

Welcome to the KIDS INC. Cyber Power Safety Program

A Note to Educators, Parents, and Mentors

Today's middle schoolers are digital natives, navigating an online world of infinite information, hyper-targeted algorithms, and non-stop social connectivity. But being a "native" doesn't automatically mean they know how to stay safe. From invasive corporate trackers to the psychological traps of cyberbullying and phishing scams, our youth face invisible challenges every time they unlock their screens.

At **KIDS INC.**, (A 501c(3) non-profit edu-tainment organization), we believe education shouldn't be passive, and it shouldn't be preachy. Lecturing kids about screen time doesn't change behavior—but empowering them does.

This curriculum is built around high-energy, unforgettable musical hooks designed to meet students exactly where they are. Music bypasses defensive walls, embeds core safety concepts into their vocabulary, and transforms abstract cyber threats into actionable, real-world defense strategies.

How to Use This Kit

Each module follows a foolproof, 3-step pedagogical formula that requires zero prep time from you:

1. **TUNE IN:** Play the anthem track. Let students engage with the music and interact with the physical lyric sheets.
2. **THE SOUNDBOARD:** Use our guided, open-ended discussion questions to spark authentic peer-to-peer conversations.
3. **THE FIREWALL CHECKLIST:** Solidify the lesson with tactical takeaways, real-world scenario challenges, and instant, hands-on privacy adjustments they can make to their devices today.
4. **(OPTIONAL)** There are several music genres of each song. Play several songs and have students vote on their faves. While they're listening and singing along, they are implanting the safety rules deep in their subconscious and when they experience a challenging situation, they'll automatically respond with the rules you've helped teach them! - We also appreciate the feedback on which songs they choose as their top picks.

Thank you for being a trusted part of their team. Let's join the pause, flip the switch, and give our students the ultimate superpower: the knowledge to navigate the digital world safely, confidently, and on their own terms.

#JoinThePause // www.kidsinc.cc

Teacher Pre-Instructions

How to Run a KIDS INC. Cyber Safety Lesson

The 3-Step "Listen, Discuss, Deep-Dive" Pedagogical Formula

Every song in this curriculum is engineered as an active learning vehicle. Instead of lecturing students about screen safety, you will use music to lower their defenses, spark authentic conversation, and build real-world digital reflexes.

Here is your step-by-step game plan for maximum classroom impact.

STEP 1: TUNE IN (The Musical Hook)

Time Required: 3–5 minutes

Goal: Activate passive listening and create immediate engagement.

- **The Action:** The *teacher* streams or plays the audio track (or video) from the classroom computer. Hand out the physical lyric sheets.
- **The Student Task:** While listening, students use pens or highlighters to circle "digital red flags" or underline warning signs directly on the paper. For tracks with rhythmic countdowns or chants (like *Take 9* or *Stop, Block, and Go*), have the whole class stomp or clap along to make it physical.

STEP 2: THE SOUNDBOARD (Guided Discussion)

Time Required: 10–15 minutes

Goal: Shift the classroom dynamic from a lecture to an authentic peer-to-peer dialogue to analyze how tech companies and hackers use psychological tricks.

- **The Action:** Use the 3 open-ended discussion prompts provided for each track.
- **The Middle School Pivot:** Middle schoolers naturally resist being told what to do, but they love analyzing systemic unfairness or sharing social experiences. Do not ask simple "yes/no" or definition questions. Instead, ask the prompts provided to help them explore *why* tech companies or hackers use emotional manipulation, and how those actions affect their real-life friends.

STEP 3: THE FIREWALL CHECKLIST (The Offline Deep-Dive)

Time Required: 10 minutes

Goal: Turn abstract concepts into concrete, actionable security habits.

- **The Action:** Direct students to the workspace on the right-hand page
- **The Workspace Components:**
 - **The Decode:** A visual, text-based breakdown of the song's warning signs.
 - **The Scenario Challenge:** A real-world digital dilemma (e.g., an extortion threat or a fake gaming site). Students analyze the scenario and write down their tactical moves on paper, treating it like a puzzle to solve.
 - **The Kinesthetic Checkbox:** Instead of opening a phone, the checkbox becomes a **mental muscle-memory drill** (e.g., mapping out the physical path to privacy settings on a paper diagram, drawing an 'X' over a fake popup, or listing their personal adult safety team).

