Children & Youth Sabbath School

TEACHER'S GUIDE

SAFETY SABBATH®

Adventist Risk Management, Inc.

safetysabbath.org

Table of Contents

How to Use This Guide

This year for Safety Sabbath, Adventist Risk Management, Inc. (ARM) encourages churches to improve online safety and network security. Part of that emphasis is ensuring members have the education and tools they need to protect themselves online. Often a security breach is the result of users who don't practice online safety.

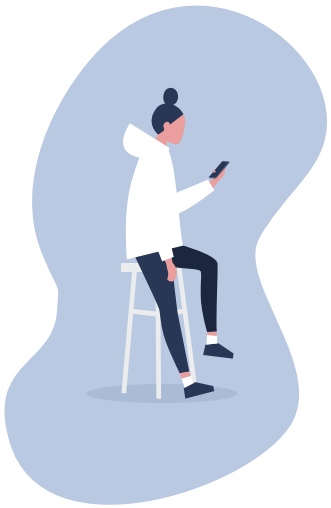
This Sabbath School teacher's guide is a collection of resources you can use to address online safety with the children and youth you know. The first section, Talking with Kids About Online Safety, is designed to help you understand how to approach this subject as a teacher. The rest of the document contains resources you can use with your Sabbath School classes from Primary through Youth.

As young people spend more time online, identifying and avoiding common risks is increasingly important. Having these conversations with children and youth is critical, but don't assume these conversations will happen at home or school. Even if they are, reinforce the importance of practicing online safety all the time.

The ***Common Internet Dangers*** section is written for children and youth. You may print out this section as a resource for them to take home. Younger children may enjoy the activity as a way of reinforcing the dangers you discuss. At the same time, older youth may get more out of the included discussion questions.

The Apostle Paul gave us useful guidance that can be applied to our usage of the internet. In Philippians 4:8, he said, "Finally, brothers and sisters, whatever is true, whatever is noble, whatever is right, whatever is pure, whatever is lovely, whatever is admirable—if anything is excellent or praiseworthy—think about such things."[1]

[1] Biblica, Inc. (2011). The *Holy Bible*. New International Version



Talking with Children and Youth about Online Safety

Parents, teachers, and youth leaders understand the need to talk with children and youth about the potential dangers online. Yet, these conversations don't happen as often as they should; when they do, they often miss the mark in affecting any measurable change. Learning how to talk with children and youth about the power of social media and the Internet can give adults the confidence and resources they need to have this important conversation.

Educate Yourself

The Internet changes with lightning speed, often leaving parents and adults in the dark when it comes to understanding the dangers of the Internet. Before any meaningful conversation can occur, adults must invest in educating themselves in digital landscape.

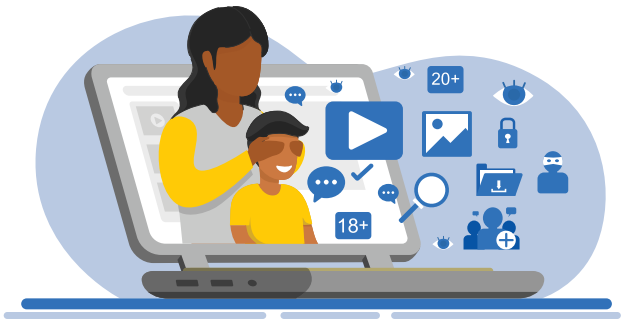
Knowledge of how young people are using the Internet gives adults the opportunity to direct the conversation to relevant topics. This gives the adults more credibility in the eyes of young people, which makes them more likely to take seriously the advice the adults are giving them.

Some of the areas parents and adults should stay current in, include:

- **Text Slang**—A whole new language of abbreviations and slang has developed in the digital space. Understanding what kids are actually saying is important as you monitor their online communication.
- **Social Media**—Familiarize yourself with social media platforms currently popular with young people. Create an account and spend time on the app to understand how it is used.
- **Online Games**—Online gaming has grown increasingly social in recent years. Many popular games are designed to be played by groups of people who connect online and even talk together while playing. Know what the latest game craze is, how it's played, and if there is a risk of meeting strangers.

