

RADICALIZATION & EXTREMISM

INTERACTIVE RESOURCE GUIDE



SAFER
SCHOOLS
TOGETHER



International Center for
Digital Threat Assessment



Copyright © 2025 Safer Schools Together. The reproduction of this material is strictly prohibited without the written permission of the copyright owners. All rights reserved. Disclaimer: Given the rapidly evolving nature of technology and social media applications, this information (especially social media platform-related) is current as of the date of publication.

This is an interactive document. Click the underlined links to read more or navigate to the correlating section of the document.

TABLE OF CONTENTS

- INTRODUCTION 1**
- UNDERSTANDING EXTREMISM 2**
- RADICALIZATION PATHWAY 3**
- WORRISOME, CONCERNING, OR THREAT-RELATED BEHAVIORS 4**
- ONLINE PLATFORMS & DIGITAL ENVIRONMENTS 6**
- EXTREMIST SUBCULTURES & COMMUNITIES 8**
- SYMBOLISM, MEMES & CODED LANGUAGE 9**
- GLOSSARY OF KEY TERMS 12**
- PLATFORM SPOTLIGHTS 14**
- 4CHAN UPDATE – APRIL 2025 16**
 - Incident Summary 16**
 - Current Status 16**
- MYTHS VS. FACTS 17**
- IDENTIFYING AND REPORTING RADICALIZATION 18**
 - Signs to Watch For 18**
 - Practical Steps for Educators 18**
- ADDITIONAL RESOURCES 19**

INTRODUCTION

Extremism and radicalization content can be embedded in the digital environments youth engage with daily. This guide is meant to support the Radicalization & Extremism Module by providing School Safety and Threat Assessment (SS/TA) Teams with real-world context, images, and links that help decode online radicalization.

We recommend that SS/TA Teams download and/or browse the platforms and forums referenced in this guide at their own discretion. The majority of the content shown on these platforms include content related to racism, radicalization, pornography, derogatory comments, and violence, which may activate a strong emotional response when seen. In line with the recommendations provided in our Digital Threat Assessment® training (available as a [live virtual training](#), [module](#), or [custom group trainings](#)), we also suggest that your SS/TA Teams create specific accounts for data collection. [Safer Schools Together \(SST\)](#) recommends against using personal accounts when searching as there is a possibility that the searching methods demonstrated may notify the Subject(s) of Concern (SOC).

UNDERSTANDING EXTREMISM

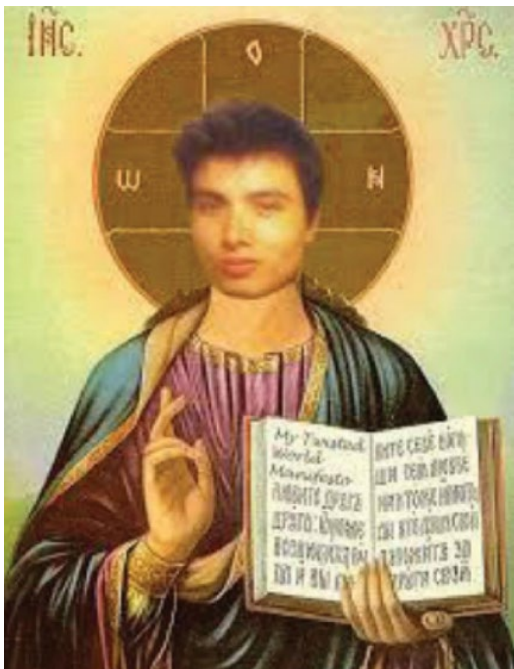
Extremism refers to ideologies that justify violence to achieve political, religious, or social goals. It thrives on absolutism, dehumanization, and often justifies harm against perceived adversaries. The Australian Government defines violent extremism as “supporting or committing ideologically motivated violence to further political goals.”¹

Notable ideologies known to adopt extremist and radical views include:

- White supremacy and nationalism
- Incel subcultures
- Anti-government/sovereign citizen movements
- Religious fundamentalism
- Accelerationist ideologies
- True Crime Community (TCC) fandoms and school shooter idolization

For information about various extremist ideologies, access the following resources:

- [Southern Poverty Law Center](#)
- [Anti-Defamation League](#)
- [Educate Against Hate](#)
- [Counter Extremism Project](#)
- [DHS](#)
- [Tech Against Terrorism](#)



An image depicting a noted incel attacker as a saint. This practice is common amongst extremist ideologies.

