IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CYBER THREATS TO K-12 REMOTE LEARNING EDUCATION

DEFEND TODAY, SECURE TOMORROW

December 2020

The information in this fact sheet is provided for non-technical educational professionals.
**This product was written with contributions from the Federal Bureau of Investigation (FBI).

The Threat and How It Impacts Remote Learning Education

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.

Since March, uninvited users have disrupted live-conferenced classroom settings by verbally harassing students, displaying pornography and violent images, and doxing meeting attendees.

For detailed information on these threats and actions to take, visit the Joint Cybersecurity Advisory on this topic, jointly developed by CISA, FBI, and the Multi-State Information Sharing and Analysis Center.

Common Cyber Terms and Concerns

MALICIOUS CYBER ACTOR
Person, group, or entity that creates all or part of an incident with the aim to impact an individual's or organization's security.

DOMAIN SPOOFING
The act of registering web domains similar to legitimate websites in an attempt to trick individuals who mistype URLs or click on similar looking URLs.

DOXING
The act of compiling or publishing personal information about an individual on the internet, typically with malicious intent.

END OF LIFE SOFTWARE
Out-of-date software and equipment that no longer receives patches, security updates, technical support or bug fixes, making the user vulnerable to attacks.

PHISHING/DECEPTIVE E-MAILS
The fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card or bank account details, by disguising oneself as a trustworthy entity in an electronic communication.

What's in this overview:

General Cybersecurity Best Practices

To minimize service disruptions, CISA encourages educational providers to review and establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by cyber threat actors.

PREPARING FOR LIKELY ATTACKS

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Set antivirus and anti-malware solutions to automatically update and conduct regular scans.
- Monitor privacy settings and information available on social networking sites.
- Do not pay ransoms. Payment does not guarantee files will be recovered. It may also inspire cyber actors to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and fund illicit activities.
- Configure network firewalls to block unauthorized IP addresses and disable port forwarding.

Video-Conferencing Best Practices

- ***Ensure*** participants use the most updated version of remote access/meeting applications. Require passwords for session access.
- ***Encourage*** students to avoid sharing passwords or meeting codes.
- ***Establish*** a vetting process to identify participants as they arrive, such as a waiting room.
- ***Establish*** policies to require participants to sign in using true names rather than aliases. Ensure only the host controls screensharing privileges.
- ***Implement*** a policy to prevent participants from entering rooms prior to host arrival and to prevent the host from exiting prior to the departure of all participants.

Information Resources

CISA encourages K-12 education entities to become MS-ISAC members. MS-ISAC provides multiple cybersecurity services and benefits to help K-12 education entities increase their cybersecurity posture. To join, visit learn.cisecurity.org/ms-isac-registration.

- CISA Telework Guidance and Resources
- CISA Cybersecurity Recommendations and Tips for Schools Using Video Conferencing
- CISA Ransomware Publications
- CISA Emergency Services Sector Continuity Planning Suite
- CISA-MS-ISAC Joint Ransomware Guide
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA Tip: Understanding Patches
- CISA and CYBER.ORG “Cyber Safety Video Series” for K-12 students and educators
- FBI PSA: “High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations”