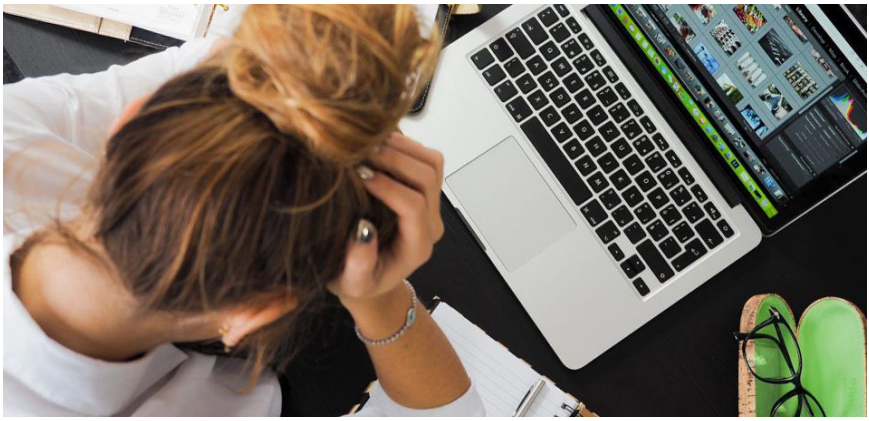
Online Safety

Royce Kimmons



Learning Objectives

- Understand common threats to personal security online (e.g., malware, hacking, phishing) and how to recognize and counteract them;
- Understand legal and ethical requirements placed upon teachers to keep students and their information safe and secure (e.g., privacy, inappropriate content, cyberbullying, child pornography);
- Recognize strategies for making a classroom safe and secure for students' online activities.

Since there has been an internet, there have been those who seek to use it for malicious purposes. Many of these people have very sophisticated understandings of both human nature and internet technologies, and this allows them to take advantage of those with limited understanding of these technologies or who are naive in providing sensitive materials online. As a user of the internet and as a teacher, it is essential for you to understand these threats and to develop strategies for addressing these threats in your own life and in the lives of your students. We will approach this issue from two directions. First, we will consider how teachers should seek to ensure their own personal safety and security while using these technologies, and then second, we will explore how teachers should safeguard their students in the classroom and beyond.

Watch on YouTube https://edtechbooks.org/-qQ

Key Terms

Child pornography

: any pornographic or illicit depiction of a child; viewing, sharing, or owning child pornography is a felony in the United States

Cyberbullying

: a form of bullying that uses internet and other technologies as a means for perpetrating bullying behaviors

Hacking

: when a person or program bypasses or tricks normal security procedures in order to gain access to a site or service

Malware

: malicious software or any software or app that is designed to steal your personal information or cause your electronic devices to behave improperly

Phishing

: an attempt to maliciously exploit sensitive personal information online; a play on the word "fishing," because it implies the use of bait to trap a victim

Personal Security

In this section we will explore three ways that those with malicious intent may seek to make your personal online experience less secure

and less safe through malware, hacking, and phishing. As we explore each, we will provide examples of how the threat might impact lay internet users and also provide guidelines for simple threat reduction or prevention.

Malware

Malware or malicious software is any software or app that is designed to steal your personal information or cause your electronic devices to behave improperly. It was recently estimated that the number of malicious programs created and available on the web now exceeds the number of non-malicious programs and that about 7% of all downloads that users make are malicious in nature.

There are many different categories of malware. Viruses are some of the most well-known, which are typically designed to delete your information or do your computer harm, but there are many other forms as well. Spyware is very common and is software designed to spy on you while you use your device or the Internet, collecting information about you as you go. You may not believe that what you do on your device is particularly interesting and wonder why anyone would want to spy on you, but the simple answer is that information is valuable and that you provide a lot of information on your device that might be profitable to someone. This information includes financial information, such as credit card or bank account numbers, or personal information, such as Social Security numbers, addresses, or phone numbers. a third category of malware is bloatware, which is a type of program that may not necessarily be malicious, but merely takes up space, slows down your device, forces you to view advertisements, or does other things that are not conducive to the kind of experience you want with your device.

Most modern devices are equipped to deal with malware and new updates are released almost daily to combat these threats, so there is little possibility that your device will become infected on its own as

long as your software is up to date.