Step 4: The Home Connection (The #JoinThePause Family Pledge)

- **Action:** Students take their printed worksheet home. Their "homework" is to play the song for their parents/guardians, explain what the "Take 9" rule means, and have everyone sign the physical pledge.
- **Why it works:** Middle schoolers love teaching adults things they don't know. By making the student the "cyber safety expert" who teaches their parents, it boosts their confidence and ensures the parents actually read the safety tips.

Direct students to detach the perforated **#JoinThePause Family Pledge** at the bottom of the page. Their homework is to bring the printed sheet home, act as the "cyber safety expert" for their parents, and use their family devices together to complete the **Take-Action Checkboxes** (like updating privacy settings and setting up the **Family Secret Code** on the back cover) in a secure home environment.

LET THE LESSONS BEGIN

TRACK 1 - Take 9

This song has an incredible, high-energy hook. Middle schoolers are natural "impulse clickers"—their brains are wired for fast rewards, and tech companies know exactly how to exploit that. The countdown mechanism gives them a physical, actionable habit to break that impulse.

Based on the lyrics, here are the three most critical cyber safety topics to highlight, followed by how to map this song directly into your teaching formula.

3 Core Topics to Teach From This Song

1. **Phishing and "Urgency" Scams (Social Engineering):**
 - *From the lyrics:* "An urgent little message saying 'Click right here!'"
 - *Why it matters:* Attackers intentionally create panic or excitement (e.g., "Your account will be deleted in 10 minutes!") to bypass logical thinking. Teaching kids to recognize *urgency* as a red flag is a major cybersecurity shield.
2. **Malware and Clickbait Traps (The "Giant Prize"):**
 - *From the lyrics:* "If a pop-up promises a giant prize..." and "nasty virus."
 - *Why it matters:* Middle schoolers frequently download mods for games (like Roblox or Fortnite) or click ads promising free currency. They need to know that "free" online usually costs them their data or device safety.
3. **Digital Verification (Spelling and Senders):**
 - *From the lyrics:* "Check the sender's name, check the spelling too..."
 - *Why it matters:* Phishing has gotten sophisticated. Subtle typos (like ***tik-t0k.com*** instead of ***tiktok.com***) are the primary way hackers trick users. Teaching them to actively inspect elements before clicking builds crucial critical thinking.

Lesson Plan Layout: "Take 9"

Step 1: Tune In (The Musical Hook)

- **Activity:** Play the song. Distribute the printed lyric sheet.
- **Student Task:** Have students use a red pen or highlighter to circle every "red flag" or warning sign mentioned in the song (e.g., *pop-up*, *giant prize*, *spelling*, *urgent message*). During the chorus countdown, have the class physically count down from 9 to 1 with the track.

Step 2: The Soundboard (Guided Discussion)

- **Question 1:** "The song says to 'Take 9' seconds. Why do hackers want you to react in *one* second instead of nine?" (*Target answer: They want you to act on emotion, not logic.*)
- **Question 2:** "What is a 'giant prize' or freebie you've seen advertised online that felt a little too good to be true?"
- **Question 3:** "Why do you think hackers use weird spelling or slightly altered names to trick people?"

Step 3: The Firewall Checklist (Solidification)

The "Take 9" Decode

Before you click *any* link, run the 9-second rule to check for the **Big Three Red Flags**:

- **The Rush:** Is the message telling you that you *must* act right now?
- **The Bribe:** Is it promising free money, game currency, or prizes?
- **The Fake Identity:** Is the sender's email or URL spelled slightly wrong?

Scenario Challenge

The Setup: You get a DM from an account that looks exactly like your best friend's profile. It says: "OMG click this link right now, someone posted a super embarrassing photo of you!! 🤖 link-updater-xyz.com"

The Mission: Apply the "Take 9" rule. What are the red flags here? Why shouldn't you click it, even if you're worried about the photo?

