Online Safety for Kids Ages 8-13
Parent and Guardian Presentation

Instructions:

1. Use the script below as a guide to discuss Online Safety with your child.
2. *Optional: Offer your child the quiz to test their online safety knowledge.*
3. Celebrate your child's accomplishment by awarding them the certificate of completion and encourage them to use their cyber safety superpowers to protect the whole family.
4. Once complete, provide your thoughts and feedback. Your input will help us continually improve this program.

Script

Slide 1: Today we are going to learn about staying safe when you're online. You usually use the internet whenever you're on a device and using the internet means big responsibility.

Slide 2: I know that you have been on 'the Internet,' but can you tell me what it actually is?

The Internet connects BILLIONS of computers all over the world. Each computer has its own address, just like your house has an address. IN REAL LIFE, every house and business also has a door. Some doors are safe to enter, and others aren't, right? (like a stranger's door).

If your computer is connected to the Internet, you can visit computers all over the world—which can be AMAZING, as long as you're taking the right steps to keep yourself safe.

Slide 3: What kinds of electronic devices do you use to connect to the Internet?

Even though these kids are sitting at home on their devices, they're traveling on the Internet, connecting to websites and people.

So, let me ask you a few questions:

1. What types of websites do you visit? *(like: email, games, Google, chat)*

2. Have any of you ever accidentally entered a “bad website” on the Internet? What happened? *(like: weird pop ups, content is glitchy)* So if you see a bad website what are you responsible for doing?

Slide 4: What does responsibility mean and what does it mean to act responsibly online?

It means:

- Keeping yourself safe
- Keeping your stuff safe
- Being responsible for what you say and do online

All of these behaviors are important if you want to be considered a ‘responsible cyber citizen.’

Slide 5: Do any of you remember being taught to stop, look and listen before crossing the street?

There’s also safety rules for the Internet, and they are simple to remember, do them after me:

[USE YOUR HAND SIGNALS]

STOP *[Put your hand up and wait for kids to copy]*

THINK *[Point to your head and wait for kids to copy]*

CONNECT *[Put two thumbs up and wait for kids to copy]*

Let’s do that again!

Slide 6: *Control+Click to start the video. Runs just under 2 minutes.*
(Here’s the video link if it doesn’t work through PDF:
https://www.youtube.com/watch?v=HIEmDJHnt6o*)*

Slide 7: Personal information is SO IMPORTANT that we should keep it as protected as if it were locked in a safe. Can you tell me some personal information that you should keep private?

Answer: password, parents’ credit card number

Right, now let’s go over some other important information to keep safe:

- Your age
- Where you go to school

- Where your parents work
- Where you live
- Your phone number
- Passwords **Only you and your parents should know this!!!

Slide 8: Remember, before sharing ANY information online, STOP and THINK:

WHO is asking for my personal information?

WHAT information is being requested?

WHY do they need this information?

Even if there appears to be a good reason to give your information, you should ALWAYS ask your parent or guardian FIRST.

In most cases, you can't really know who you're talking to online. You can't see them. You don't know them, which is why you should always ask a trusted adult before you give out any private information.

The online bad guys are trying really hard to get it. **Why?** Because with your personal information, they can find ways to steal from you and your family or harm you in other ways.

Slide 9: You've heard of computer viruses, right? What's the big deal? *[Take responses.]*

Once a virus is on your computer, it opens the door for the bad guys to steal important information about you or your family.

You should NEVER download a file or click on a link from someone you don't know. If you do, you can be downloading a virus that can harm your computer, delete important files, or make it so you can't even use it anymore and it could even steal information about your family leading to identity theft!

Can you tell me what phishing is?

We have all heard of going fishing for fish, but online there is a different kind of phishing that starts with a "ph" This type of phishing a cybercrime in which a target is contacted by email, telephone or text message by someone posing as a real business to trick you into providing personal information that we just finished covering a few slides before!