The real problem with malware is that it is typically installed or spread by accident as users circumvent security measures on their own devices or are tricked by a website or program that seems legitimate. For instance, you might go to a website and see a popup that says you have 98 viruses on your computer and that you should click a button to scan your computer. By clicking that button, the website is actually trying to get you to download and install malware. That is, people are often tricked to install malware by thinking that they are removing it. For this reason, you should never trust any popup unless you know what program it is coming from. If you have an anti-virus program on your computer and it detects malware, any popups warning you of this threat will be clearly identified as belonging to that program. If, however, you see a pop up that comes from any other source, then you can know that it is malware, and you should not click on it.

Another common way that malware is spread is through email. If you receive an attachment through email that you have to click to open, by clicking that attachment you may install something malicious on your computer. For this reason it is important to know and understand the types of files that you might receive over email and how to identify legitimate files. The simplest way to identify a legitimate file is by looking at the file extension, or the part of the file name that goes after the period, such as .pdf, .xls, .zip, or .doc. Each of these file extensions signifies a different type of file. Some of these types of files are commonly used to spread malware while others are safer.

Some of the most dangerous file types that you need to be aware of include the following: .exe, .msi, .dmg, .zip. Just because a file has this extension does not mean that it is necessarily malicious, because there are many legitimate files and programs that use these extensions, such as legitimate programs that you may download from the Internet. However, you typically should not expect to receive these kinds of files in an email. So, if you see one of these types of files in an email, you should be very careful about installing it and only do so if you can verify the legitimacy of the sender.

If you have malware installed on your computer there are two simple things you can do to help remove it. First, if you see a program running on your computer that you do not recognize or that you think should not be there, you can uninstall it. On some operating systems, you can even find a list of all the programs installed on your computer and go through the list one by one, removing any programs that you think are not legitimate. When you do this, some malware will not allow you to completely uninstall it or will install a second program

when you try to uninstall the first. Sometimes this means that you will have to go through and uninstall multiple programs in a row in order to clean your computer but also that you may not ever be able to remove everything on your own.

The second step is to install a legitimate antivirus program and allow it to clean your computer for you. There are many legitimate programs available online or at the store, but not all are equal. To figure out what kind of antivirus will work best for you, consider reading reviews from reputable sites. Most legitimate antivirus programs require an annual subscription fee (e.g., McAfee, Norton), but there are some companies as well that may have an introductory version of their antivirus software that is available for free or on a trial basis (e.g., Avast!, AVG).

Hacking

Eine Computer-Tastatur by Colin, CC BY-SA

In the context of online security and safety, a **hack** is when a person or program bypasses or tricks normal security procedures in order to gain access to a site or service. Hacks can be problematic for everyone, because it means that a hacker can gain access to personal information about users, such as credit card information or passwords, or make online purchases or use services without consent. Even legitimate websites can sometimes be hacked, giving hackers access to company information or personal information of users.

Sometimes these websites are hacked at a site-wide level, wherein lots of users' information is compromised, but it is more often that they are hacked at the user level, wherein a hacker gains access to a single person's account.

As a lay user, there's not anything you can do to prevent a site-wide hack, but you should recognize that such acts are possible and that any website you give your information to has the possibility of being hacked. This means that if you are not certain that the website values your security and privacy or that it is run by a company that has the technical expertise necessary to counteract potential hacks, then you should be hesitant to provide information to such a site. Additionally, if a site really doesn't need certain information about you (e.g., does Facebook really need to know your address), then you should consider not including this information.

Personal hacks, however, are much more common and preventable. Most personal hacks occur for one of three reasons: 1) failure to logout, 2) weak passwords, or 3) unsecured wifi. The first reason is the easiest to counteract, because it typically occurs on a device that is either publicly used or shared by multiple users. If someone else has access to the device, then you should logout of your accounts as soon as you are done. Many people, for instance, have their Facebook accounts hacked my roommates, family members, or friends, and though this may not lead to financial or legal trouble, it can have social ramifications that could be avoided by a simple logout. Also, if you are using a shared computer, do not allow the web browser to remember your passwords. Rather, ensure that if anyone wants to get into your account on that device, then they will have to enter your username and password themselves.

