

NC TOOLKIT for
Digital Readiness



Session 7 Instructor Guide

Online Safety & Privacy - Combined Group

OVERVIEW

Session 7 - Internet Safety

Session Time

(1 hour 55 min including 10 minute break)

Description

When it comes to the internet, safety is a top concern and it's not always easy to understand. In this session, we will talk about how to protect your information, your accounts, and yourselves while using the internet as well as how we can help make the internet a safe place for everyone. This will include discussions about passwords, account settings, and how everyone can use the internet in age-appropriate ways.

Objectives

Learners will be able to:

- Identify the risks on online activities
- Evaluate the safety of visiting a URL
- Find and choose common privacy settings
- Create strong passwords
- Consider the digital footprint collected by digital tracking

Adults will be able to:

- Discuss device usage and boundaries with students

Students will be able to (ISTE Standards 3a, 3b, 3d):

- Initiate conversations with adults about online situations
- Use online report and block tools



Preparation

- Print:
 - Adult handouts (one per adult)
 - Family Media Agreements (one per family)
 - *Optional:* Printable activities *When In Doubt & Should I Report It* (also in slides)
- Customize slides with Wi-Fi password and any relevant announcements

Just Before Session

- Open slideshow on presentation computer.
- Place sign-in sheet near entrance.
- Talk with assisting facilitators about how you would like them to roam among participants and field individual questions. Answer any questions they have about the session.



OUTLINE

Session 7 - Internet Safety

Arrival | 10 Minutes

All participants sign in. Use this time to make sure each family brought their device, they can sign into their device, it is charged or connected to an outlet, and connected to Wi-Fi.

Introduction & Agenda | 5 minutes

Introduce facilitators present. Set expectations for communication during session. Outline session schedule and goals.

Participant Introductions & Icebreaker | 8 minutes

Have each participant introduce themselves and answer the discussion question as they do.

- Discussion Question:
 - » What do you do, or avoid doing, to protect yourself online?

First Steps Towards Protecting Accounts & Devices | 30 minutes

(Slideshow Overview and Group Activities)

- **What is at Risk?**
 - Discuss evaluating the risk of various online activities and the kinds of things that could be at risk.
- **Be Careful Where You Go**
 - Activity: Check if a website is secure by clicking on the icon on the address bar.
 - Key Terms: *secure website, malware, look-alike links*
 - Activity: Visit transparencyreport.google.com/safe-browsing/search



■ Be Careful What You Share

- Activity: Decide which context (websites) are acceptable for which information.
- Discuss how to find and understand common security settings.
- Discussion Questions:
 - » Which settings do you think are important for your privacy and security? How often do you check your privacy settings?
- Key Terms: *privacy vs. security, account settings, location services, etc.*

■ Make it Harder for the Bad Guys

- Discuss software updates, avoiding emotional reactions, and passwords.
- Discussion Questions:
 - » What do you think makes a good password? How many different passwords do you use?
- Activity: Test out howsecureismypassword.net
- Discussion Questions:
 - » How long would it take a hacker's computer to crack your password? What if you add one more word or one more symbol?

Break | 10 minutes

Digital Tracking & Cookies | 18 minutes

- Video: [Understand Digital Tracking](#) from GCF Learn Free
- Activity: Brainstorm digital data created by *Daisy's Digital Day*.
- Discussion Questions:
 - » Is there anything Daisy does that you might avoid because it's not worth the creating the digital data? Do you have any suggestions for Daisy about how to protect her privacy?
- Demo: How to view cookies collected by a website.



Protecting Students Online | 12 minutes

(Slideshow Overview & Group Discussion)

Go over options for helping keep students safe online, from controlling and limiting their activity with software to setting boundaries together and understanding their online activity better.

- Key Terms: *browser history, filters*
- Discussion Questions - Students:
 - » What do you think about your adults possibly filtering or limiting the content you can see online or the apps you can use?
 - » Do you know students who try to get around limits to their device and internet usage? Why do you think they do that? Do you think that is a good idea?
 - » Do you think you could benefit from agreeing to certain limits on your device?
- Activity: Look at information about a website or app your student uses on www.common sense media.com and discuss with them.

Google's Be Internet Brave | 12 minutes

(Group Activities and Discussion)

When to Get Help and Report It Online, Too adapted from [Google's Be Internet Awesome Curriculum](#) under [CC BY 4.0](#)

- Discussion Questions:
 - » If you were in the cafeteria at school or at a basketball game or at the store and you saw something that might be a problem, what might be smart things to do?
- Handout: optional printable versions of activities in slides
- Activities: Read situations and decide how you might respond with your partner.