Focus on Real Challenges

When talking with young people about the Internet, resist the urge to reduce the conversation to simply



saying, "the Internet is bad." Internet use is deeply embedded in today's society, especially in educational curriculum in the earliest years of elementary school. Children and youth also see how frequently adults use the Internet, which can give them the impression of a double standard.

Teaching children and youth about the real challenges of the Internet empowers them to safely navigate the Internet. This is a skill they will need for the rest of their life and the sooner they can develop it, the better off they will be.

While it's important to have age-appropriate conversations with young people, the dangers of the Internet do not discriminate on the basis of age. Anything that exists on the Internet is available to anyone.

Important topics about online safety you should be able to cover with children and youth include:

- What content is inappropriate and how to avoid it
- Verifying someone's identity
- Recognizing online scams
- Identifying credible information
- Privacy protection
- Strong password management
- "Oversharing" on social media
- The permanence of things said online
- Proper responses to cyberbullying

Foster Open Discussion

When it comes time to have a conversation about online safety with children and youth, it's important to frame the conversation as a discussion rather than a lecture. Foster an environment where they are comfortable about having open and honest dialogue with you.

The virtual world is no different than the real one and this age group is often self-conscious and insecure. They may even have their own concerns about the Internet and what they experience there. Having a discussion with young people gives them the opportunity to express those fears and find reassurance and guidance from parents and adults.

Teaching children and youth about the real challenges of the Internet empowers them to safely navigate the Internet.

Common Internet Dangers

Every year the internet becomes more integrated into all aspects of life. There's no doubt it can be a valuable resource, in addition to being an excellent source of entertainment. Still, the internet is not free from potential dangers that can put you at risk.

The news regularly reports stories about young people who meet someone online and go missing after they attempt to meet their new "friend." You might say, "I would never do that," and you may be right. But there are many other online dangers that have serious consequences.

Since the digital world is so interconnected, your online safety actually affects your friends, family, church, and school. Basically, anyone you interact with online can also be at risk because of your online activities.

Consider this scenario: your email gets hacked, which allows a hacker to send out malicious software (called malware). Since it looks like it came from you, your friends are more likely to open it and click on the link. If this happens at your school, now the school network and all its users are at risk. You can see how quickly these events can snowball out of control.

Hackers are continually creating new schemes to trick you. Here are some of the most common methods used. As you review the potential dangers, think about whether you have encountered any of them. How easy would it be for you to fall for some of these tricks if you were exposed to them?

Password Security

Your password is the only thing standing between you and a hacker. If someone can access your email, social media, or other online accounts, they can "become" you. This can give the hacker even greater ability to access more of your accounts or to pose as you when performing other hacks.

Avoid using words or numbers in your password that are meaningful to you. Yes, this makes it easier to remember. Still, hackers can also use information gathered from your social media profile to try and crack your password. Favorite sports teams, birthdates, and pet names should never be part of your passwords at all.

When you create a password, experts recommend using a combination of lowercase and uppercase letters, numbers, and special symbols. Longer passwords are better, and you should never use a password shorter than eight (8) characters.

If you have one password for all your online accounts, even a strong password, you're at risk! Passwords that become compromised are often sold between hackers or shared on the "dark web." If you use the same password for multiple accounts, a compromised password gives access to all your accounts.

Using a password management app is the best way to ensure you are using good password protocols. Many of these apps will autofill your information for each account, which means you can use long, unique, strong passwords for each one. Be sure to protect your password management app with a strong password you don't use anywhere else. You may want to consider using what's called a passphrase to secure your password management app. A multi-word phrase or sentence can be easy for you to remember but can be challenging to hack.

The bottom line is this: everything you do online hinges on how secure your passwords are. Use unique passwords for every site and never share your password with anyone.

Catfishing

You may have grown up hearing the phrase "stranger danger." This has been drilled into us since we were little, and as a result, we are often cautious about people we don't know. With our friends or people we know, it's easy to let your guard down. We feel safe, and so we share more than we would with a stranger.

But do you personally know all the people who follow you on social media? And how do you know that the person you are interacting with online is who they say they are?

