Member Exclusive
March 2020

# Cybersecurity Considerations in a COVID-19 World

With the declaration of COVID-19 as a global pandemic, school systems across the country are closing their doors, restricting travel, and moving to remote or distance learning models in an effort to provide learning continuity. It is essential to consider cybersecurity and privacy before implementing technology-driven alternatives to classroom learning. Neglecting to consider cybersecurity and privacy until the end of the planning and implementation process or forgetting about them altogether poses significant security and privacy risks for students and educators. This resource highlights key considerations for protecting students, staff, and data.

## Protecting Educators, Parents, and Students from COVID-19 Scams

Crises of any kind provide hackers endless opportunities to exploit people when they're already feeling vulnerable. One common tactic is to spread misinformation and trick end users into sharing login credentials, credit card information, and other personal details through phishing attacks that appear to be official messages from the school or district.

School systems can help their staff, students, and parents avoid phishing attacks by providing clear guidance with regard to district methods of communication.

- Clearly identify all official methods of communication. Direct constituents to official web pages and social media sites to obtain information. Be clear that other sources are not authoritative or accurate.
- Remind end users that IT staff will never ask for their login credentials via email or threaten to turn off access to school accounts if they don't click on a link.
- Consider implementing two-factor or multi-factor authentication whenever possible. If this is too difficult to implement quickly, start with the information technology and finance staff, who pose the highest risk if their credentials are compromised.
- Consider reviewing/enabling email settings for Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKM) to validate that email messages have been sent from authorized or approved mail servers. This will help prevent spam and identify-forged or spoofed messages.
- Advise students and parents that they should not expect to pay for, or provide a credit card for, access to school resources.
- Avoid sending emails to staff, students and parents that contain links.
- Provide staff, students and parents with an email address to which they can forward suspected phishing attacks. Evaluate the forwarded emails and post a list and description of known phishing attacks online so recipients can see if they've received a similar email.

### Remind Educators to Protect District Equipment and Data

With an increased number of educators, using district owned devices for off-site work consider the risks and remind personnel of their responsibilities when using district devices off campus. Specific steps to take include:

- Encrypt hard drives to ensure that data is protected, even if the device is lost or stolen
- Review district procedures and guidelines regarding non-employee use of district devices. For example, can family members use a staff device? What if the family member is a student using it to access remote learning materials?
- Determine employee permissions for district-owned devices. Can they add users and profiles? Are they allowed to install software? If so, under what circumstances?
- Determine if staff may use tools such as Google backup, Dropbox, etc. that automatically sync files and passwords to the cloud. If improperly configured, these sync options can result in the exfiltration of data to an employee's personal cloud account(s). Make sure sync options are configured correctly and only for district- owned cloud storage. Provide clear guidance on device transportation and off-site storage.

## Set Security Basics in Place for Online Learning

As schools and districts rush to move learning online, it is important to make sure good cybersecurity practices are in place. The CoSN Member Bulletin Preparing to Take Your Schools Online describes in detail a range of instructional, infrastructure and equity considerations. This brief focuses specifically on device and network security. While quickly scaling teaching and learning in a distributed environment may be the primary goal, security should remain a priority.

*Planning for Web Content Filtering*

One challenge faced by districts quickly making the transition to online learning is not having enough devices for students. As a result, students may need to use both district-owned and personally-owned computing devices to access online resources. Campus-based web content filtering may not be available when devices are used off campus. Important content filtering considerations include:

- Ensuring that district devices can continue to provide content filtering when off campus. If filtering is not available, clearly communicate this to parents.
- If district devices are not currently filtered off campus and the district decides to enable remote web filtering, this decision needs to be clearly communicated to all staff, parents and students.
- Districts allowing students to access district resources using personally-owned computers should notify parents that content filtering would not be provided if students use their browser to access non-school resources. Parents should be advised to either monitor student activities or enable content blocking on their home network or devices. Several free resources for parent-enabled content filtering are available online.
- Districts may also opt to provide wireless hotspots to students who lack home Internet access. Local laws/congregation restrictions must be taken into consideration. Content filtering should be enabled on these devices and the default administrative password changed before the device is deployed to the student.