The second way to prevent personal hacks is to use secure passwords. Passwords that are short or that use common words are easy to guess. Some sites will show you the strength of your password when you first create it or even require you to create a password that meets certain

security requirements. The more complex and lengthy your password is the more difficult it will be for someone else to guess it. For this reason, you should introduce complexity into your password in one or more of the following ways: use both upper and lower case letters; use both letters and numbers; when possible, use symbols; use a complete sentence or lengthy phrase; and avoid common words (e.g., "lucky") or common word variants (e.g., "1ucky"). You should also consider changing your passwords frequently and using different passwords for different sites. Having multiple passwords can be unwieldy and difficult to remember, so you may want to consider using a password manager such as Keychain Access on Mac OSX, KeePassX, or LastPass to help you keep track of many different or difficult passwords.

And the third way to avoid personal hacks is to only use secured wifi or to avoid doing sensitive work over unsecured wifi. This is especially important in highly trafficked public areas, such as airports, university campuses, or markets. When you connect to wifi, you will typically be warned if the wifi is unsecured, and secure wifi is typically identified by your device with a security symbol (such as a lock).

If you access the internet over unsecured wifi, this means that any information your device sends or receives may be intercepted by a third party. So, submitted sensitive information over unsecured wifi (e.g., passwords, credit card numbers) could be intercepted and recorded by someone else "listening" for data on that wireless network. Being already logged into a site before connecting to the unsecured wifi could be problematic as well, because someone could "listen" to your credentials for that site and hijack your session (e.g., if your email account is already open, they could potentially begin using it).

There are ways to make an unsecured wifi network more secure for sensitive use (e.g., using a VPN), but this typically requires third-party software and some technical know-how. Generally speaking, if you are

using an unsecured wifi network, then you should avoid doing any sensitive work and be careful about the sites you access and the information you submit, because this might open you up to a personal hack.

Phishing

One final way that sensitive personal information can be exploited by those with malicious intent is through the use of phishing scams. **Phishing** is a play on the word "fishing," because it implies the use of bait to trap a victim. Phishing scams take many forms, but the most common form is through an email and fake website combination.

You might receive an email that tells you that your bank account password has expired and that you must login to update your password. When you click on the link, it takes you to a site that looks like your bank, and this site has fields for you to enter a username and password. If you enter your username and password into these fields, the website will record this information, and the scammer who created the site can use it to log into your actual account without your knowledge. Another variation of a phishing scam might be an email that asks you to send your personal information including credit card information, usernames, or passwords to an email administrator at a particular address. Both of these types of scams are dangerous, because they can extract information directly from users that scammers can then use to access sensitive information or resources online.

To avoid phishing scams, there are three easy guidelines to follow. First, never send sensitive information to anyone over email. Actual administrators will never ask for your password or other information over email, and fake email addresses can often look legitimate. Also, email addresses can be hacked, and there have been cases where hacked email addresses of people in administrative positions have been used to request additional passwords from others.

Second, if you receive an email that gives you a link to follow, be suspicious of the link even if it seems to come from a legitimate source. Typically, if you hover your cursor over the link you can see the full address. Sometimes, a scammer may send you an email that claims to be from your school, university, or financial institution and give you a link to login to a site that purportedly belongs to that institution. When you hover on that link, you should see the full address and can determine whether or not it really is linking to the intended destination. Often, the text of the link will say one thing but actually link to something very different.

Third, before you enter username or password information into any sensitive site, such as an online banking system, university email system, or online shopping site, check the address to see if it is a secure site. Most website addresses begin with the letters "http," which stands for Hypertext Transfer Protocol. This is the protocol used for most standard websites that you access on the Internet, and if you cannot tell, you should assume that the site uses HTTP. HTTP,

however, is not a secure protocol. Anyone can create a site that begins with "http" without any type of verification, and for this reason, scammers will often create sites that look valid in order to steal your information.

If the URL begins with "https," however, this is a very different story, because "https" is the secure version of "http." Setting up an HTTPS site requires more verification than the alternative, which means that it is less likely to be a phishing site. All major sites that ask for sensitive information should use this protocol, and if you are ever directed to enter sensitive information into a site that does not use "https," then you should not do it.