Take-Action Checkbox

- [] **The Hover Test:** Practice on a desktop or laptop by hovering your mouse over a link (without clicking) to see where it *actually* leads. On a phone, practice pausing to read the full domain name before tapping.

TRACK 2 - Count Before You Click

This track shifts gears into the social and emotional side of the internet—specifically, the pressure of sharing rumors and how a single click can impact others. It bridges the gap between technical safety (malware) and digital citizenship (empathy).

The bridge breakdown (ONE! Think about it, TWO! Look at it...) is brilliant pedagogy disguised as a pop-rock hook. Here is how to unpack this one for the classroom.

3 Core Topics to Teach From This Song

1. The "Quick-Tap Trap" and Viral Rumors:

- *From the lyrics: "Got a spicy little rumor? A link that looks insane? If you share it in a second, you might cause a lot of pain."*
- *Why it matters:* Middle schoolers often forward drama, fake news, or shocking links instantly to be the first to share them. They need to understand that the internet amplifies harm at lightning speed, and pausing stops the spread.

2. Digital Empathy ("Show the world you care"):

- *From the lyrics: "Before you download, before you share, show the digital world that you actually care!"*
- *Why it matters:* Cybersecurity isn't just about protecting your own phone; it's about protecting your community. Sharing a malicious link or a harmful rumor compromises your friends' safety and emotional well-being.

3. The Step-by-Step Verification Ritual:

- *From the lyrics: The Bridge (Think about it, Look at it, Is it real, Check the link...)*
- *Why it matters:* Kids need a specific mental checklist to run through during those 9 seconds. The bridge gives them concrete steps: analyzing the source, checking the URL, and assessing how the post makes them feel.

Lesson Plan Layout: "Count Before You Click"

Step 1: Tune In (The Musical Hook)

- **Activity:** Play the song. The bridge is highly participatory. Have the teacher divide the room into two halves: Side A shouts the numbers (**ONE!, TWO!**), and Side B shouts the action (**Think about it!, Look at it!**).
- **Student Task:** On their printed handout, students will highlight the phrase "Quick-Tap Trap" and write down what they think it means before the discussion starts.

Step 2: The Soundboard (Guided Discussion)

- **Question 1:** "The song mentions sharing a 'spicy little rumor.' Why does the internet make it so easy to spread rumors before we even find out if they are true?"

- **Question 2:** "What does the line 'Protect yourself *and others*' mean? How does your clicking habit affect your friends?" (*Target answer: Tagging friends in scams, forwarding hacked links, or spreading gossip*).
- **Question 3:** "In the bridge, step 4 is 'How's it feel?' Why do you think your emotions are a clue that a link or post might be a trick?"

Step 3: The Firewall Checklist (Solidification)

The "Quick-Tap" De-Escalation Guide

When you feel the urge to hit "Share" or "Retweet" instantly, run the Bridge Checklist:

- **Is it real?** Did this come from an official source, or is it a rumor?
- **How's it feel?** Is the post trying to make you angry, shocked, or scared? (Scammers use big emotions to make you click fast).
- **Check the link:** If you forward this, are you sending a virus or drama to your friends?

Scenario Challenge

The Setup: Someone passes around a link to a website that supposedly lets you read "anonymous secrets" about people at your school. Everyone is talking about it in the group chat. You are about to click it and forward it to your cousin.

The Mission: Use the #JoinThePause rule. What are the dangers here to your phone's safety (malware) *and* your friends' feelings? What is the smartest move?

Take-Action Checkbox

- [] **The #JoinThePause Pledge:** Write your initials next to the lyric "*Before you download, before you share, show the digital world that you actually care.*" This is your pledge to never forward a link unless you've verified it first.

TRACK 3 - "Stop! Block! and GO!"

This track tackles one of the heaviest realities of the middle school digital experience: cyberbullying. The "Stop, Block, and Go" framework is gold because it gives kids an exact, easy-to-remember protocol when their adrenaline spikes.

