# Cybersecurity

## Recommendations and Best Practices

As schools rely more and more on technology, they have become potential targets for cyberattacks. Even prior to the rapid adoption of virtual learning due to COVID-19, schools were increasingly becoming the focus of cyber threats. One recent report found there were 348 publicly-disclosed incidents that involved K-12 schools, which was nearly triple the publicly-disclosed incidents in 2018.[i] Successful cyberattacks can lead to data breaches, interrupt school operations, and/or expose students to inappropriate material. While technology is constantly changing, there are numerous best practices that can help to prevent or mitigate a cyberattack.

### Cybersecurity Threats

Schools must safeguard against a variety of cyber threats and cyberattacks that will use multiple strategies. While not an exhaustive list, some of the most common threats schools may face include:

- **Phishing:** Fake emails that pretend to be sent from a legitimate source. These emails attempt to trick the recipient into providing personal information or to click a link that could install malware. Phishing emails may target the recipient by addressing them by name. The sender may also use an email that appears to be from an administrator to attempt to get information from staff.
- **Malware:** A wide variety of malicious software that is intended to damage data, networks, or systems. This includes viruses, spyware, ransomware, etc. Malware can be introduced by phishing emails and can lead to data breaches.
- **Ransomware:** A specific type of malware that encrypts the victim's data and demands a ransom to decrypt the data. The attacker may also threaten to release the data unless the ransom is paid. Paying the ransom does not guarantee the school will regain access to its data and may encourage the attacker to target other organizations.[ii]
- **Data Breach:** Confidential information is accessed by an unauthorized user, is stolen, or is improperly released.
- **Distributed Denial of Service (DDoS):** A network or service made inoperable due to an overwhelming amount of traffic from different sources. This prevents legitimate users from accessing the service.
- **Zoom Bombing:** The interruption of a video conference class or meeting by an individual who is not part of the class. The individual may attempt to share pornographic or other inappropriate content with members of the class.

### District Recommendations

- Ensure that policies and practices follow the Family Educational Rights and Privacy Act, the Children's Internet Protection Act, the Children's Online Privacy Protection Act, and other privacy regulations.

- Incorporate cybersecurity policies into the school or district's Emergency Operations Plan.
- Review policies regarding the use of technology and distance learning and ensure policies address requirements for informational security. Ensure that the entire school community is aware of the policies.
- Ensure staff understands the process for having new tools (e.g., software, applications, browser extensions, plugins, add-ons, etc.) approved.
- Back up sensitive data regularly on an external device that is not connected to the internet. If a ransomware attack occurs, the backup data will not be encrypted if it is separate from the network.
- Use virtual private networks (VPNs) to encrypt traffic if possible.
- Require two-factor authentication (2FA).
- Use strong email spam filters to prevent phishing emails from reaching end users.
- Ensure that content filtering works off campus. School issued Wi-Fi hot spots should have content filtering enabled.

## Recommendations for Students and Staff

Cybersecurity is the responsibility of the entire school community. Both students and staff could be possible targets of a cyberattack so it is important to promote best practices for all stakeholders. Some best practices both students and staff should follow are:

- Require students and staff to agree to an Acceptable Use Policy.
- Only use approved software and tools for school-related work.
- Ensure students and staff keep all devices updated.
- Restrict the ability of students and staff to install software on a district issued device.
- Advise students and staff that school officials or information technology personnel will not request login credentials by email, ask for credit card information, or threaten to remove access to their account if they do not click a link.
- Have a way for students and staff to easily report suspicious emails.
- Notify students and staff if phishing emails have been sent to school email accounts.
- Advise students and staff to update their home routers and use complex passwords.
- Students and staff should use a district issued device for school-related work. If this is not possible and a student needs to use a personal device:
    - Require strong passwords to log in.
    - Close all other non school-related windows and applications while doing school-related work.
    - Keep the device up to date and use an anti-virus software.
    - Advise parents that content filtering will not work on personal devices. Advise parents to enable content filtering on their home network.

## Recommendations for Online Meetings

Virtual learning has unique cybersecurity challenges. It is important to keep class meetings private, student and staff information secure, and to ensure that classes are not interrupted by

individuals who should not be present. Best practices to promote safe virtual learning include:

- Do not make class meetings public unless it is necessary. The meeting link should be sent directly to individuals.
- Advise students not to share the meeting links with strangers and to never share their passwords with anyone.
- 2FA can add an additional layer of security and lower the possibility of the meeting being interrupted by an individual who is not part of the class.
- Limit who can share their screen and manage recording and file sharing permissions.
- Make sure that visual and audio surroundings do not reveal private information when the individual is on camera.
- Teachers should be familiar with security options provided by the video conferencing software. This may include using waiting rooms to approve participants, locking meetings once they begin, disabling cameras, and removing individuals.
- Teachers should have a plan regarding how and when it may be necessary to terminate a meeting.[iii]

If a school or school district has been affected by a cyberattack or possible cyberattack, administrators should contact the Michigan Cyber Command Center via phone at 1-877-MI-CYBER (1-877-642-9237) or email at MC3@michigan.gov.

The Michigan State Police, Office of School Safety, can be reached via email at MSP-SchoolSafety@michigan.gov.

---

[i] Levin, Douglas A. (2020). *The State of K-12 Cybersecurity: 2019 Year in Review*. Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. Retrieved from: https://k12cybersecure.com/year-in-review/.

[ii] *2019 Internet Crime Report* (2020). Federal Bureau of Investigation. Retrieved from: https://pdf.ic3.gov/2019_IC3Report.pdf.

[iii] *Cybersecurity Recommendations for K-12 Schools Using Video Conferencing (*2020). Cybersecurity and Infrastructure Security Agency. Retrieved from: https://www.cisa.gov/sites/default/files/publications/CISA_Cybersecurity_Recommendations_for_K-12_Schools_Using_Video_Conferencing_S508C_3.pdf.