Strategies for Personal Security

- Create and use secure passwords (eight characters or more that combine upper- and lower-case letters, numbers, and symbols);
- Check domains of links provided in emails and never login to a page that you access from an email message;
- Remove unnecessary identifying information from your online profiles (e.g., your address and phone number from your Facebook account) and other documents (e.g., resumes), and make your profiles as private as possible;
- Never enter sensitive information (e.g., credit card, bank account, social security number, password) into an insecure site (i.e. "http");
- Use a reputable anti-virus software, and don't install programs unless you know what they are and what they do.

Learning Check

Which of the following are true for safeguarding yourself online?

a. only enter personal information into secure (https) sites that you trust
b. use the same complex password on every site
c. open email attachments of files like .exe or .zip to see if you get a warning
d. logout of sites after using a public computer

Student Safety

All of the threats and strategies described above also apply at the classroom level, and the teacher should take steps to ensure that student uses of devices and internet technologies in the classroom are free from malware, hacking, and phishing. Teachers should recognize that as the closest point of contact for their students, they need to take an active role in ensuring their students' safety and security, but they are not alone in this endeavor. School and district technology professionals typically exist to help support the classroom teacher and can be great resources to help the teacher safeguard students. Most districts and schools have an acceptable use policy for their devices and networks. Teachers and students using these resources should understand and abide by these policies because they are designed to help ensure that everyone stays safe and also that the school complies with special legal requirements regarding student safety. Some of these requirements stem from mandates at the federal level, while others stem from mandates at the state level. Though these requirements may vary somewhat from district-to-district and state-to-state, there are some common areas where teachers are expected to take an active role in safeguarding students, in addition to those described above. We will now proceed by highlighting four examples of these areas, including: privacy, inappropriate content,

cyberbullying, and the creation and sharing of child pornography or sexting.

Privacy

At the federal level, the Family Educational Rights and Privacy Act (FERPA), requires teachers and other school personnel to keep student educational and private information secure. This means that grades and student work should not be distributed online or made available to others without the consent of the students and their parents. At the school district level, this means that student information systems and grade books should be secured in such a way that they cannot be accessed by anyone other than the student, their parent or guardian, and necessary school personnel. At the classroom level, however, these principles still apply, and there is a clear potential for violations if teachers share student work in public places or require students to create accounts on services that may not meet school security requirements, such as public email, blogging, or social media accounts. For instance, an English teacher who has traditionally required students to keep a daily paper-bound journal may now have students create an account on a popular blogging platform and keep a journal there instead. Even if the teacher does not make grades visible in this platform, the journal entries are examples of student work, and if the information in that journal is accessed publicly or by anyone without permission, the teacher would be violating FERPA. It is the teacher's job to ensure that students have a safe learning experience and that their school work is kept private. Questions about privacy and security should be explored with school and district personnel who have expertise in determining compliance with regulations, but at its heart, FERPA means that teachers need to be respectful of their students' right to privacy and avoid using Internet technologies in any way that may undermine this right.

Inappropriate Content

7/365 – Blue Eyes, Axel Naud, CC-BY SA

Even in well-filtered districts, students can still gain access to inappropriate content.

Schools are required by law to filter their students' access to Internet resources. The purpose of this is to ensure that students are not using provided resources to access materials that can cause them or others harm. School district acceptable use policies are often very explicit in what they consider to be inappropriate content, and they often reflect language from state level agencies and standards related to safe classroom environments and moral appropriateness. Blocked resources typically include but are not limited to content that is pornographic, violent, abusive, illegal, or otherwise inappropriate, sexually explicit, or harmful.

However, laws tend to be very fuzzy and subject to interpretation with regard to actual implementation. Thus, while one school district might completely block YouTube, another might enable access to specific channels within YouTube, and another might make the entire site available. In each case, school districts implement filtering policies that they believe strike a suitable balance between legal/ethical considerations and pedagogically valuable access to information.

Given this variability, district or school level filtering policies may not always be appropriate for specific classroom settings. That is, a

district may implement a single policy for all students and teachers in the entire district, but this level of access may not be equally appropriate for teachers, graduating seniors, and first graders. For this reason, teachers should consider what resources students are accessing in their own classrooms and layer on top of district or school filtering mechanisms their own structures for ensuring that students are making wise and safe use of those resources.