The truth is you don't. "Catfishing" is the term used when someone creates an elaborate fake identity to pretend to be someone else. This often is used to manipulate someone else.

Many people, including adults, have been fooled by catfishing scams. In the best-case scenario, it is embarrassing to realize you were tricked into believing your online "friend" is someone they are not. Often there are worse circumstances where the victim can be conned, blackmailed, bullied, or emotionally, and even physically abused.

Here are some tips to verify someone's online profile matches their identity:

- **Search their name** — if someone uses their full name in their online profile, search for them in Google or another search engine. If you find the same person on multiple social media platforms, that's a good sign. You can also use where they live or their school's name as other search terms to focus your search.

- **Reverse Image Search** — On images.google.com, you can perform a reverse image search to see where this image shows up on the internet. Click on the camera image in the Google search bar and enter a URL for the picture or upload the picture file itself. Suppose their profile picture is from a stock image site or used on several different social media accounts (all with other names). In that case, they may not be who they say they are.

If you think someone is not who they say they are, block them right away! This cuts off the access they have to your information.

Protect Your Privacy

Social media is meant to be just that—social. Because we're connected with friends, it's easy to put more information online than we should. This is especially a problem if we don't have the proper privacy settings on our accounts. Still, as we learned with catfishing, it can also be a problem if we are "friends" with people we don't know.

Start by checking the privacy and security settings of all your social media and internet accounts. Be sure your photos, videos, posts, and other personal data are only visible to your contacts. Many services allow you to set these privacy settings as a global default. Still, you need to investigate what happens to any posts you made before you changed your default privacy settings.

While you are checking your settings, be sure to review your location services settings as well. Location services are handy for apps and websites to know where you are and make suggestions or offer services based on your location. But they can also populate the internet with data about where you live, go to school, or hang out.

Turn off location services for apps and then evaluate each app or website that asks for permission to use location services. If you absolutely need this functionality, only give the app permission to track your location when using it. This prevents the app from tracking your movements when it isn't open.

Don't "overshare" on social media or other online accounts. Everything you share in the digital landscape can be used to create a profile about you. Consider carefully the memes, jokes, and opinions you share online. The internet doesn't forget, and later in life, your seemingly harmless joke or TikTok video may keep you from getting your dream job.

The best rule of thumb is to assume that anything you put on the internet is public information, and anyone can see it. Privacy settings can help, but it really requires you to stop and think before each post, share, like, or follow.

Identifying Scams

Internet scams are everywhere. The 2019 FBI's Internet Crime Complaint Center (IC3) annual report showed the agency averaged 1,200 complaints per day, with many more unreported. The losses for victims in 2019 exceeded $3.5 billion. While elderly people are more likely to be taken by these scams, the IC3 report showed more than 55,000 cases reported by individuals under 30, with losses for these cases at $596.2 million in 2019 alone.[2]

Knowing how to identify a scam is a crucial step in not getting taken by scammers. Here are some ways to "spot the scam."

- If it's too good to be true, it probably is! You're not going to get the latest gadget or most popular shoes or headphones at 50 percent off.
- If money is involved, be suspicious. This includes people who want to give you money requiring you to provide them with your bank account number. Even requests for money from people you know should be double-checked, including the amount they are requesting, how best for you to send it to them.
- Before clicking any links in email, texts, or social media posts, verify who sent you the link and if it's legitimate. Hover over links before clicking on them to see where it will actually send you. If you're not sure about a link, don't click it. Try finding the site using a search engine and see if the URLs match.
- Scammers often use fear or urgency to get people to act without taking time to think. Messages demanding you respond right away are often scams. This is especially true if they appear to come from official-sounding agencies like the Social Security Administration. (No, they aren't going to cancel your Social Security Number.)
- Know the URL of the company you are interacting with and verify that you're on the correct site. Scammers often buy similar domain names or URLs that are commonly mistyped, especially if you're on your phone.