Family Media Agreements | 5 minutes

Families discuss internet safety and Common Sense Media's Family Media Agreement.

- Handout: Common Sense Media Agreement

Wrap-Up | 5 minutes

(Further resources and exit survey)



SCRIPT

Session 7 - Internet Safety

Italicized words are instructions and notes to you, not to be read aloud.

Highlighted text indicates that participants should complete those instructions.

Arrival | 10 minutes

- *Allow some time for participants to arrive and get settled so everyone can start together.*
- *Each participant who arrives needs to sign in (both the adult and the student).*
- *Use this time to make sure each family has a device that is charged, connected to Wi-Fi, and signed in.*

Introduction and Agenda | 5 minutes

- *Introduce facilitators present.*
- Today, we are discussing online safety, security, and privacy.
- These can be big, complicated topics but by the end of this session, you'll understand some basics and you'll be more prepared to make decisions about how you want to use the internet.
- We'll start with some simple strategies to be safer online, then learn a little about how our data is collected and tracked online. We'll finish up by looking at some issues facing young users of the internet.

Introductions and Icebreaker | 8 minutes

- Before we get started, let's all introduce ourselves in case we haven't all been together before. So please say your name and answer this question:



Discussion Question: What do you do, or avoid doing, to protect yourself online?

- *Answer the question and give your name as an example.*
- *(ex. always log out of my accounts when I'm finished using a shared computer)*
- There are so many ways you can protect yourself online, and some work better



than others.

- Today we're going to talk about a few smart choices and a few good habits you can use to be safer online and protect your privacy.

First Steps Toward Protecting Accounts & Devices | 30 minutes

(Slideshow Overview & Group Activities)

What is at risk?

- Let's take a second to think about what is at risk when we use the internet.
- Just about everything you do comes with risks. Reading a book puts you at risk for paper cuts. Eating puts you at risk for tasting something bad.
- Understanding risks helps you decide what's worth taking the risk and what activities to avoid because the risks are too high.
- I know sharks live in the ocean, but I know the risk of being bitten while swimming at the beach are low, so I don't mind to swim there. However, if someone invited me to swim in a tank of hungry sharks, I would probably say "no" because the risks would be higher.
- We have broken down the risks of internet use into four categories of things that might be endangered by your online activity:
 - Computer could be compromised (**devices**),
 - Personal information could be shared inappropriately (**privacy**),
 - Financial information could be stolen (**money**),
 - Physical and psychological well-being could decline (**health**).
- Thinking about the risks of using the internet can be discouraging, but there are some simple things you can do to make internet use less risky so that you can continue using the internet for all its benefits.

Be Careful Where You Go

- First, just like in real life, it's important to be careful where you go online.
- Knowing a little about the website you are visiting will help you decide what is safe to do and what you should avoid.
- For example, some websites are safe to visit but not safe to share your information on.



- If there isn't a **lock icon** on the URL bar, then you don't want to input any passwords, credit card numbers, or personal information.
- Sometimes you can learn about the security of the website by clicking on the icon that's here, whether that's a lock or not.
- 🔍 Try that now. Open a browser, visit a website and click on the icon to the left of the URL.
- The lock icon and "secure" rating means you can share passwords, etc. If it doesn't have a lock icon, it might be safe to visit this website but not share sensitive information.
- Other websites aren't safe to visit at all. Websites with bad intentions can install malicious software on your computer.

Be Careful Where You Go: Malware

- If you came to the Communicating Online workshop, you might remember the word we used: malware.
- **Malware** is a catch-all term for software designed to attack your computer, like computer viruses.
- It may harm your computer, collect information from your computer, or send information from your computer to someone else.
- Opening an email, link, or file could install malware so always be careful where you click.

Be Careful Where You Go: Look-alike URLs and links

- If you are familiar with the website you plan to visit, be sure you aren't accidentally clicking on a look-alike URL. We talked about these in our communication workshop too.
- **Look-alike URLs** are links to fake websites that look similar to real URLs. They are a tactic used to trick you into thinking you're visiting a website you know and trust when you are not.
- Sometimes links will look like this – asking you to click on a button or word that doesn't show the URL.
- You can hover over a link or button to see the destination URL. Check those for look-alikes as well.



- One way to avoid bad links for websites you are familiar with is by typing the URL you know directly into the address bar or using a search engine, rather than using the link. Better safe than sorry!
- If you haven't tried the phishing quiz, it's a great way to practice hovering over links and spotting look-alike URLs. The URL for the quiz is on your handout.