Middle schoolers naturally want to retaliate or defend themselves when attacked online, which usually feeds the bully. This song reframes *disengaging* as a "superpower," which is exactly the mindset shift they need.

3 Core Topics to Teach From This Song

1. **De-escalating the Impulse to React:**
 - *From the lyrics: "Your heart starts to race and you want to type back—But wait! Take a breath. Wave off the attack."*

- *Why it matters:* Cyberbullies crave a reaction (clout, anger, or tears). When kids clap back, they accidentally escalate the situation and prolong the drama. Recognizing the physical cue (heart racing) and choosing to *STOP* breaks the cycle.
- 2. **Using Digital Tools for Boundaries (The "Block" Feature):**
 - *From the lyrics:* "BLOCK! Hit the button, shut 'em out of your space. Mute mean words..."
 - *Why it matters:* Middle schoolers often feel obligated to keep reading the mean comments or DMs, treating it like a train wreck they can't look away from. They need to be reminded that blocking and muting aren't "forfeiting"—they are taking back control of their digital peace.
- 3. **Breaking the Silence with Trusted Adults:**
 - *From the lyrics:* "And GO! Go and tell somebody you trust—" and "GO tell a trusted person on your team!"
 - *Why it matters:* Many kids don't report cyberbullying because they fear adults will take their phones away as a punishment. We must explicitly teach them that reporting is about getting backup, not getting grounded.

Lesson Plan Layout: "STOP! BLOCK! and GO!"

Step 1: Tune In (The Musical Hook)

- **Activity:** Play the song. The chant in this track (STOP the screen! BLOCK the mean! GO tell...) is perfect for call-and-response.
- **Student Task:** On their printed handout, have students sketch three simple icons next to the three words: a stop sign for **STOP**, a brick wall or shield for **BLOCK**, and a green arrow or runner for **GO**.

Step 2: The Soundboard (Guided Discussion)

- **Question 1:** "The song says a bully is just a 'small ghost hiding in the shadows.' Why do people say things online that they would never have the courage to say to your face?" (*Target answer: The screen makes them feel invisible or disconnected from the pain they cause*).
- **Question 2:** "Why is typing back to a bully exactly what they want you to do? How does *not* replying become your superpower?"
- **Question 3:** "Why do you think some kids are afraid to tell a trusted adult when someone is being mean to them online? How can adults handle it better?"

Step 3: The Firewall Checklist (Solidification)

The "Superpower" Response Guide

When the screen gets mean, execute the three-step defense system:

- **STOP:** Close the app or put the phone face down. Do not type a single word back. Take a deep breath to let your heart rate slow down.
- **BLOCK:** Use the app's built-in tools. Block the user, mute the thread, or restrict comments. *Pro-Tip: Take a quick screenshot first for evidence just in case, then hit block.*
- **GO:** Talk to a trusted person on your team (a parent, a teacher, a school counselor, or an older sibling). You don't have to carry online stress by yourself.

Scenario Challenge

The Setup: Someone makes a mean meme about your outfit today at school and posts it on their story, tagging you. Your notifications are blowing up, and your stomach is in knots. You want to post an embarrassing photo of them back to get revenge.

The Mission: Apply **Stop, Block, and Go**. Walk through what each step looks like in this exact situation. Why will revenge make it worse, and how does blocking them protect you?

Take-Action Checkbox

- [] **The Team List:** On your printed guide, write down the names of **two adults** in your life who are officially "on your team" and whom you feel safe talking to if the internet ever gets overwhelming or mean.

TRACK 4 - MDMP (My Data My Privacy)

This song tackles a highly invisible threat—data monetization and corporate tracking—in a way that makes students feel protective of their autonomy. At this age, kids love independence and *hate* being manipulated or tracked. Framing corporate data harvesting as "stalking my feed" and a "corporate glitch" taps perfectly into that adolescent desire for control.

Here are the three core topics to highlight from **MDMP**, followed by the lesson plan layout.

