CENTER FOR DEMOCRACY & TECHNOLOGY

CYBERSECURITY IN EDUCATION

PROTECTING STUDENT DATA & SYSTEMS

August 2021

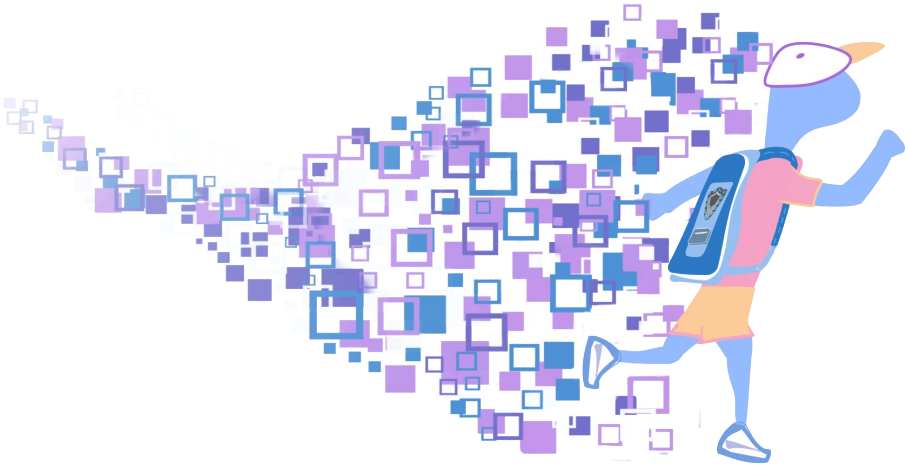
Introduction to the Training Module

Welcome to the Center for Democracy & Technology's training on Cybersecurity in Education. The goal of this training is to equip **state and local practitioners**, including administrators and teachers, to protect their technology and data against hacking and other attacks.

In this material, we will cover:

- The importance of cybersecurity in an education context.
- Important terms and definitions.
- Best practices for keeping systems and data safe.

MOTIVATION AND KEY TERMS



Cybersecurity is Critical to Protecting Students

Cyberattacks can put students, families, and school employees at risk by exposing their personal information, putting them at risk of financial damage, or even physical harm when their addresses are exposed. It can also deprive students of instructional time as schools take time to restore their systems in the wake of an attack.

FBI alerts of rise in PYSA ransomware targeting schools

The 'real consequences' of ransomware against schools

K-12 Schools Warned of Increasing Cyber-Attacks in U.S. Advisory

School cyber-attack affects 40,000 pupils' email

FBI alerts of rise in PYSA ransomware targeting schools - SecurityMagazine.com
The 'real consequences' of ransomware against schools - StateScoop.com
K-12 Schools Warned of Increasing Cyber-Attacks in U.S. Advisory - Bloomberg.com
School cyber-attack affects 40,000 pupils' email - BBC.com

Cybersecurity and Privacy

Security and privacy mindsets are critical to keeping students and the community safe. While there is overlap between these two facets of data and system protection, they serve different purposes and require different approaches. This presentation will use the following definitions for security and privacy:

- **Privacy** is the idea that people should be able to control their own information, and that the entities that are authorized to collect and use that information do so in ways that respect an individual's autonomy. Privacy-forward approaches often include things like strong data governance practices and community engagement around data use and collection.
- **Security** is the practice of preventing damage or unauthorized access to information and the networks and systems that transmit or hold it. Security-forward approaches include steps such as maintaining up-to-date systems and requiring strong passwords.

Cybersecurity Is Everyone's Job

Computer systems generally need to allow multiple people to interact with systems and data to some extent in order to do their jobs. Teachers need to be able to input and review grades for their students, administrators need to be able to view class schedules and manage staffing, etc.

Because all of these interactions represent a security risk (whether because the user makes a mistake or because a malicious actor is able to take advantage of their access), anyone who interacts with systems and data bears a responsibility for protecting students, families, and the school community.

- Because of this shared responsibility, everyone who works or interacts with a school's technical systems needs to play a role in keeping the system secure. For example:
    - All users must prioritize the security of their accounts in the systems, such as by not sharing their passwords with others.
    - Teachers who need to use apps as part of their efforts should work with IT and administrators to find privacy- and security-friendly options.

KEEPING ACCOUNTS SECURE

Keeping Accounts Secure

A key element of system security is ensuring that the accounts on the system are themselves secure. That means ensuring that only the intended user has access to the account. This provides important security and privacy assurances:

- Malicious actors cannot steal a legitimate user's access to data or manipulate the system.
- IT and other technical staff can be confident they know who is accessing systems and their data and, in turn, ensure those users are properly trained.
- Security frameworks, like those that keep track of who accesses certain data, can be trusted to be accurate.