Be Careful Where You Go: Unfamiliar URLs

- If you're not familiar with a site and want to find out if it's safe or not before you visit it, you can get more information by using Google's Transparency Report.
- 🔍 Visit transparencyreport.google.com/safe-browsing/search and type in the URL for a website you use.
- This is a tool that scans websites for malware. Searching unknown URLs here could warn you before you accidentally visit a website with malware.

Be Careful What You Share

- Now let's imagine you've learned all these methods, you're very careful, and you're only visiting safe websites. Oversharing can get you in trouble even on sites you trust.
- Everyone has a different idea of what should be private online, and that's okay. The most important thing is to think about the context in which you're sharing that information.
- If you're on your hospital's secure patient website, it is safe to share personal medical information. You may not want to share that same information in a Facebook post.

Be Careful What You Share: To Share or Not to Share Activity

- Let's practice thinking about whether we'd want to share information in different online contexts.
- *Ask people to volunteer to share their opinion, perhaps by polling, and then ask for comments about why they made their choice. Remember, these are personal choices without right and wrong answers, just more and less risky choices. Some comments are below to help the conversation if need be. Feel free to add your own.*
- Would you share your **social security number** on ...
 - Secure bank website – *should be safe but make sure it's the right website*
 - Public social media post – *very risky*



- Friends/followers-only social media post – *risky because they might choose to share it further or share it accidentally*
- Private message or email – *risky because they might choose to share it further or share it accidentally*
- Would you share your **favorite movie** on ...
 - *Not very risky anywhere because there are very few consequences to people knowing your favorite movie.*
- Would you share your **current location** on ...
 - Secure bank website – *should be safe but not necessary, so it's better not to share unless there is a reason.*
 - Public social media post – *do you want strangers to know where you are?*
 - Friends/followers only social media post – *do you care if EVERYONE with access to that post knows where you are and where you aren't? What's an example of a location that would be okay to share (I'm at school) and one that's less okay to share (here's my home address)?*
 - Private message or email – *consider who you're sharing with, who they might share with, and the consequences if they accidentally share with others.*
- Would you share your **phone number** on ...
 - Secure bank website – *should be safe, but make sure it's the right website.*
 - Public social media post – *if your phone number is associated with any of your online accounts, it could be used to reset your password and gain access to your account.*
 - Friends/followers only social media post – *remember, they might share it, too.*
 - Private message or email – *safest option.*

Be Careful What You Share: Privacy Settings

- You also need to think about information you may be sharing unintentionally.
- When we talked a little about social media in the communications workshop, we covered the difference between public and private messages and profiles. You can control how private and public some of your information is in the settings of your social media accounts.
- On the screen are some account settings and app permission options for Facebook.



Discussion Questions:

- Which settings do you think are important for your privacy and security?



- What do you think about the advertising settings? Why might you decide to turn personalized ads on or off?
 - » Not all privacy settings are about security. Sometimes they are personal preference about how much information you're willing to share.
- Do you want Facebook to be able to access your location information?
 - » Location settings refer to the geolocation data from your mobile device's GPS. It doesn't affect if you choose to share information about your location, like if you type in a message that you are shopping at "Wally-world" without actually tagging Walmart's location.
 - » You might leave that on if you want to tag the location of your photos or get suggestions of nearby events. You might turn it off so you don't unintentionally share your current location with other Facebook users or allow Facebook to share that information with advertisers other websites.
- How often do you check your privacy settings?
 - » Every time you make an account or download an app, look at permissions and privacy right away. Then review them regularly.
 - » It's a good idea to give the minimum permissions necessary to use the account in the way you prefer.
 - » Websites and apps could change their privacy and permission policies and checking them will help you stay in control of your information.
 - » How often you check them and what you share depends on your preferences and what kind of information you might be associating with this account.
- If you're looking for settings in an account, look for the gear icon. Sometimes you'll have to click on the hamburger first (the three lines) to open a menu that includes settings.

Make it Harder for the Bad Guys

- The last strategy for staying safe online is to do a few little things to make it harder for whoever might be trying to get your accounts or information.

Make it Harder for the Bad Guys: Software Updates

- First, in addition to keeping your privacy settings up-to-date, keep your antivirus software, operating system, browser, and apps up-to-date.




- When companies learn about weaknesses in their security, they fix them with updates.
- So make sure you're updating software and apps when new versions become available.

Make it Harder for the Bad Guys: Act Slowly and Suspiciously


- Like we talked about in our communications workshop, if it seems too good to be true, it might be. If there is something bad that might happen quickly, someone might be trying to scare you into making a bad choice.
- Take a moment to think carefully about why someone might benefit from the action they are asking you to take and what the consequences would be if that action is a mistake.