¹ [Australian Government, Living Safe Together \(n.d.\)](#)

RADICALIZATION PATHWAY

Much like the pathway to violence, radicalization is not a single event. It is a gradual process that typically begins with perceived injustices/grievances and ends in behavioral change or action. This process can be slow and subtle, especially in digital environments.

Radicalization typically follows a progression:

- **Perceived injustices/grievances:** the subjective belief or feeling that one has been treated unfairly or unjustly, often leading to negative emotions and potentially impacting recovery from injuries or illnesses.
- **Ideological Adoption:** adoption of extremist or radical ideology
- **Mobilization:** the actions taken by individuals or groups to prepare for and initiate violence or other harmful actions in furtherance of their extremist ideology

Behavioral Clues: Withdrawal, rigid beliefs, niche language, fascination with violence, and sudden online behavioral changes.

The National Counterterrorism Center (NCTC), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) created a useful guide containing additional information mobilization indicators.² School safety professionals should familiarize themselves with these indicators.

References

[RAND, *Countering Violent Extremism Online* \(June 2023\)](#)

[United Nations, *Countering Violent Extremism and Terrorist Narratives* \(n.d.\)](#)

[NPR, *Experts Warn That Recent School Shootings Show Growth in New Radicalization Pattern* \(March 2025\)](#)

[CIDOB, *What does Radicalisation Look Like? Four Visualisations of Socialisation into Violent Extremism* \(December 2016\)](#)

² [National Counterterrorism Center, *US Violent Extremist Mobilization Indicators* \(2021\)](#)

WORRISOME, CONCERNING, OR THREAT-RELATED BEHAVIORS

According to Dr. Meloy, these eight key behaviors are often present in individuals as they are radicalized to commit acts of violence.³

1. Pathway Behaviors

- Planning, research, and logistical preparation for an attack
- Includes weapon gathering, target selection/identification, and surveillance

2. Fixation

- Obsessive focus on a person, cause, or grievance. Often accompanied by deteriorating social behavior.
- In one study,⁴ 4 out of 5 violent mass attackers exhibiting some sort of fixation prior to committing the attack.

3. Identification

- Identification is when the SOC adopts the help belief as absolute and assumes the persona of a warrior, avenger, or even ideological soldier.
- The devolution from fixation to identification is especially concerning and must be acted upon immediately.

4. Novel Aggression

- Violent or aggressive behavior that is not goal-oriented (e.g. punching things, hurting others)
- Used to test capability or desensitize the self to violence.

5. Energy Burst

- Increase in activity before an attack (e.g. last minute preparations, writing, proselytizing).
- A surge of behavior is often linked to planning, travel, or gear acquisition.

6. Leakage

- Leakage is communication of intent (directly or indirectly) to a third party
- This is most frequently observed online in today's digital climate.
- Can include direct threats, vague references, manifestos, or shared violent ideologies.

7. Directly Communicated Threat

- Explicitly stated threat to harm a person or place.
- Less common among targeted attackers but still critical to assess.

8. Last Resort Behavior

- This is when an individual views their violent act as the only possible path forward; think martyrdom.
- Expression of desperation or urgency to act violently.

³ [Dr. Meloy, *Lone-Actor Terrorism: An Integrated Framework* \(December 2019\)](#)

⁴ [Dr. Meloy, *Terrorist Radicalization Assessment Protocol-18 \(TRAP-18\)* \(2016\)](#)

- Often tied to a perceived existential threat or final justification for violence.
- **IMMEDIATE CONCERN. SHOULD BE ACTED ON ASAP.**

For purposes of this training, we will focus on leakage. According to Dr. J. Reid Meloy, in the context to threat assessment, “leakage is the communication to a third party of an intent to harm a target...Leakage is a type of warning behavior that typically infers a preoccupation with the target, and may signal the research, planning, and implementation of an attack.”⁵

Leakage can often be observed as:

- **Fantasy:** glorifying violence, shooting memes, dark humor
- **Planning:** Specific threats or references, maps, weapons research
- **Justification:** Ideological reasoning, manifestos
- **Outcry:** suicidal ideation, grievance narratives, isolation

Behavioral clues: username(s) references extremists and/or attackers, manifestos, dark humor memes, or posts about violence, racism, or other extremist ideologies.