This section will discuss a number of security practices that help keep accounts secure.

Passwords

Strong passwords are a critical component of keeping accounts and information secure. Unfortunately, they can also be hard to remember. This tends to lead to users having to reset their passwords often, write their passwords down, or reuse passwords for different accounts. Each of these workarounds make passwords less effective:

- If users are regularly resetting their passwords, either they will be frustrated by that process (if the reset process is too hard), or the reset process itself can be a way for attackers to gain access (if the process is too easy).
- If users are writing down passwords, particularly in a shared space like an office or classroom, it can provide an easy way for unauthorized users or bad actors to gain access to a system.
- If users are reusing passwords across multiple accounts, it can mean that if an attacker gains access to one account, any other accounts with that same password are likely to be compromised as well, exacerbating the damage of the compromise.

Password Managers

One way users can minimize the problems associated with passwords is to use a password manager. Password managers are tools that store all of a user's passwords, protected by a single primary password (which should be very strong).

There are some considerations schools should consider when using password managers:

- If a user's primary password is not strong enough, an attacker can gain access to all of a user's passwords in one go, so schools should educate users about what makes a strong password and why it is important to use one in this context.
- If a user forgets their primary password, they are essentially locked out of everything, and it can be time-consuming and frustrating to regain that lost access. Schools should have a process in place for helping users restore access in this instance.

Multifactor Authentication

Another technique users can use to make password-based systems more secure is *multifactor authentication*, or MFA (sometimes referred to as "two-factor authentication" or 2FA). MFA systems add another "factor" to the login process, often a single-use code sent to or generated by the user's phone each time they go to log in.

This means that even if an attacker gets hold of a user's password, they still need the extra code to get into the account, which is difficult to obtain without access to the user's phone.

For many systems managed or maintained by the school (like Google for Education), the system administrator needs to enable MFA for user accounts. Users should talk to whoever maintains their software systems (like their IT department or a CISO) to ask them to enable MFA.

PROTECTING SYSTEMS FROM ATTACK AND MISUSE

Operational Security - Part 1

Operational security, or OPSEC, is the practice of protecting yourself or your systems against attacks that don't rely on software or hardware vulnerabilities, but rather on manipulating users or taking advantage of mistakes.

- Social engineering is the practice of manipulating people to divulge sensitive information or skirt security practices. Most common is pushing people to break security rules by pressuring them to follow *social* rules, like gaining access to a secure building by walking behind someone close enough that they feel obligated to hold the door.
    - Users can avoid these types of attacks by following security protocols at all times, even if it feels rude, and by seeking help or double-checking protocols when something feel suspicious to them.
- One common OPSEC vulnerability is "shoulder surfing," the simple act of looking over someone's shoulder as they access sensitive information.
    - To prevent these attacks, don't access sensitive information in insecure spaces, like coffee shops. Privacy shields for computer screens can be helpful, but they don't block all visibility, so you still need to be aware of people seated directly behind you.

Operational Security - Part 2

In addition to social engineering, there are a number of other common OPSEC attacks targeting documents.

- "Orphaned" documents are documents left unattended on printers or in other public spaces, such as communal mailboxes. To avoid unauthorized people from reading documents, you should collect them immediately upon printing.
- Documents left in recycling or trash bins can also be grabbed by unauthorized users, so sensitive documents should be shredded rather than recycled or thrown away.
- Additionally, documents should not be left unsecured in semi-public spaces, such as desks or teachers' lounges, as this may still lead to unauthorized access, whether by colleagues, students, guests, or attackers who have gotten into the space.

What is Phishing?

A very common type of OPSEC attack is “phishing,” usually via emails. Phishing emails are generally designed to trick a user into revealing personal or confidential information, or to click a link or open a file (such as a word document or spreadsheet) that is then used as a way to download malicious software onto the user’s system, allowing them to steal data or damage the system. There are two main kinds of phishing attacks:

- General phishing emails are sent to large numbers of people, and are not specific to the user. Sometimes, this can make them easier to spot, but they can still appear legitimate, like a request to fill out a new timesheet that appears to come from HR.
- “Spear phishing” emails are crafted for a specific user, often referencing specific personal details. This can be used to make the email feel more urgent or important, making the user more likely to provide the requested information or open the malicious link.

How to Spot Phishing

There are a few ways of spotting phishing emails, though most of these aren't foolproof, so when in doubt, you should always reach out to your system administrator or technology manager.

- Checking the sending email address may help identify a phishing email. An email that claims to be from a colleague but is not sent from their usual work email can be cause for concern.
- Emails that appear to reference a conversation that you do not remember having, or impose urgent deadlines for work that you don't remember agreeing to do, should also be treated with caution.
- If you are at all uncertain about an email, contact your system administrator or, if you know the supposed sender, contact them via phone or their usual email address to ensure that they actually sent the email.