Make it Harder for the Bad Guys: Have Good Passwords

- And finally, use good passwords.

 Discussion Question: What do you think makes a good password?

- A good password is easy to remember but difficult to guess.
- There are kinds of software that try to guess passwords by testing every word in the dictionary.
- People interested in stealing account information often try to find easy accounts and skip more difficult ones. Making your password a little more difficult by not using common words can make your account much more secure.
- Longer passwords are more secure, so using several words together can help.

 Discussion Question: How many different passwords do you use? (*Maybe try to figure out who has the most different passwords.*)

- Using the same password over and over again means all your accounts are only as secure as your most vulnerable account. It's best to use different passwords, at least on your most important accounts that store your most sensitive information.
- It's actually okay to write your passwords down, if you need help remembering them.
- If you want to be extra secure, you might check out a password manager, which will create very secure passwords and remember them for you. There's information on the handout about password managers, in case you are interested.



Make it Harder for the Bad Guys: Test your Passwords Activity



Go to howsecureismypassword.net, and type in a password similar to yours.

- For example, if your password is a 5 letter name, try a 5 letter name.
- You might not want to type in your real password. Even though this is a secure website, it's always a good idea to avoid sharing any information when it isn't necessary or helpful.



Discussion Questions: How long would it take a hacker's computer to crack your password? What if you add one more word or one more symbol?

Break | 10 minutes

Digital Tracking & Cookies | 18 minutes

- Now that you've had a break, we're going to talk about the most complicated topic of today: cookies and digital tracking.
- 🔍 Discussion Questions: Have you ever searched for something on one website and then seen an advertisement for that same thing on a different website? Are there examples of when you think your device might be remembering the things you do?
- These might be examples of digital tracking, often through the use of cookies.
- You may have seen a message on a website asking you to allow cookies before continuing and it's easy to quickly click "accept" without thinking.
- That's not necessarily the wrong choice, but we're going to try to understand the implications of that choice a little better.
- We're going to watch a short video to start off our discussion about cookies.
- Watch [Understand Digital Tracking](#) from GCF Learn Free on YouTube.
- Cookies are another example of when we compare the risks of using them to the benefits we get from using them.

Daisy's Digital Day

- To get an idea of how companies can learn about you based on your device use, let's think about how much digital data you might create.



Open a new document on your computer. Raise your hand if you need help with this.



- Meet Daisy. She's a high school student. Imagine it's Saturday and she has a soccer game this morning. After that, she plans to visit a coffee shop, stop at a store, pick up some fast food, and then spend some time online at home.
- 🔍 In your document, type all the digital data you think she might create during this day.
- 🔍 Think about both the data she creates actively, like posting a picture, and passively, like visiting a business while the GPS on her phone is collecting her location.
- Give families two minutes to complete this activity.
- 🔍 Each group will share one thing from their list. If you have the same one, highlight that text in your document. When it's your turn, share something that hasn't been highlighted. *Depending on the skill-level of your group, you may demonstrate those instructions.*
- Groups continue rotating and sharing until all groups have read their entire list.
- 🔍 In another browser tab, open <http://bit.ly/digdaisy> and spend a couple minutes reading about some of the data we missed.
- ❓ Discussion Questions: Is there anything Daisy does that you might avoid because it's not worth the creating the digital data? Do you have any suggestions for Daisy about how to protect her privacy?

How is Data Used?

- Most data that is collected from users is used in two ways:
 - To create a better experience for the user. (Like remembering your language preferences or what things you added to your shopping cart).
 - Sold to advertisers.
- 🔍 Visit one of these websites (displayed on the slide). Choose one you might use.
- 🔍 Click on the lock on the address bar like we did before.
- 🔍 Then choose "cookies" from the drop-down.
- 🔍 Read the websites that are collecting information using cookies on this site.
 - Some of them are the website itself, used to give you a better experience.
 - Others are probably advertisers, who collect your information for the companies that advertise with them.
- ❓ Discussion Question: Are you surprised at the number of cookies on this site?



- Working to control how much you are tracked online is difficult, and sometimes it isn't necessary. But being aware that your activity might affect your interactions with websites can help you understand your role in the online world and protect your privacy in ways that matter to you.
- If you'd like to know more about cookies, online tracking, and how to gain some control, there are resources on today's handout.

Protecting Students Online | 12 minutes

(Slideshow Overview & Group Discussion)

- A common question from parents is "How can I control what my student does online?"
- There are a few different approaches people tend to take.