References

[Aggression and Violent Behavior, *Leaking in terrorist attacks: A review* \(2021\)](#)

[Frontiers in Psychiatry, *Editorial: Radicalization Among Adolescents* \(May 2022\)](#)

[U.S. Secret Service National Threat Assessment Center, *Mass Attacks in Public Spaces: 2016-2020* \(January 2023\)](#)

⁵ [Dr. Meloy, *The Concept of Leakage* \(2015\)](#)



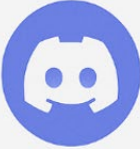


ONLINE PLATFORMS & DIGITAL ENVIRONMENTS

Youth engagement with extremist content often occurs on widely used platforms. Platforms such as Instagram, TikTok, YouTube, and countless others are exploited by individuals seeking to spread dangerous rhetoric to a more widespread audience. This section outlines where concerning behaviors may appear and the methods used by individuals to signal or reinforce radical ideologies online.

A 2024 report conducted by United States Government Accountability Office found that violent extremists were exploiting gaming platforms and social media to radicalize and recruit new individuals. The report further concluded that the FBI and DHS have not developed strategies to effectively communicate such concerns between key stakeholders.⁶ These findings underscore the critical importance of school-based digital threat assessments and multidisciplinary collaboration to detect and address online radicalization indicators early.

Common platforms of concern include but are not limited to:

- **TikTok:** POV shooter content, school shooter aesthetics, glorification edits
- **Instagram:** Shooter-themed aesthetics, incel humor reels, edgy quote pages
- **YouTube:** Shooter tributes, manifesto summaries, content promoting violent ideologies
- **Reddit:** Shooter-themed subreddits, manifestos, AMA threads
- **Telegram/Discord:** Encrypted communities for tactical discussion
- **Gaming Platforms:** Use of skins, custom maps, chats in Roblox/Minecraft

⌘ Online Platforms & Digital Environments				
				
TikTok	Telegram	Discord	Reddit	Roblox
Extremist content in edits & memes	Enables encrypted 'Terrorgram' chat channels	Private servers sharing manifestos, propaganda	Extremist subreddits, anonymous 'alt' accounts	Extremist usernames, 3D worlds, private chats

⁶ [United States Government Accountability Office, Countering Violent Extremism \(January 2024\)](#)

References

[The George Washington Program on Extremism, *The Third Generation of Online Radicalization* \(n.d.\)](#)

[European Commission, *Extremists' Use of Gaming \(Adjacent\) Platforms* \(2021\)](#)

[United Nations Office of Counter-Terrorism, *Examining the Intersection Between Gaming and Violent Extremism* \(n.d.\)](#)

[ISD Global, *Young Guns: Understanding a New Generation of Extremism Radicalization in the United States* \(2023\)](#)

EXTREMIST SUBCULTURES & COMMUNITIES

Subcultures tied to extremist ideologies often reward harmful worldviews, offer identity, and provide group validation—particularly for individuals who feel isolated, angry, or disillusioned. These communities operate across both mainstream and fringe platforms and use shared language, memes, and symbology to normalize violence and radical beliefs. Many of these groups overlap in ideology and aesthetics, making it critical to evaluate behavior in context. Subcultural immersion is often gradual and may begin with passive consumption before progressing to glorification or mobilization.

Common subcultures relevant to digital threat assessments include:

Subculture	Description
TCC (True Crime Community)	Fan pages for previous mass attacks. “Edits” often framed as aesthetic or empathetic but serve to glorify the violent acts and encourage others.
Incel ideology	Incel is short for involuntary celibate. Often appears in TikTok duets, Discord threads, and Reddit. Language includes black pill, rope, Stacy, Chad.
Accelerationism	Shared content may include references to societal collapse, eco-fascism, and strategic violence.
764	A numerically coded community referencing a network of fringe users, who glorify mass shooters and promote stochastic terrorism. Known for nihilism, edgy aesthetics, and overlaps with TCC and incel content.
RMVE (Racially Motivated Violent Extremism)	Includes white supremacist, neo-Nazi, and “great replacement” rhetoric. Often spread through manifestos, coded memes, Telegram channels, and targeted propaganda on mainstream platforms.

References

[ADL, *Research and Analysis* \(n.d.\)](#)

[MDPI, *Involuntary Celibacy \(Incel\) Identity: A Thematic Analysis of an Online Community’s Beliefs and Emotional Experiences* \(February 2025\)](#)

[The George Washington Program on Extremism, *Domestic Extremism* \(n.d.\)](#)

[ISD Global, *ISD Explainers* \(n.d.\)](#)

SYMBOLISM, MEMES & CODED LANGUAGE

Radicalized individuals frequently use memes, slang, and coded visuals to express beliefs or communicate within online networks. Symbols, numeric codes, usernames, and image-based humor are often used to normalize violence and bypass moderation. These tactics are intentionally designed to appear harmless, ironic, or ambiguous—giving individuals plausible deniability while reinforcing shared ideologies. Many symbols and phrases evolve rapidly and are recycled through niche communities, making constant monitoring and contextual review essential.

