

POSTER SESSION GUIDELINES

COMPETITION INFORMATION

Eligible to compete: Full-time undergraduate and graduate students

Submission Deadline: October 11, 2020 at 11:59 PM PST

Contact: Mohammad Husain for any inquiries (mihusain@cpp.edu)

[Submission Link](#)

Mission: The goal of this Zoom presentation is to raise awareness among the fair's audience in a cybersecurity related topic. The format is using the provided power point example along with your communication skills.

Poster board topics: Emerging topics in the field of Cyber Security & Information Assurance, etc.

Sample topics		
Internet of Things	Cloud Security	Mobile Security
E-commerce Security	Secure Coding	Forensics
Authentication	Smart Cities	SCADA
BYOD	Election Security	Cryptography
Physical Security	Digital Profiles	Biohacking

Thanks to the support and generosity of the Los Angeles Chapter of ISACA, competition winners will receive:

- **First Place: \$300**
- **Second Place: \$250**
- **Third Place: \$200**
- **Fourth Place: \$150**
- **Fifth Place: \$100**

IMPORTANT: The Cyber Security and Awareness Fair will only distribute the reward to the team leader. It is then the responsibility of the team leader to redistribute the reward fairly amongst other members of the team. We suggest that you choose a responsible and trustworthy team leader.

Virtual Requirement

Top 5 submissions will be chosen for final presentation at the Cyber Security and Awareness Fair based on the abstract submission. The final judging will be on October 29th, 2020. Contestant/Team **must be available to virtually present content of their abstract from 10am-2pm**. Final judging for the winners will be held between 11am-1pm. Decision of the judges is final. Teams are limited to a maximum of 5 members.

- The virtual presentation will be via Zoom session during the event.
- Visual materials must be comprised of the abstract content and be capable of being easily read on a screen.
- Presentations should be discussed, rather than simply read
- Displays frequently require more planning and preparation and can include more complex figures.
- Contestant/Team will be given a 30-minute window for which the judges will be in attendance of the zoom session.

POWERPOINT SPECIFICATIONS

- Contestant/Team must submit their presentations using the provided Power Point Template.
- Contestant/Teams that do not use the Power Point template will not be accepted.

RECOMMENDATIONS

- Include an identification sign of the abstract including the title of presentation and student(s) name, school, and faculty member.
- Use a large enough fonts and colors to be visible by someone that is visually impaired.
- Be sure to leave enough white space to allow people to focus on what is most important for them to see.
- When using graphics, do not put too much information in one figure or chart.
- When using text, avoid long sentences; instead use bulleted statements.
- If using acronyms, provide definitions.

PRESENTATION TIPS

- Dress professionally.
- Establish eye contact as if you were in a physical room.
- Prepare a short statement to walk the viewers through your figures to discuss your project.
- Be prepared to briefly discuss your hypothesis, point out your work, address key pieces of data, and summarize your conclusions.
- Point to specific parts of your poster as you explain your project.
- Speak to the viewers, not your poster.
- Keep in mind that you likely know much more about your project than the viewers. Don't assume knowledge on their part.

INITIAL REVIEW CRITERIA

- Relevance to the field of cyber security, information assurance and forensics – The topics need be related to the theme of the cyber security and awareness fair. How someone can securely use computing and handheld devices in an Internet connected environment, how not to become a victim of a cyber attacks, discussion of existing cyber attacks and defense techniques for computing and handheld devices including their communication networks
- Potential for practical impact - The topic should be real life application oriented. It should be a topic that can be easily communicated to a non-technical person who might be a user of that technology in real life. An audience should be able to relate it to everyday life and understand the implication of the topic presented.
- Degree of originality - This attempts to evaluate the importance of the study. Judges will consider the following questions: Does the study show originality or creativity in research design and/or interpretation? Does it address a new problem, or an old problem in a new way? Are the study and its results important? Do they shed new light on the issue at hand, or suggest important new methods, procedures, etc.? Or does the study report a necessary and valuable replication of earlier work? Does the abstract make a clear case for how the research fits into a larger context? Does the student address the issue of the study's importance to the field of cyber security, information assurance and forensics? (Please pay particular attention to these last two questions.)

- Technical depth - This will measure whether the presenter has done enough literature review of the existing literature to present adequate information to the audience and be able to answer the queries of an audience.
- The overall quality of the submission – This attempts to evaluate the overall impression of the student’s research achievement. Judges will consider the following questions: Did the observations presented support the conclusions? Was there evidence of progress towards the goals & objectives? Was there evidence that the project led to learning beyond the classroom?