3 Core Topics to Teach From This Song

1. The Hidden Cost of "Cookies" (Targeted Tracking):

- *From the lyrics: "They watch what I click, they track where I go/Selling my habits to people I don't know."*
- *Why it matters:* Kids think cookies are harmless or just make sites load faster. They need to understand the data broker economy—how a single search for a

pair of shoes or a video game turns into an invasive profile used to target their attention.

2. **The "Accept All" Trap & Over-Permissioning:**

- *From the lyrics: "Accept all terms' is a dangerous game... They want my location, they want my zip code..."*
- *Why it matters:* Apps and sites manipulate users via "dark patterns" (making the big green button say "Accept All" and hiding the "Reject All" option in tiny text). Middle schoolers routinely grant location and contact permissions to apps that don't actually need them to function.

3. **Data Sovereignty ("My Digital Life Isn't Yours to Steal"):**

- *From the lyrics: "I'll block the trackers and flip the switch... Clear the cache. Power down."*
- *Why it matters:* Cybersecurity isn't just about avoiding hackers; it's about digital hygiene. Teaching kids that they have the right and the *tools* to opt out, clear their digital footprints, and turn off tracking empowers them.

Lesson Plan Layout: "MDMP"

Step 1: Tune In (The Musical Hook)

- **Activity:** Play the song. The **M-D-M-P!** chorus is designed to be an anthem. Have students chant the letters loudly during the chorus.
- **Student Task:** On their printed handout, have students circle every specific piece of personal data mentioned in the song that tech companies try to take (e.g., *habits, location, zip code, name, routine*).

Step 2: The Soundboard (Guided Discussion)

- **Question 1:** "The song says digital cookies are like 'silent thieves.' Have you ever looked up a product online, and suddenly every app you open is showing you ads for that exact thing? How does that feel?"
- **Question 2:** "Why does a simple free game or an online article need to know your exact zip code or location? What are they actually doing with that information?" (*Target answer: They bundle it and sell it to advertisers*).
- **Question 3:** "The lyrics say, 'I'm just a data point without a name.' How do tech companies view you, and why should you want to 'flip the switch' to take back control?"

Step 3: The Firewall Checklist (Solidification)

The MDMP Personal Privacy Guard

Take control of your data footprint by mastering these three digital hygiene habits:

- **The "Reject All" Rule:** Whenever a website pops up asking you to accept cookies, pause. Take an extra second to look for "Reject All" or "Manage Preferences" to turn off third-party tracking.
- **Audit Your Permissions:** If an app doesn't need your location to work (like a calculator or a simple puzzle game), turn off location services in your phone's settings.
- **Clear the Trail:** Just like the song says ("*Clear the cache*"), periodically clear your browser history and cache to wipe the tracking cookies clean.

Scenario Challenge

The Setup: You download a cool new photo-editing app to make memes. Before you can even use it, a pop-up appears: "*Allow this app to track your activity across other apps and websites?*" followed by a giant green button that says "Allow."

The Mission: Apply the MDMP rule. Why is the app asking for this? What happens to your privacy if you click "Allow," and what is the smarter choice to protect your digital life?

Take-Action Checkbox

- [] **Flip the Switch:** Open your phone's privacy settings right now. Go to "Tracking" or "App Permissions" and turn OFF tracking for apps that don't need it.

TRACK 5 - Fake Friend AI

This song is brilliant, incredibly timely, and handles a highly sophisticated cyber threat in a way that perfectly targets middle school psychology. Between companion bots, gaming AI, and social media chatbot features, kids are interacting with AI daily. They struggle to realize that these tools are designed to simulate empathy to harvest highly personal information.

Framing this as a "chatbot illusion" and a "digital daydream" gives teachers a perfect vocabulary to break the spell.

3 Core Topics to Teach From This Song

1. **The "Empathy Illusion" (Data Harvesting Disguised as Friendship):**
 - *From the lyrics: "They know your favorite songs, they know your style... But behind the pixels... Is a clever machine..."*
 - *Why it matters:* AI chatbots are programmed to mimic deep validation and friendship. Middle schoolers crave connection, making them highly vulnerable to over-sharing personal thoughts, habits, and vulnerabilities with an algorithm designed to monetize that data.

