. **Car security:** keyless entry relay attacks, connected car apps, and car hacking research
16. **Drone security and privacy:** how drones can be hacked or misused, and the rules around them
17. **Satellite and space security:** why satellites and GPS are targets, and what happens when they're attacked
18. **Quantum computing and encryption:** why quantum computers could break today's encryption, and what post-quantum encryption is
19. **Bug bounty programs:** how companies pay hackers to find bugs, and how people get started

20. **Careers in cybersecurity:** the main job roles, certifications, and how to get started in the field
21. **Red, blue, and purple teams:** how attackers and defenders practice against each other inside companies
22. **Zero trust security:** what “never trust, always verify” means, and how companies use it
23. **Software supply chain attacks:** attacks like SolarWinds and the XZ Utils backdoor, where trusted software is used to spread an attack
24. **Open-source software security:** who looks after the free code everyone relies on, and what happens when it has a bug
25. **Commercial spyware:** spyware like Pegasus that’s sold to governments, who it’s used against, and how it’s found
26. **OSINT (open source intelligence):** what can be found about a person or company from public information, and how to limit it
27. **Data brokers:** how companies collect and sell personal information, and how to opt out
28. **Biometrics:** how face and fingerprint unlock work, how secure they are, and what happens if they’re stolen
29. **Wearables and health data:** what fitness trackers and smartwatches collect, and who can see it
30. **Public Wi-Fi and evil twin hotspots:** how fake Wi-Fi networks trick people, and how to stay safe on public Wi-Fi
31. **Email authentication:** how SPF, DKIM, and DMARC help stop spoofed and phishing emails
32. **Disinformation and bot networks:** how fake accounts spread false information, and how platforms try to find them
33. **Digital IDs:** mobile driver’s licenses and digital IDs, and how they’re kept secure
34. **Cyber insurance:** what it covers, why companies buy it, and how it’s changing security
35. **Security for programmers:** common coding mistakes that lead to security bugs, and how developers avoid them

Resources

The Final Presentation instructions Link: <https://www.aholdengouveia.name/InfoSec/labs/finalpresentation.html>