*Classroom Supervision*

The shift to online instruction creates challenges for teachers. Teaching in an online classroom is very different from an in-person classroom. Consider all available options to mitigate risk with regard to student interactions and classroom monitoring. Potential options may include:

- Turning off student-to-student video chat in classroom environments.
- Allowing students to contact teachers using softphones, district-provided cell phones, email, conference calling, and district approved messaging services to protect teacher's personal phone numbers and allow them to turn off the phone at the end of the day.
- Leveraging asynchronous instruction methods such as email and/or learning management systems that do not require students to be present online at the same time.

*Availability*

Availability is one of the three pillars of effective cybersecurity practice (confidentiality, integrity, availability. A device isn't any good if it is not available for use. It is important to plan for and try to prevent damage to district devices such as laptops and tablets. Consider the following:

- To ensure continued access to online resources, determine how to handle password resets. Determine when and how to make self-service options available. For systems without self-service password reset options, determine how password resets will happen. For example, can students receive their password at a non-district provided email? Other options are to send the passwords to parents via US mail. Or alternatively, a previously documented email address? Will the school or district reset all passwords and require the temporary password be changed immediately?
- Before distributing devices, identify your inventory and checkout process. This will accelerate the response to automatic notification processes, such as virus alerts, that may require resolution from IT support staff.
- During a pandemic, inappropriate cleaning procedures pose a significant risk to district devices. Users concerned about spreading the virus through keyboard and tablet screens may unintentionally damage devices. Provide clear instructions to staff, students and parents on how to clean and care for district devices. Advise against the use of paper towels, Windex, alcohol or ammonia-based cleaners, and significant quantities of water. Keyboards, but not screens, can be cleaned with antibacterial wipes. Instruct users to power off devices before cleaning, use a very slightly damp soft cloth or microfiber cloth, and dry gently. Remind users not to press on the screen.
- Determine how to handle damaged devices. There is a standard failure rate for devices, especially when deployed off campus. Develop a plan for troubleshooting technical support issues remotely, possibly providing onsite repair, and replacing devices as needed. Because the international nature of the pandemic may result in significant supply chain issues, be prepared to handle device repair or replacement creatively. Remember to disinfect recovered devices as current guidance indicates the virus may live on certain surfaces for up to three days.

- Tech support in districts is often building centric. Consider if this is a viable approach in the event of school closures.

## Consider and Plan for the Privacy Implications of Online Learning

In addition to cybersecurity considerations, it is also important to ensure the staff and student privacy when deploying online instruction. There are several distinct issues to consider when leveraging video-enabled teleconferencing:

- Do schools enable the ability for students to initiate video and/or chat? If so, is the teacher required to be present or are students allowed to converse privately? Examining the privacy concerns of turning on a webcam in a private home. That applies to be teachers and students.
- The second issue revolves around the privacy concerns of turning on video interactions in the homes of educators and students. Turning on a webcam in someone's private home can potentially be viewed as invasive. Teachers and students may be uncomfortable with video conferencing or may not have an appropriate space in their home to do so. Consider when and where it is appropriate to use video conferencing. Is it one way, or bi-directional? Teachers may prefer to record video material from campus instead of web conferencing from home.
- Remind teachers not to do confidential work when they are on unsecure network like Starbucks or McDonalds.
- Sending a batch email to parents is not a best practice. School's messenger system OR using the BCC ensures parents' emails will not be shared with the entire group.
- IT Leaders need to have multiple discussions with staff about their process for getting new learning resources approved. Teachers should not be entering into click wrap agreements because they may be agreeing on behalf of their school district, which is probably not authorized.

In addition, students may be reluctant to admit that they don't have adequate home access to devices or broadband. Determine how the district will provide support, devices and Internet connectivity to students while not singling them out among peers.

Remember that COVID-19 and efforts to deliver instruction in non-traditional ways do not negate FERPA and the requirement that schools and districts protect the privacy of students' educational records. Additional guidance specific to COVID-19 and FERPA is available at the US Department of Education at: https://studentprivacy.ed.gov/resources/ferpa-and-coronavirus-disease-2019-covid-19

Cybersecurity and privacy considerations should be at the center of district plans to support instruction through any natural disaster and certainly a pandemic. Failure to include them in the planning and execution of short, medium and long-term COVID-19 response plans can put network security and stakeholder privacy at risk.