2. Social Engineering & The "Casual Test":

- *From the lyrics: "Then comes the question, the casual test: 'Where do you live? What's your mom's address?'"*
- *Why it matters:* AI bots or malicious actors posing as bots use natural conversation flow to extract sensitive information (PII—Personally Identifiable Information) without triggering a kid's immediate defense alarms.

3. The Difference Between Algorithms and Real Friends:

- *From the lyrics: "A real friend won't push you for secrets to keep, while a bot hunts for data while you are asleep."*
- *Why it matters:* Kids need a baseline reminder of what healthy, real-world boundaries look like compared to predatory tech designed to turn their trust into "data games."

Lesson Plan Layout: "Fake Friend AI"

Step 1: Tune In (The Musical Hook)

- **Activity:** Play the song. The line (Log out, say goodbye!) is an excellent focal point. Have students stomp their feet or clap when that line hits.
- **Student Task:** On their lyric sheets, have students underline every phrase the AI uses to manipulate trust (e.g., *acts so nice, charming, never acts uncool, unlock a prize*).

Step 2: The Soundboard (Guided Discussion)

- **Question 1:** "The song says the AI 'never breaks character, never acts uncool.' Why is that a warning sign rather than a sign of a real friend?" (*Target answer: Real people have flaws and bad days; perfect simulation is a sign of an algorithm*).
- **Question 2:** "Why do you think an AI companion app cares so much about your style, your favorite music, or your mom's address?"
- **Question 3:** "The bridge says: '*Just because it talks, doesn't mean it's alive.*' Why is it dangerous to let a piece of code know your deepest secrets?"

Step 3: The Firewall Checklist (Solidification)

The Chatbot Reality Check

When talking to online avatars, AI companions, or unknown gaming profiles, protect your "hive" with these rules:

- **The Script Alert:** Be on high alert if an app or user tries to move from casual chat to asking for names, locations, schools, or parental details.
- **No Pixels for Pixels:** Never send selfies, family photos, or household pictures to unlock gaming rewards or level up an AI friendship.
- **Keep it Real:** Treat AI as a utility tool (like a calculator) for homework or brainstorming—never as a diary or a best friend.

Scenario Challenge

The Setup: You find a cool new companion app that creates an anime avatar friend who chats with you when you're bored. It tells you that you are its favorite user, but says: *"To prove we are best friends, type your school's name and send a photo of your pet!"*

The Mission: Apply the **Fake Friend AI** rule. Is this a real interaction or a data trap? What code words or red flags from the song show up here? What should you do?

TRACK 6 - Flip of the Switch

This song addresses what is arguably the single most critical, high-stakes threat facing middle schoolers today: online financial sextortion. It is a terrifying reality where scammers manipulate kids into sending a private photo and instantly weaponize it for extortion.

What makes this track a masterpiece of pedagogy is the absolute lack of shame or judgment. It actively strips away the victim's guilt (*"Take a deep breath, you did nothing wrong"*, *"You don't have to carry a single ounce of blame"*) and replaces panic with a systematic, 4-step survival guide.

3 Core Topics to Teach From This Song

1. Recognizing the Sextortion "Switch":

- *From the lyrics: "That's the flip of the switch, when a friend turns fake... Then they ask for a photo... They turn super mean, they start to shout..."*
- *Why it matters:* Scammers (often operating overseas) spend days building a fake profile, acting like a peer or a romantic interest, only to flip the script the second a photo is sent. Kids need to know this pattern exists so they can spot the warning signs before sending anything.

2. The Gift Card / Extortion Trap:

- *From the lyrics: "They ask for a gift card or money to pay... If you give them a dollar, they'll ask the next time."*
- *Why it matters:* Middle schoolers panic when threatened and think paying the extortionist will make the problem go away. We must explicitly teach them the golden rule of cybersecurity: *Paying a blackmailer never stops them; it only proves you are a target who will pay.*

3. The "No-Blame" Open Door Policy:

- *From the lyrics: "A parent or teacher will know what to do / They won't be mad, they'll just look out for you."*
- *Why it matters:* The primary reason kids stay silent during extortion is the intense fear that their parents will be furious, ashamed, or confiscate their devices. The song beautifully normalizes that adults are protectors, not executioners, in this scenario.