Other Security Concerns

Here are some other tips to help you stay safe online:

- If you use a public computer, such as at the library or school, do not allow the computer to save your username or password. Log off the computer when you are done to clear the cache and delete temporary files you may have accessed.
- External drives can carry viruses and malware. Do not use a USB drive you find on the ground. If you don't have antivirus software on your computer, you should not use a friend's external drive either.

[2] Federal Bureau of Investigation Internet Crime Compliant Center. (2019). 2019 Internet Crime Report. Retrieved from FBI IC3 website https://www.ic3.gov/Home/AnnualReports

- Be cautious of public USB charging stations. These can also contain viruses that can infect your phone or computer. It's always best in public to charge your devices using an electrical charger rather than a USB cable.

Cyberbullying

Cyberbullying is one of the biggest challenges facing children and teens on the internet. Many people who would never be a bully in real life become bolder when hidden away behind a computer screen, especially if they think they're anonymous.

The United States Centers for Disease Control and Prevention (CDC) define bullying as "unwanted aggressive behavior by another youth or group of youths…that involves an observed or perceived power imbalance, and is repeated multiple times or is highly likely to be repeated." Notice that bullying does not have to involve physical violence or even verbal abuse. Spreading rumors about someone, posting demeaning photos, or intentionally leaving them out of the group can fit the definition of bullying. The CDC states 1 in 6 high school students report being bullied online.[3]

In some ways, cyberbullying is worse than the abuse from a physical bully. When you're being bullied at school or the playground, your shame and embarrassment are limited to those present. When you leave that physical location, the bullying stops. This allows you to escape the situation.

With cyberbullying, there is no escape. A bully can follow you virtually and continue to harass you even when you are not with them. And your embarrassment is on display for everyone to see. In this sense, cyberbullying can be worse than physical bullying because there is no escape.

If you are a victim of cyberbullying, you should not feel ashamed. You are a victim, and you didn't do anything wrong. But you do need to take steps to prevent this from continuing:

1. Do not retaliate. It's understandable to want to "fight back" and post nasty things online about your bully. However, this will not solve the situation and may make it worse.
2. Document the bullying. Make sure you screenshot messages and posts so they cannot be deleted. Record the date and time of the message, as well as who sent it.
3. Involve an adult. Share the images of the bully's messages with a parent, teacher, or another adult. Tell them how these messages make you feel and ask them to help you resolve the situation.

Remember, cyberbullying is more difficult for parents, teachers, or adults to notice, so it is essential that you tell an adult if you are being harassed online.

[3] Centers for Disease Control and Prevention. (2014). Preventing Bullying. Retrieved online at https://www.cdc.gov/violenceprevention/youthviolence/å/fastfact.html

ACTIVITY

After talking about some of the issues children face online, use this simple game to reinforce what they've learned.

Preparation

Print out enough copies of the two included emojis (page 13) so each child can have one of each. Consider printing them front and back to save paper. You can also attach them to wooden craft sticks if you like. If you don't have access to a printer, the kids can use their hands to give a thumbs up or thumbs down.