Common Symbols and References	Description
Pepe the Frog	Originally a benign meme, now often remixed to support extremist content or hateful messaging.
Rope	Common in incel communities, often implying suicide or violence.
“Pill” terminology (Redpill, Blackpill, etc.)	Originating from the Matrix metaphor, these terms are used to describe an ideological awakening or rejection of mainstream values. In extremist contexts, they represent fatalism (blackpill), misogynistic beliefs (redpill), or political radicalization (various color variants). They are heavily used in incel, alt-right, and conspiracy communities to signal worldview and reinforce in-group identity.
Soyjack	A meme character based on Wojak, shown with a bearded face and open mouth in exaggerated enthusiasm. Used to mock “feminized” or progressive men and often contrasted with “Chad” in far-right or incel-aligned meme culture. Frequently used in layered memes to ridicule emotional expression, liberal values, or perceived weakness.

Examples





References

[ADL, *Hate on Display™ Hate Symbols Database* \(n.d.\)](#)

[SPLC, *Resources* \(n.d.\)](#)

[ISD Global, *Memes & the Extreme Right-Wing* \(2022\)](#)

[Moonshot, *News and Resources* \(n.d.\)](#)

[National Counterterrorism Center, *Use of Memes by Violent Extremists* \(July 2022\)](#)

[NPR, *How Extremists Weaponize Irony to Spread Hate* \(April 2021\)](#)

GLOSSARY OF KEY TERMS

Digital language used in radical spaces can be intentionally vague or misleading. It supports accurate interpretation of digital content by clarifying common extremist references, euphemisms, and terminology encountered in online threat investigations.

Key Term	Definition
14	Refers to the “14 Words,” a white supremacist slogan: “We must secure the existence of our people and a future for white children.”
88	A white supremacist code for “Heil Hitler,” referencing the 8th letter of the alphabet (H), used to express allegiance to Nazi ideology.
109/110	Antisemitic codes referencing a conspiracy that Jews have been expelled from 109 (or 110) countries throughout history, used to justify bigotry and violence.
1488	Combination of two white supremacist codes: “14 Words” and “Heil Hitler.”
Based	Praised for being politically incorrect, unfiltered, or extreme.
Black sun (Sonnenrad)	Frequently used in accelerationist and white nationalist iconography.
Boogaloo	Reference to a second civil war, often used by anti-government or militia groups.
Chad/Stacy	Incel slang for attractive, socially successful men/women.
ER	Elliot Rodger, mass attacker idolized in incel spaces; often referenced in usernames or tribute posts.
Fed/Glowie	Slang for an undercover federal agent or informant, often used in far-right chats.
Gamification	Describing violent acts using video game terminology (e.g., “high score,” “loadout”).
Groyper	Far-right cartoon frog character; symbol of alt-right youth.
IRL	“In real life”; used to contrast digital behavior with offline action.
KHHV	“Kissless, hugless, handholdless virgin”; used in incel discourse to measure perceived social failure.
Normie	Dismissive term for people perceived as socially average or mainstream.
NPC	Meme implying others are mindless or lack independent thought; used to dehumanize.

Sigma male	Internet archetype idealizing emotionally detached, self-reliant men; can overlap with incel content.
Siege	Reference to the neo-Nazi text “Siege” by James Mason; encourages lone-actor terrorism
Totenkopf (SS skull)	A historic Nazi emblem co-opted by modern violent extremists.
Terrorgram	Nickname for Telegram-based extremist channels distributing manifestos, guides, and propaganda.
Waffen-SS (bolts)	Common in neo-Nazi accelerationist and RMVE communities.
ZOG	“Zionist Occupied Government,” an antisemitic conspiracy term suggesting global Jewish control.




In addition to resources such as the [ADL and SPLC](#), [Urban Dictionary](#), [Reddit](#), and even [4Chan](#) can be powerful for tools for understanding context in communications.

PLATFORM SPOTLIGHTS

Digital threat indicators vary by platform. It provides practical strategies for identifying red flags and contextual behaviors unique to each platform used by youth and subjects of concern.