Slide 10: Another way online criminals can hack into your computer and steal your information is by getting you to click on a link that promises a reward.

Here's an example of a pop-up that promises you free money if you click on the link. Have you have received this kind of message for something free? Did you click on it? What happened?

Have you ever known anyone who got anything FREE just by clicking on some links? Of course not!

If it sounds like it's too good to be true – it probably is!

Never click on a link from a pop-up or email or text claiming that you are the winner of a prize. Bad guys are either trying to get you to go to a dangerous site where they can put a virus on your computer, or they are trying to get you to give up your personal information.

Slide 11: To safely close of a pop-up on a PC, press Alt and F4 at the same time.

To get rid of a pop-up on an Apple computer, press the Command Key and "W" at the same time.

Slide 12: Can you tell me what "Stranger Danger is?"

Friends are people that you know and trust in real life. People that you are chatting with online, are not always your real friends. Often, they are simply the people you are chatting with online. <u>You don't know them</u>.

Online bad guys can pretend to be someone you know or someone you will want to know, in order to trick you into giving them personal information.

For example, here's a kid chatting online with someone they think is another kid…

But really, they are chatting with this scary guy who is pretending to be their age.

What should you do if you are online and someone you don't know messages you claiming to be a student at a nearby school?

<u>Answer:</u> Do not accept their invitation to chat (it could be someone trying to trick you). Then tell an adult immediately that a stranger is trying to talk to you online.

Slide 13: I know that you have enough common sense to stay away from strangers in real life. You need to be extra careful when you're online because you can't see who you're talking to.

-- Don't chat online or exchange ANY information with strangers (not even your e-mail address)

-- Don't accept online "friends" that you don't know and trust in real life

-- Don't post personal information online (like where you go to school, where and when you play afterschool sports, other activities, etc.)

-- Don't leave your mobile devices where others can access them

-- Don't share passwords with ANYONE (games, email accounts, logins)

-- Don't meet with someone you met online.

Slide 14: Do you think this statement is true?

Once you hit "Send" or "Enter" and put something on the Internet, you can't take it back. I'll explain why...

<click to next slide for example>

Slide 15: This girl has just a "funny" message about a classmate and she sends it to 4 of her closest friends, with the subject, "Don't show anyone!

Slide 16: They think it's so funny that they send it to a few of their friends...

Slide 17: Who send it to a few of their friends...

Slide 18: Who posted it on Facebook...

Slide 19: and so on.

Eventually, the private message she sent to her 4 best friends went viral, reaching hundreds of people including teachers at her school and even the classmate who was hurt!

Earlier, we said that traveling the Internet was like going down a street where every house has an address and a door. By clicking "send," this girl and her friends have sent this picture through MANY doors, and on its way to each door, it has left digital footprints. The girl may be able to delete the message from her web profile or even her device, she will never know how many people have downloaded and saved the message not to mention her classmate whose feelings that were hurt.

Slide 20: Part of being a responsible cyber citizen means **always** treating others the way you want to be treated.

Have you heard of cyber bullying? What is it?"

The definition of cyber bullying is when someone frightens, embarrasses, harasses, or otherwise harms someone else online over and over.

Cyber bullies may use any form of online communication--instant messenger, email, texts, web posts, games to torment their victim(s).

- What would you do if you received a message from a cyber bully?
- What if someone forwarded you a mean message about someone else?

What do you do if you are being cyber bullied or know someone who is?

1. **STOP** correspondence with that person. Never forward or respond to a bully's message.
2. **BLOCK** that person from sending you any more emails, messages, texts, wall posts, etc.
3. **TELL** an adult, like a teacher or a parent

Slide 21: Now that you've learned some really important rules about being online, I want you to tell me what you do before you download or post, give away a password or give personal information... Stop. Think. Connect. And ALWAYS ask a trusted adult.

Slide 22: Do you have questions? What did you learn today?

Thank you so much for giving me your attention and learning how to be a safe cyber citizen! You earned a special certificate!