Online Safety for Kids, Intel Free Pass, CC-BY SA

Ensuring safe use of internet resources can be achieved in three general ways. First, teachers can implement their own filtering systems in their classrooms or structure classroom access of these resources in such a way that accessing other resources would be difficult. One way of doing this is to set the homepage for all classroom devices to a classroom home page that only has direct links to the resources that the teacher approves. Sites like Symbaloo or Only2Clicks make setting up this type of landing page simple and can reduce confusion or frustration by students who may need a simple method for accessing necessary resources in the classroom.

Sometimes this approach might not be appropriate, because you may want students to seek out information on their own or to find information from multiple sites. In this case, you can consider creating a custom search engine through a tool like Google Custom Search, which allows you to have fine-grained control over the types of resources that will be returned to your students through their searches. For instance, as students conduct a research project on Ancient Greece, you might provide a custom search engine that only returns results from Discovery, History Channel, and Encyclopedia Britannica. This allows you to still teach essential research and media literacy skills while also exercising greater control over the types of resources that students will need to parse through.

These strategies will not prevent students from typing in unlisted web addresses directly to the address bar, nor will they prevent students from using a general search engine to find new results. Similarly, even in the most restricted school districts, students can still find ways to bypass security settings by using proxy servers or other hacking mechanisms. For these reasons, even in the most structured classroom and well-filtered district, monitoring of student activities is essential to ensure that they are on task and not accessing resources that are inappropriate. This is especially important in 1-to-1 classrooms, which are becoming increasingly prevalent, wherein every student has a device at their disposal.

In addition, to help ensure that students know and understand classroom technology rules, you should make these rules clear and visible to students either by printing them on a poster or making a desktop background for devices that highlight them.

You can put your rules on your students' desktop backgrounds (click on the image and make a copy to create your own using Google Drawings)

When all is said and done, however, the teacher's greatest asset in monitoring their students is their own presence. If a student is afraid that you will look over their shoulder, he will be much less likely to seek after things that are inappropriate. For this reason, you should structure the physical layout of your classroom in such a way that allows you to see what is on your students' displays at all times and also allows you to have a physical presence near your students so that they know they are being monitored.

Some software products exist to help support this, such as classroom management or classroom monitoring software. They operate by collecting images from every student's display and combining them on the teacher's device so that the teacher can see all activities in the room at once. The major limitation of such software, however, is that it loses its power once the teacher is no longer monitoring the screen and essentially binds the teacher to a device and/or physical location, thereby removing necessary flexibility to move about the classroom.

Finally, if students know that they are being monitored, then it should

also be made clear to them what they are expected to access and what they are not. When a student accesses something that is inappropriate, it is important for the teacher to react in a manner that is suitable for the transgression. Sometimes advertisements may have inappropriate content and may pop up on a screen through no misbehavior on the student's part, and a student who intentionally accesses a pornographic website should be responded to differently than a student who accidentally opens a page with a few swear words on it. In every case, the teacher should set a standard for behavior and reporting processes by requiring students to report to her right away if they come across inappropriate content and assuring them that if they do this they will not get into trouble. This type of understanding allows the students to take an active role in helping moderate the classroom themselves but also sets the expectation that even accidental access of these types of resources needs to be avoided, reported, and addressed.

Cyberbullying

Bullying online can feel even more real and pervasive than bullying offline.

Bullying has always been a problem in schools. In fact, most people who have gone through a school system have probably experienced

bullying of some form, whether physical, verbal, or psychological. Some may treat bullying as commonplace and expected, but the effects of bullying are far-reaching and may influence students' emotional states, their ability to interact appropriately with their peers, their ability to be successful in their school work, and even their desire to lead a fulfilling life. Many high-profile cases have existed wherein bullying has escalated to extreme consequences, resulting in assault, murder, or suicide, which should lead us to recognize that bullying is a rampant form of abuse that should be counteracted at all levels.