Note that additional operational security measures should be in place before visiting these platforms. Visit these websites at your own discretion.

Note: Analysis of [TikTok](#), [Telegram](#), [Discord](#), [Reddit](#), and gaming platforms is covered in other SST modules.

Platform	Description
<p>4chan / Other 'Chan' Boards</p> 	<p>4chan and its offshoots (e.g., 8kun) are anonymous imageboards where extremist content can thrive with little moderation. Imageboards such as /pol/ (politically incorrect) frequently use extremist rhetoric and shooter manifestos. Look for image-based memes, racial slurs, numeric codes, and explicit references to prior mass casualty events.</p>
<p>8kun</p> 	<p>A successor to 8chan, 8kun is a highly fringe anonymous imageboard often used to host manifestos, extremist propaganda, and shooter tributes. It has historical ties to violent events and is frequently cited by attackers in pre- or post-incident content. Boards are minimally moderated, and references to past violence. Similar to 4chan, look for image-based memes, racial slurs, numeric codes, and explicit references to prior mass casualty events.</p>
<p>Kiwifarms</p> 	<p>A forum known for doxing, harassment campaigns, and extremist rhetoric. It has been linked to several real-world attacks and suicides. Posts often involve stalking behavior, ideological purity tests, or detailed “exposés” targeting individuals with fringe conspiracy overlays. Users typically hide behind the guise of internet transparency or anti-censorship.</p>

Gab

A fringe alternative to Twitter with a large presence of white nationalist and Christian nationalist users. Gab posts have been observed containing uncensored manifestos, calls for violence, and racially motivated violent extremism. Accounts often mimic official-looking usernames or news sources to spread propaganda. Search activity by name, hashtags, or quotes shared from banned influencers.

Discord

Private servers allow like-minded users to share radical ideology with little oversight. Look for encrypted chat groups, manifesto archives, shooter tribute channels, or shared tactical resources. Invite-only servers may be used to groom and isolate individuals under the guise of community.

Rumble

A video-sharing platform used by deplatformed individuals and fringe influencers. While it includes benign content, it is also a haven for conspiracy theories, anti-government messaging, and white nationalist narratives. Videos may glorify violence, summarize manifestos, or feature ideological recruitment.

Odysee

A decentralized blockchain-based video platform often used to circumvent mainstream moderation policies. It hosts ideological content including RMVE narratives, accelerationist propaganda, and fringe conspiracy media. Often framed as “free speech” content but includes high volumes of unmoderated extremist material.

References

[*Institute for Strategic Design, Researching the Evolving Online Ecosystem: Telegram, Discord and Odysee \(n.d.\)*](#)

[*Australian Government, Trends & Issues in Crime and Criminal Justice \(December 2024\)*](#)

[*Trends Research & Advisory, From Fringe to American Mainstream: The Rise of Far-Right Extremism in the 21st Century \(August 2024\)*](#)

[*Politico, Fringe Social Media Networks Sidestep Online Content Rules \(January 2022\)*](#)

4CHAN UPDATE – APRIL 2025

Incident Summary

Update: As of mid-May 2025, 4chan is back online and operational following the April cyberattack that temporarily took the site offline.

On April 14, 2025, 4chan was the target of a cyberattack that forced the site offline. The site reappeared featuring a previously banned board (soyjack.party) and the message “U GOT HACKED” at the top of the page. Hackers reportedly had access to 4chan’s systems and internal data for over a year before launching the attack that included doxxing many of 4chan’s moderators.

