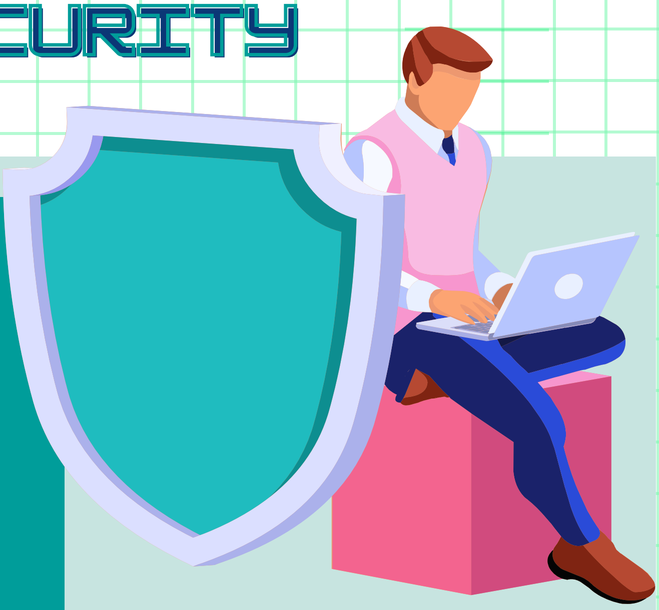
NEBRASKA CYBERSECURITY NETWORK SUMMARY



"The Cybersecurity and Infrastructure Security Agency (CISA) has seen an increase in malicious activity with ransomware attacks against K-12 educational institutions. Malicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible to basic functions, including remote learning. In some instances, ransomware actors stole and threatened to leak confidential student data unless institutions paid a ransom."

https://www.cisa.gov/stopransomware/cyber-threats-k-12-remote-learning-education

To combat the increase of attacks, enter the Nebraska Cybersecurity Network (NCN). The NCN is a network of educational entities, per interlocal agreement, who share in the common interest to improve the landscape of cyber security in their respective areas. Join your like-minded counterparts to take proactive measures to dedicate the resources necessary to keep education safe from cyber threats that are becoming increasingly common in the world.

Here is how to become a partner of the NCN:

- Sign the interlocal agreement
- Commit to the initial contribution amount, which will not exceed $12,000, which provides membership from January 1, 2023 until June 30, 2023. Continuing funds will be decided at a meeting of NCN members in May 2023.
- Attend regular monthly meetings starting January 2023.

What if I cannot contribute the initial funds for the January to June membership?

- Interested ESUs who are not charter members of NCN may join by a vote of the current members, by the terms outlined by the NCN
- Please note that the funds to become a member will increase after the charter membership period has passed.

THE KEY GOALS OF THE NCN ARE THE FOLLOWING:

- Hire dedicated or contract cyber security personnel who will, as applicable and as requested:
  - Primary duties include:
    - Collaborate with industry and education experts to provide the best recommendations for members;
    - Provide analysis of a member’s cybersecurity posture;
    - Reviews external threat intelligence feeds from cyber security agencies, sends alerts and coordinates with responsible parties to patch high risk vulnerabilities;
  - Secondary duties include:
    - Troubleshoots network performance, network security issues and analyzes network traffic;
    - Assist with incident response, computer forensics, data preservation and investigations related to network breaches and/or unauthorized access of data;
    - Interpret and analyze reports regarding risks and vulnerabilities;
    - Helps maintain configuration records and documentation;
    - Assists with the research, testing, evaluation, and implementation of security tools, systems, and processes;
    - Maintains, monitors, and modifies security tools, systems and processes;
- Provide access to group buy opportunities on discounted software and tools, including but not limited to:
  - Endpoint Detection and Response (EDR)
  - End User Security Awareness Training
- Provide access to cyber security grant opportunities, including grants with matching funds.