SET SEG CYBER BREACH PREVENTION

Cyber criminals are attacking public schools at an alarming rate. Malicious actors are exposing personally identifiable information, demanding millions of dollars of ransom, and districts are losing valuable time and money before they are able to regain control of their systems. It's imperative that our members act now to try to prevent breaches before they happen.

TIPS TO PREVENT A BREACH

- Conduct ongoing Security Awareness Training (including simulated phishing attacks).
- Require staff to use a Multi-factor Authentication (MFA) before logging in to a district device or system.
- Apply security patches to your systems and install antivirus updates regularly.
- Maintain separate networks for non-district owned or managed devices.
- Issue unique IDs and passwords to employees connecting to or accessing the internal network.
    - Ensure these passwords require periodic changes and mixed-character combinations.
    - Use password management software.
    - Manage the use of portable media.
- Deploy an Endpoint Protection Product (EPP) to serve as a firewall and block all insecure ports, including Remote Desktop Protocol (RDP) port 3389.
- Do NOT allow school employees to have administrative rights to school devices and applications.
- Establish a business recovery plan and incident response plan and test both regularly.
- Back up computer data and store it off site.
    - Regularly test and verify these backups to ensure they're operating properly.
- Oversee third-party service providers and ensure they're capable of maintaining appropriate security measures.
- Form a Cyber Security Response Team with regular training on cyber breach response.