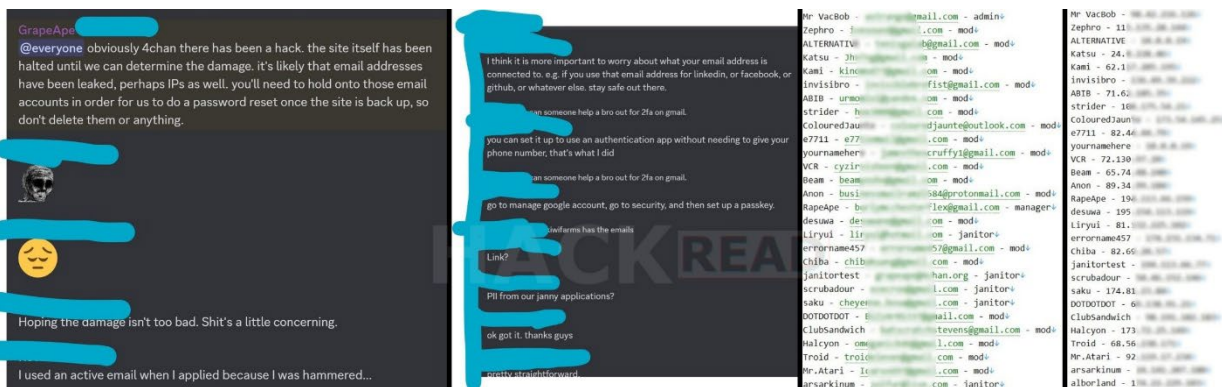
Current Status

As of late April 2025, 4chan remains inaccessible. In the aftermath of the cyberattack, 4chan moderators took all servers offline to prevent further damage. Due to the site’s long-term outage, several online commentators have speculated that the site will be down permanently citing the damage to the site’s infrastructure and reputation.

Although 4chan is down, archived repositories of the site exist for research and evidentiary purposes. As of this writing, the following tools are still able to search and access previously posted content on 4chan:

- <https://4search.neocities.org/>
- <https://4chansearch.org/>
- <https://4chansearch.com/>

Overall, the fall of 4chan – even if temporary – is a significant development in the landscape of online extremism. School safety professionals should treat it not as an end point, but as a shift in terrain, as extremist actors are expected to adapt to new forums. By staying informed about such disruptions, safety teams can better anticipate where the next hotspots for radical content may emerge and adjust their digital threat assessment strategies accordingly.



The screenshot shows chat from 4chan’s Discord server, email addresses, usernames and IP addresses (Image credit: Hackread.com)

MYTHS VS. FACTS

Myth: Girls aren't involved in this content

Fact: Girls often participate in this subculture and have assisted with and/or committed mass attacks in relation to this content.

Example: In December 2024, 15-year-old girl carried out a targeted attack at Abundant Life Christian School in Madison, Wisconsin. Investigators found she had expressed admiration for prior mass shooters and engaged with TCC spaces online. Her digital history revealed aesthetic shooter edits, usernames referencing past attackers, and glorification content consistent with prior incidents.

Myth: They're just being edgy or joking

Fact: "Joking" is often used to disguise the introduction to ideology

Example: The earliest digital footprint associated with the Christchurch shooter (2019) was their posting of racist memes on 4chan, before eventually publishing a manifesto and carrying out a mass shooting.

Myth: If it's not a direct threat, it's not actionable

Fact: Leakage and glorification are critical early indicators.

Example: The Buffalo shooter (2022) left behind a digital trail of glorification, Discord logs, and manifesto content, none of which were reported prior to the attack. His behavior included references to past shooters and ideologically motivated language.

Myth: Extremist behavior is always tied to a specific group or movement

Fact: Many youth adopt extremist behaviors or symbols without formally affiliating with any group. Online radicalization often occurs in decentralized or ideology-blended spaces.

Example: The shooter in Uvalde, Texas (2022), had no known ties to any organized group but displayed fixation on prior mass shooters, conducted weapon research online, and exhibited behavioral leakages consistent with mobilization.

IDENTIFYING AND REPORTING RADICALIZATION

Educators and school staff are often the first to observe shifts in student's behaviors that may be indicative of radicalization. While not expected to be investigators, teachers and staff play a crucial role in recognizing patterns and documenting concerns of potential radicalization.

Signs to Watch For

- Has the student expressed perceived injustices or grievances?
- Are there shifts in baseline behavior or ideology?
- Do they glorify violence or mass shooters?
- Are they used coded language or extremist slang in communications, both on and offline?
- Have they made comments reflective of a need for revenge or a sense of hopelessness?

Practical Steps for Educators

- Document patterns – save concerning usernames, memes, artwork, etc and report to safety teams.
- Identify emerging themes – Note repeated references to violence or extremist rhetoric.
- Ask neutral, open-ended questions – “what does this mean to you?” encourages discussion without accusation.
- Treat “jokes” serious – extremist recruitment tactics rely on the use of irony and jokes to spread the ideologies.
- Refer immediately – report concerns immediately. Information can only be acted on if it has been reported.

ADDITIONAL RESOURCES

- [*American Public University: What Are the 4 Stages of Radicalization? Why Extremists Act.*](#)
- [*National Coordinator for Counterterrorism and Security \(Ministry of Justice and Security\): Far right memes: undermining and far from recognizable.*](#)



SAFER
SCHOOLS
TOGETHER