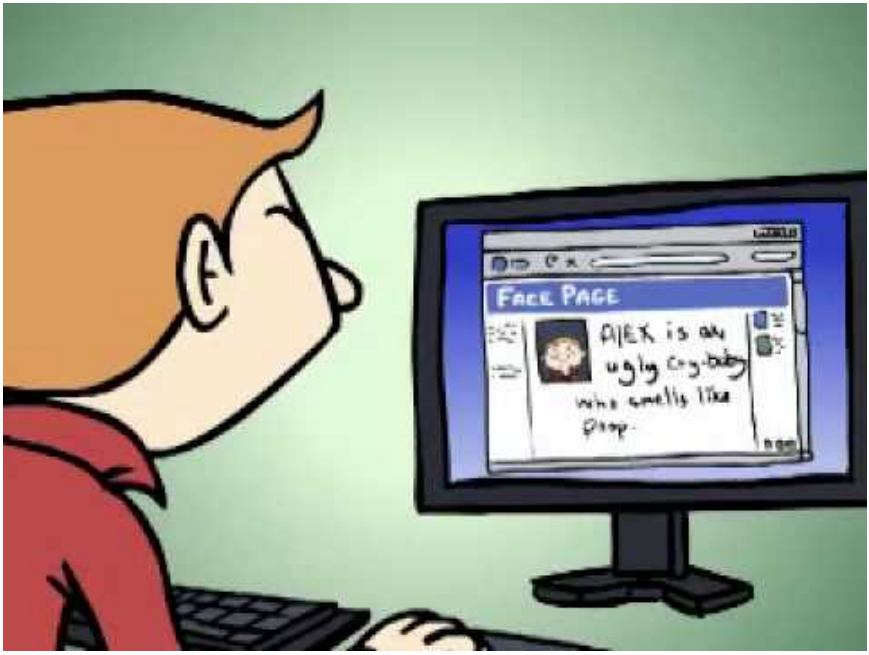
Cyberbullying is a form of bullying that uses internet and other technologies as a means for perpetrating bullying behaviors. It has gained attention in recent years not because bullying is a new phenomenon but because these technologies have enabled bullies to enact abuse via new media with greater persistence and prevalence. Before the internet, a student being bullied might be able to find solace from tormentors in an after-school program or by going home, but these technologies allow bullies to insert themselves into the persistent experiences of students through online posts, text messages, and other venues. A student who uses Facebook when she goes home, for instance, might find herself stalked and verbally abused by the same bullies that were abusing her at school earlier in the day. Cyberbullying removes the opportunity for reprieve for the victims and allows bullies to cause emotional harm in a manner that is social, persistent, and invasive into the their personal lives.

Many teachers may approach the issue of cyberbullying with skepticism, either because they do not believe that it is a problem or because they do not believe that the teacher should play a role in combating it. However, recent high-profile cases have shown that in situations of extreme abuse, lawsuits have been filed against schools and teachers for their unwillingness to respond to bullying behaviours online and their inability to punish students who use social media as a venue for abuse. Whether or not it is the teacher's role to be

investigators and enforcers in this area, it is the teacher's role to be an advocate for their students and to understand the relationship between classroom social interactions and the well-being of their students at large.

For this reason, it is now commonly encouraged for teachers to take a proactive role in speaking out against cyberbullying and addressing specific instances of abuse when they arise. For comparison, if a teacher were made aware that one student followed another student home every day after school and left threatening notes on the victim's doorstep, it would be expected that the teacher would speak up and contact appropriate school and law enforcement officials about the situation. The realization that teachers need to have is that online interactions are just as real as face-to-face interactions, and instances of abuse need to be addressed despite the medium through which they occur. In short, victimized students need teachers to be their advocates, and bullies need to be taught about the real-life consequences of their actions, even if those actions do occur online.

Addressing Cyberbullying with Young Children



Watch on YouTube https://edtechbooks.org/-cLL

Child Pornography and Sexting

Texting by Jhaymesisviphotography, CC BY

A specific subset of inappropriate content that teachers and students need to understand is child pornography. **Child pornography** is any pornographic or illicit depiction of a child, and viewing, sharing, or owning child pornography is a felony in the United States. In the U.S., a child is defined, for these purposes, as anyone under the age of

eighteen (18), and the internet and mobile phones have made child pornography a difficult problem for everyone to deal with.