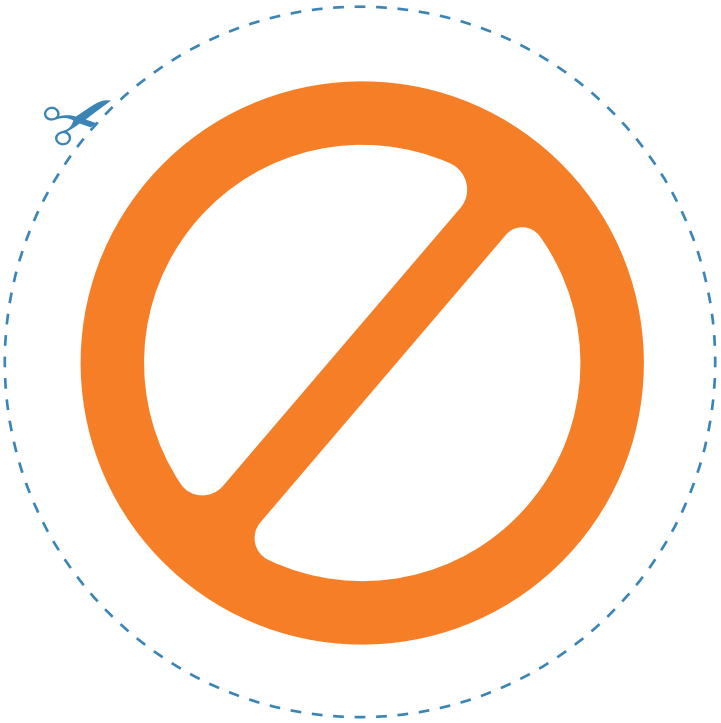
How to Play

Read the list of scenarios to the class and have the children use the emojis to respond if that activity is *"on target"* or something to *"avoid."*

Most will get these questions right, and those that are wrong are likely because they accidently put up the wrong emoji. If someone gets a question wrong, take the opportunity to reinforce the principle behind the scenario.

Scenarios

- Use your cat's name and your birth year as your password.
- Tell your friends to stop making fun of a classmate online.
- Verify that a link in an email from your grandma is safe before you click it.
- Sign up for a new social media platform without talking to your parents first.
- Accept a friend request from someone you don't know, as long as they say they know your parents.
- Do some research before accepting a friend request to make sure the person is who they say they are.
- Have a private chat in a Zoom room with one of your youth leaders or Pathfinder staff.
- Delete email, texts, or private messages right away from people you don't know if they have a link in the message.
- Share memes that make fun of people from other cultures or countries.
- Tell an adult if you are being bullied online.
- Think about what you want to post online before you hit send, especially if you're upset or it's late at night.
- Set your social media privacy settings so only your friends can see your posts and information.
- Click on the link for 80 percent off AirPod Pros that your friend shared on their Instagram story.
- Share inappropriate pictures of yourself or anyone else.
- Avoid public USB charging ports.
- Use a different password for each account you have.
- Talk bad about a classmate in a private chat since they will never see it.
- Post a picture of your house online.
- Block and report anyone who sends you inappropriate comments or pictures.
- Post on social media that you'll be at your local mall later this afternoon without an adult.
- Tell an adult if someone online tries to get you to meet them somewhere.
- Assume everything you put online is public.
- Share the link for your online Zoom classroom on the public Discord channel.
- Don't retaliate if you are being bullied online.
- Use only numbers for your password.



DISCUSSION QUESTIONS

Use the following questions to start a discussion with your class about how they use the internet and social media and how they think they could be safer online.

What are some of your favorite apps/websites to visit? Are you on any social media apps? If so, which one(s) do you use most often?

What are some of the positive and negative things about social media? Do you think the positives outweigh the negatives? Do the negatives outweigh the positives? Or, are they about equal?

Not counting school and/or homework, how much time a day do you think you spend on the internet each week? Has that time increased or decreased during the pandemic? What types of things are you missing out on when you spend time online?

What type of restrictions do your parents put on your internet / social media usage? Why do you think they have these restrictions? Should you have more restrictions than what you currently have?

Where do you get your news and information from on the internet? How can you be sure that the "facts" you see are accurate? Why do you think some sites or social media accounts share information that is not accurate? What can you do when you find incorrect information online?

What examples of cyberbullying have you seen? Were you the one being bullied, or was it someone else? How did you respond to those incidents? How should you have responded?

What peer pressures do young people face when it comes to the internet and social media? Do these pressures come primarily from people you know, from people you don't know, or from celebrities and/or influencers?

Obviously, the internet wasn't around during Jesus' ministry? If it was, how do you think He would have used these tools in His ministry? What are some of the ways your church could use the internet and/or social media to spread the Gospel? How can you use your online presence to show God's love?

Adventist Risk Management,® Inc. (ARM) is invested in the safety and success of your ministry. We provide risk management resources to help you protect the people and physical assets at the heart of your ministry. *Our ministry is to **protect** your ministry.* Learn more at AdventistRisk.org/About-Us. **#ARMcares**

REPORT YOUR CLAIM RIGHT AWAY
1.888.951.4276 • CLAIMS@ADVENTISTRISK.ORG

STAY INFORMED
ADVENTISTRISK.ORG/SOLUTIONS