Control and Track Their Usage

- The most hands-on, technical option is to try to control and track their usage using various software.
- The biggest barrier is that any tool to do this is imperfect and can be undone or avoided by a clever student, if they choose to do so.
- You can look at the browsing history on your devices to see what websites have been visited, but there are ways to delete these histories.
- There are filters that block certain websites or apps. These can be avoided, but that doesn't mean they're useless. Some people use them to block distractions like social media and games for themselves when they are trying to be productive. Others block certain kinds of content they would prefer not to see, spoilers for TV shows they haven't seen yet, or a celebrity they find annoying. **These methods work best if the person who will be blocked from visiting websites agrees to the rules applied.**
- Similarly, some apps and devices will allow parent accounts some control over student accounts, like Apple, Google, and YouTube. These can set parameters controlled by the parent's account.


Discussion Questions - Students:

- What do you think about your adults possibly filtering or limiting the content you can see online or the apps you can use?
- Do you know students who try to get around limits to their device and internet usage? Why do you think they do that? Do you think that is a good idea?



- Do you think you could benefit from agreeing to certain limits on your device?

Understand Their Usage

- There are so many different apps and websites that students like to use, and there are new ones all the time.
 - Understanding these apps and websites can help both understand how to use them safely.
 - **Common Sense Media** is a website we have mentioned before because it has many tools for parents.
 - They have reviews of apps and websites and can help you understand the positives and possible risks associated.
-  Go to commonsensemedia.org and search for one app or website your student uses. Spend two minutes reading some of the information and discussing it together.

Discuss Their Usage


- The best way to understand and be involved with your student's online activity is to talk to them about it often.
- In a few minutes, we're going to look at a family agreement you might like to use to help your family discuss what you're doing on your devices and what risks are worth taking.

Google's Be Internet Brave: When in Doubt, Talk it Out | 12 minutes

Adapted from [Google's Be Internet Awesome Curriculum](#) under [CC BY 4.0](#)

(Group Activities and Discussion)

When to Get Help

- We've talked about a lot of things you shouldn't do online, so now let's talk about some of the things you should do.
-  **Discussion Question:** Let's think about offline safety for a second. Students, if you were in the cafeteria at school or at a basketball game or at the store and you saw something that might be a problem, what might be smart things to do?
- Talk to someone you trust.
 - Report it to the person in charge.



- These are the same things you should do if something online doesn't seem quite right, might be a problem, or makes you uncomfortable
- *Hand out optional printable version of "When in Doubt, Talk it Out".*
- 🕒 Think about the list of situations on the screen. Discuss with your adult whether any of these have happened to you and whether you wanted to talk to someone you trust to get their help when it did.
- *Allow a few minutes for families to discuss together.*
- Usually when we use the internet, we do it by ourselves, so it's always a good idea to talk things over with someone we trust rather than dealing with iffy situations alone.
- If anything online makes you uncomfortable, you should always talk to an adult you trust and they can help you understand it.

Report It Online, Too

- When something doesn't seem right online, the other way you might react is to report it to the person in charge.
- Have you ever seen a "report" button on a website?
- If you use this option, it usually sends a message to the website's manager that there might be a problem. They will review the flagged material and decide if anything needs to be done.
- For example, if you see mean and scary comments on a YouTube video, you can report it. YouTube will check that user's activity and possibly remove their account. This is important because it could prevent that user from leaving upsetting comments in the future.
- Talking to someone you trust can help you have a better experience online. Reporting something online can make the internet safer for everyone.
- 🕒 Let's look at a few scenarios. Talk to your adult about why you would and wouldn't use online tools to report anything and whether you'd also talk to an adult about it.
- *Complete "Should I report it?" activity in the slides and on the optional printable handout*
- It's always, always a good idea to talk about your online activity with an adult you trust. Sometimes it's important to do an online report, too, to make sure the internet is a safe place for everyone.



Family Media Agreements | 5 minutes

- *Hand out Common Sense Media Agreement*
- For our last activity, we are going to look at the Family Media Agreements mentioned before.
- This Family Media Agreement covers many issues related to devices and helps you decide exactly how you want to use it.
- Take a few minutes to discuss which parts of this your family might like to use. We are here to answer any questions you might have and you might want to use Common Sense Media to do a little research as well.
- There may be people that aren't here tonight that should be involved in making an agreement like this, so you may choose not to complete it now. But go ahead and discuss it.
- *Give families a few minutes to discuss the agreements. Make yourselves available but not intrusive.*

Wrap-Up | 5 minutes

(Further resources and Exit Survey)

- Again, feel free to complete these Family Agreements at home and use them however is best for your family.
- Resources from tonight's workshop are on your handout. This is a big topic and there's always more to learn, but you are off to a good start with today's discussions.
- Please take tonight's exit surveys and let us know if you have any questions.