First, though pornography is not itself illegal, pornography that depicts children is illegal in the U.S. Other countries have different laws, and much of the pornography that is produced, viewed, and shared on the Internet comes from other countries, which may not have laws against child pornography or may have a lower age of consent. This means that pornography that may be legal in another country and available online may be illegal in the U.S., and if students or teachers access or share such media, then they are guilty of a felony. For students under eighteen, this means that seeking out sexually explicit images or videos of others their age would be a felony, even though they may no longer think of themselves as children.

Second, and likely more alarming, mobile technologies, cameras, and texting have made it possible, and in some cases socially expected, for students to interact with one another in ways that are pornographic in nature, thereby leading them to not only view child pornography but also to create and share it. It is not uncommon for teens, for instance, to share sexually explicit photos with one another, and many teens do not see this as a problem, sometimes normalizing it within their peer groups. In such cases, photos are sometimes forwarded to peers, parents, and even teachers, meaning that those creating the images are guilty of a felony, but so are all of the others who received the images, viewed them, shared them, or saved them. Even if an adult gained access to such an image for the sole purpose of reporting it to the police, doing so could constitute a felony.

This state of affairs means that students and teachers need to be very careful and aware of the laws surrounding child pornography, and teachers need to counteract social influences that encourage young people to communicate and make themselves vulnerable in these ways. Students need to be taught the legal ramifications of these

kinds of activities but should also be taught their social ramifications and the potential social shaming that can result. Most of the students who get into trouble for these kinds of activities initiated them due to social pressure and a lack of awareness that these behaviors could lead to negative social outcomes or legal ramifications. As such, teachers should take seriously their role in helping students to develop the self-respect necessary to combat social influences related to sexting and child pornography and should treat this issue with just as much importance as any other dangerous, unhealthy, or illegal activity.

Strategies for Student Safety

- Keep student information, grades, and school work private;
- Proactively respond to cyberbullying, and be an advocate for your students who are victimized;
- Control and monitor what your students access in your classroom;
- Teach your students self-respect and the dangers of child pornography;
- Swiftly involve law enforcement in matters of student safety (e.g., cyberbullying, child pornography), and never look at, receive, ask for, or save child pornography (even for reporting purposes).

Learning Check

What should you do if you discover child pornography on your students' devices?

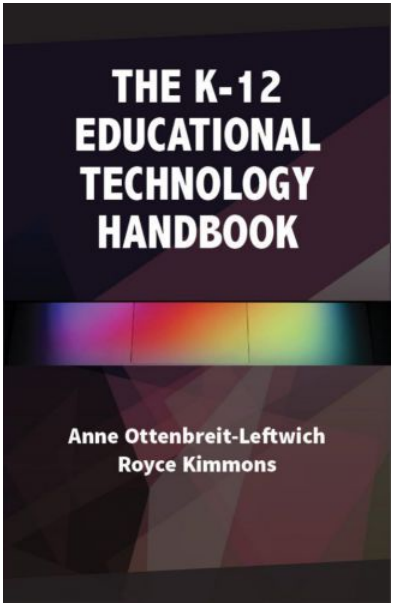
a. Save the web page, video, or image for reporting.
b. Attempt to identify students who were involved.
c. Report the incident to your principal.
d. Report the incident to law enforcement.

Which of the following statements about cyberbullying are true?

a. Cyberbullying is just a more modern way of referring to traditional bullying (e.g., on the playground).
b. Cyberbullying is rarely an issue in younger grades (K-8).
c. Cyberbullying is only the concern of teachers if it happens at school or on school-owned devices.
d. Cyberbullying is often more persistent and invasive than traditional bullying.

Conclusion

This chapter has explored issues of online safety by focusing on threats to the personal security of teachers (e.g., malware, hacking, phishing) as well as threats to student safety in the classroom (e.g., privacy, inappropriate content) and beyond (e.g., child pornography, cyberbullying). Given the severity of many of these threats, it behooves all teachers to understand these threats and to develop strategies for addressing them, both in their personal lives and in the lives of their students.



Kimmons, R. (2020). Online Safety. In A. Ottenbreit-Leftwich & R. Kimmons (Eds.), *The K-12 Educational Technology Handbook*. EdTech Books. Retrieved from https://edtechbooks.org/k12handbook/online_safety