Insecure Networks

Accessing systems in an insecure internet network, like coffee shop or airport wifi, may also leave anything you access open to attackers.

- Sensitive information should only be accessed while using a secure internet network. This means a network protected by a strong password, not an “open” network that allows access to anyone. Additionally, even password-protected networks may still allow other devices on the same network some access to your information. It is best to only access sensitive information on a trusted network, such as your home or work networks.

- For your home network, a strong password will help protect you and your systems. Additionally, because a home is typically more of a secure environment, writing passwords on paper is less of a concern than in a more public or shared space.

Secure Settings and Best Practices

- Secure systems settings can play a key role in protecting students.
    - Setting up video conferencing settings to ensure that only authorized attendees are admitted to meetings can protect students from traumatic experiences like Zoombombing.
        - Set passwords for meetings to prevent unauthorized attendees.
        - Enable waiting rooms to ensure teachers can maintain control of the entrants to the class or meeting.
- Best practices should also govern the channels for sharing and communicating sensitive information.
    - When discussing student information with other teachers or staff, consider the communication channel to ensure that it is sufficiently secure. For instance, sending sensitive information over email should be avoided, since email is not secure enough for truly sensitive information. Instead, consider something like a secure file transfer.

Keeping Systems Up to Date

Keeping software and operating systems up-to-date is an important security practice, because software developers typically try to address security issues in their software once they know about them. Once they have a fix for a security update, they will send that fix (known as a “patch”) out to their users to install. Installing that patch makes the software more secure.

- Where possible, turn on automatic updates so that the system will always have the most up-to-date security patches.
- For systems that don’t allow automatic updates, check for updates regularly, and install updates in a timely fashion when one is available.

TECHNICAL ASSISTANCE

Establishing Clear Avenues for Assistance

Teachers and administrators are likely not experts in all of the technology they use. Consequently, it is important that they have a way to seek help should they need it.

- Schools should have a channel for teachers and administrators to communicate with technology managers if they encounter concerns or issues.
- They should also have a channel to ask questions or seek clarification about technology policies.
- Teachers should ensure they know what these channels are and how to access them if needed.

WRAP-UP

Wrap-Up

Thank you for participating in this training. We hope that this is helpful in providing an overview of the importance of cybersecurity in education, as well as some of the steps that you can take to protect yourself and your school community.

To help build on this training, we've included resources from organizations working to secure schools' technical landscapes.

Please send us feedback on how we can improve this training and feel free to reach out with additional questions.

Cybersecurity Resources

- **CISA Cybersecurity Resources:** The Cybersecurity and Infrastructure Security Agency maintains extensive cybersecurity resources at a variety of levels: https://www.cisa.gov/cybersecurity
- **MS ISAC:** The Multi-State Information and Analysis Center offers government organizations resources to strengthen cybersecurity and enables organizations to share information and learn from one another: https://www.cisecurity.org/ms-isac/
- **PBS Learning Media:** PBS offers cybersecurity educational resources to help teach novice users about the importance of cybersecurity: https://nm.pbslearningmedia.org/resource/nvcy-sci-cyber101/cybersecurity-101/
- **Data Deletion in Education:** CDT's issue brief on data deletion and retention offers guidance on how to inventory, archive, and delete data to reduce the risk and severity of potential cyber attacks: https://cdt.org/insights/report-balancing-the-scale-of-student-data-deletion-and-retention-in-education/
- **PTAC Data Security Resources:** The Privacy and Technical Assistance Center of the U.S. Department of Education offers resources on maintaining data security: https://studentprivacy.ed.gov/security

Cybersecurity Resources

- **Common Sense Media resources for parents:** Common Sense Media offers resources for parents to help them in managing their children's devices and accounts: https://www.commonsensemedia.org/privacy-and-internet-safety
- **Phishing detection tips:** The Freedom of the Press Foundation offers a primer about detecting and managing phishing emails: https://freedom.press/training/email-security-tips/

CDT'S VISION

PUTTING DEMOCRACY AND INDIVIDUAL RIGHTS AT THE CENTER OF THE DIGITAL REVOLUTION

CDT's Equity in Civic Technology Project

- *Provide **balanced advocacy** that promotes the responsible use of data and technology while protecting the privacy and civil rights of individuals.*
- *Create **solutions-oriented policy resources** that are grounded in the problems that currently confront policymakers, practitioners, and technology providers who work with them.*
- *Offer **technical guidance** that can be adapted and implemented by policymakers, practitioners, and the technology providers who support them.*

Contact Us

Equity in Civic Technology Project
Center for Democracy & Technology
CivicTech@cdt.org