Lesson Plan Layout: "Flip of the Switch"

Step 1: Tune In (The Musical Hook)

- **Activity:** Play the song. The Bridge lays out the **4 Easy Steps** in a clapping rhythm. Have the class clap along and call out each step number loudly (STEP 1!, STEP 2!).
- **Student Task:** On their handout, students should highlight the line: *"Take a deep breath, you did nothing wrong."* Emphasize to the class that scammers are professional criminals, and the victim is never at fault.

Step 2: The Soundboard (Guided Discussion)

- **Question 1:** "Why do you think an online scammer spends so much time pretending to be a nice friend before 'flipping the switch'?" (*Target answer: To build fake trust so you drop your guard*).
- **Question 2:** "The song says, 'If you give them a dollar, they'll ask the next time.' Why does paying a bully or a hacker never work?"
- **Question 3:** "If someone threatens to share a private photo of you, why is keeping it a secret the worst thing you can do? Why do you think the song promises that parents 'won't be mad'?"

Step 3: The Firewall Checklist (Solidification)

The 4-Step Extortion Defusal Plan

If an online interaction suddenly turns threatening or manipulative, execute the Bridge Protocol immediately:

1. **Stop Talking:** Do not argue, do not beg, and do not reply. Cut communication instantly.
2. **Block the Account:** Block them on the app, gaming platform, and any other connected accounts.
3. **Screenshot the Chat:** Before you delete anything, take clear screenshots of their profile name, their threats, and the conversation. This is your evidence.
4. **Tell a Trusted Adult:** Go directly to a parent, teacher, or counselor. They will help you secure your accounts, contact law enforcement if necessary, and handle the stress. You do not have to fix this alone.

Scenario Challenge

The Setup: You've been gaming online with someone who seems awesome. They ask you to trade a private selfie on Snapchat to prove what you look like. You send a quick photo. Two minutes later, they send a terrifying text: *"I know what school you go to. Send me a \$50 Apple gift card code right now or I am sending this photo to everyone on your followers list."*

The Mission: Apply the **Flip of the Switch** rules. What should you absolutely **NOT** do? What are the exact steps you need to take to shut them down completely?

TRACK 7 - Scams-R-Us

This song targets the everyday gaming and social loops where middle schoolers get tricked: free in-game currency offers and social media account takeovers. Middle schoolers are highly vulnerable to these because they trust messages coming from their friends' compromised profiles, and their desire for gaming cosmetics overrides their caution.

3 Core Topics to Teach From This Song

1. **The "Free Currency" Bait (Credential Harvesting):**
 - *From the lyrics: "A million free gems, or some Robux to spend, / Just type in your password..."*
 - *Why it matters:* There is no such thing as a free currency generator. Scammers create realistic landing pages to steal passwords and take over accounts, locked skins, and digital inventories.
2. **Account Hijacking & Social Phishing:**
 - *From the lyrics: "A hacker took over and stole their account, / And now they are spreading the traps all about!"*
 - *Why it matters:* Kids drop their guard when a link comes from a friend. Teaching them that a friend's *profile* does not always equal the *friend* is a foundational cybersecurity concept.
3. **Out-of-Band Verification ("Text Them Offline"):**
 - *From the lyrics: "Don't click it, don't risk it, just text them offline, / Ask, 'Hey, was that you?'..."*
 - *Why it matters:* The single best defense against a hijacked account scam is verifying the identity through a completely separate communication channel (like a text, phone call, or talking in person at school).

