FDD | CSC 2.0

cybersolarium.org/projects

BOOST YOUR SCHOOL'S SAFETY BY TAKING THESE STEPS TO PROTECT EMPLOYEES, STUDENTS, AND FAMILIES

Organization - Wide Training

How? Incorporate cybersecurity training into mandatory back-to-school meetings and reemphasize the training in meetings throughout the year

Why? Users are the first line of defense against cyberattacks. Training can prevent users from falling victim to scams

Limit Exposure to Suspicious Content

How? Set up email filters to automatically quarantine spam and suspicious emails. Teach all users to be cautious with links and attachments from unknown senders and to notify IT personnel of suspicious emails
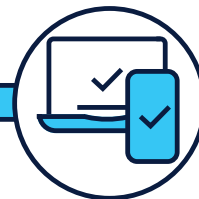
Why? Defends against email phishing, the leading way ransomware attacks begin

Update and Patch Software

How? Set up automatic security updates on all devices

Why? Cybercriminals exploit known vulnerabilities in software that has not been updated

Use Multi-Factor Authentication

How? Use a combination of strong passwords along with a verification code sent to a cell phone, email, or authentication app

Why? Reduces risk of successful cyber breaches. MFA blocks 100% of automated bots, 99% of bulk phishing, and 66% of targeted user attacks

Monitor Suspicious Network Activity

How? Install antivirus software for continuous and automatic threat detection and take advantage of the free scanning resources offered by the Cybersecurity and Infrastructure Security Agency (CISA)

Why? Early detection can prevent or mitigate the worst of the damage of cyberattacks

Practice Incident Response and Build Relationships

How? Develop a cybersecurity incident response plan using CISA's guide and build relationships with local cybersecurity and law enforcement authorities

Why? Minimizes negative impact of attacks by ensuring operational continuity and minimizes educational disruption in the event of an attack

Back up Data

How? Set up automatic daily backup to at least one onsite and one offsite location

Why? Ensures data recovery and minimizes operations disruptions in the event of a cyberattack