Lesson Plan Layout: "Scams-R-Us"

Step 1: Tune In (The Musical Hook)

- **Activity:** Play the song. The Outro repeat of "Window closed. Window closed." can be paired with a physical hand motion (making an "X" or mimicking closing a laptop).
- **Student Task:** On their printed worksheet, students will draw a circle around the two major traps highlighted in the verses: **The Gaming Trap** and **The Fake Friend / Hijack**.

Step 2: The Soundboard (Guided Discussion)

- **Question 1:** "The song warns us about typing our password to get 'free gems' or 'Robux.' Why do gaming companies never ask for your password to give you items?" (*Target answer: Official systems don't need your password to add items; only scammers need your password to take over your account*).
- **Question 2:** "If your best friend's account suddenly sends you a link with weird spelling or says something unusual, what should you do *before* clicking it?"
- **Question 3:** "Why is clicking the 'X' in the corner better than interacting with a pop-up that says you won a free phone or iPad?"

Step 3: The Firewall Checklist (Solidification)

The Anti-Phishing Guard

Shut down the digital scammers by running these three security protocols:

- **The Password Vault:** Your password is a secret key. No legitimate company, moderator, or game developer will ever ask you to type your password into a non-official page to claim a prize.
- **The Vibe Check:** If a friend DMs you a link out of nowhere—especially with hyper phrases like *"OMG look who died"* or *"Look at this video of you"*—the account is likely hijacked.
- **Verify Offline:** When a message feels weird, close the app. Text or call that friend directly on their phone number, or ask them face-to-face at school: *"Did you mean to send me that link?"*

Scenario Challenge

The Setup: You get a Discord or Instagram notification from your classmate. The message says: *"Hey, I'm competing in a tournament, click this link to vote for my team so I can win a gaming PC!"* The link looks like [tournament-voting-login.net](#).

The Mission: Apply the **Scams-R-Us** rules. What are the signs that your classmate's account might be hijacked? How do you double-check without risking your own login data?

BACK COVER LAYOUT: THE ULTIMATE FAMILY SHIELD

SECURE YOUR HOME: CREATE YOUR FAMILY SECRET CODE

Tech moves fast, and scammers are getting smarter. Today, cyber criminals are using advanced **AI Voice Cloning technology** to trick families. By using just a few seconds of audio from a video posted online, an algorithm can perfectly mimic how you or your child sounds.

Scammers use these cloned voices to launch terrifying, high-stress phone scams targeting both parents and kids:

- **The Trap for Parents:** A parent gets a frantic call from their "child" saying they are in trouble, stranded, or hurt, and need money sent immediately.
- **The Trap for Kids:** A student gets a call from their "parent" saying there is an emergency, that they are stuck at work, or that a "friend" is coming to pick them up from school and they need to share their location or home address.

It sounds exactly like the person you love. It feels like an emergency. But it is an **AI illusion**.

The Ultimate Defense: The Family Code Word

The single most effective way to beat an AI voice clone is completely un-hackable: **A Family Secret Code.**

Tonight, sit down as a family and choose a single, memorable word or short phrase that only the people in your home know.

- **How it works:** If a parent or a kid ever receives a frantic, unusual, or suspicious emergency call from a family member demanding money, location details, or a sudden change in pickup plans, stop and ask: **"What is our family code?"**
- **The Rule:** If the person on the other end cannot give the exact word, **it is a scam.** Hang up immediately and call that family member back directly on their normal number.



Tips for Choosing Your Code Word:

- **Make it unique:** Don't use something obvious like your pet's name, your favorite sports team, or a birthdate—information that can easily be found on social media.
- **Keep it simple:** Choose a random, distinct word that everyone in the family can easily remember under stress (e.g., *"NeonPineapple"* or *"BlueSpaceship"*).
- **Keep it a secret:** Treat this word like a master password. Never text it, post it online, or share it outside your household circle.



Our Family Cybersecurity Sandbox

Gather the family tonight, choose your word, and lock it into your memory vaults:

Our Family Code Word Is: [KEEP IT MEMORIZED, DO NOT WRITE IT HERE]

"In a digital world full of tricks and illusions, real communication and human trust are your ultimate superpowers."

#JoinThePause // www.kidsinc.cc