Cyber Narrative Guides

Generously funded by Craig Newmark Philanthropies

MAY 2026

GEENA DAVIS INSTITUTE

For over two decades, the Geena Davis Institute has been working to reduce negative stereotypes and unconscious bias in entertainment and media.

GDI's mission is to break barriers, challenge norms, and bridge gaps in representation, and disproportionate cyber risks create additional obstacles to full participation, leadership, and opportunity for women, girls, and other marginalized communities. We believe that thoughtful storytelling about cyber risks can help build safer digital spaces for everyone.

The guides below give screenwriters and producers practical tools for depicting four cyber threats that disproportionately affect these communities — with pitfalls to avoid, recommendations for responsible storytelling, and examples of what getting it right looks like on screen.

DMP / E+ via Getty Images

Phishing

What It Is

Phishing is an online, fraudulent practice in which attackers trick people into revealing sensitive information or installing malicious software.[1]

Why It Matters to Your Audience

Phishing scams are one of the most common cyber crimes people experience. About 39% of those who have experienced a cyberattack or digital scam attempt say they were subject to phishing.[2]

Accurate on-screen portrayals of phishing can help audiences recognize real threats, reduce stigma around being targeted, and understand that anyone can be vulnerable. When stories show how cyberattacks actually unfold, they empower viewers to spot red flags in their own lives while still moving the plot forward.

Pitfalls to Avoid

- **Overly obvious scams:** Emails full of obvious typos, flashing warnings, cartoonishly evil hackers, or outdated scam stereotypes — like a prince promising millions in exchange for temporary financial help — don't reflect how modern phishing works or how believable scams can be.
- **The "careless victim" stereotype:** Depicting most victims of phishing scams as gullible, lazy, or incompetent reinforces stigma around being a victim and misses the reality that scams are often sophisticated and emotionally manipulative. They can happen to anyone.

DO THIS INSTEAD:

- **Use everyday contexts:** Real phishing scams that hit close to home (e.g., package delivery notices, social media recovery emails, or work emails) create a sense of relatability.
- **Show phishing as calculated manipulation, not stupidity:** Focus on the use of urgency, fear, authority, or trust to trick victims into revealing personal information.
- **Normalize characters asking for help:** Show victims of phishing scams reporting an issue back to a company or workplace, sharing warnings with coworkers, and asking help from family. Reporting scams is the best way to help protect others from becoming victims as well.
- **Present new sophisticated uses of scams**: AI can be used to mimic an image, voice, or likeness of someone you care about. Spreading awareness of these emerging trends helps spread awareness of what to look out for.

On-screen Examples

- The TV series *Mr. Robot* (USA Network, 2015–2019) depicts phishing and social engineering as deliberate, methodical attack vectors rather than one-off tricks. The show is widely praised by cybersecurity professionals for its technical accuracy.[3] In *Mr. Robot,* phishing appears not as a punchline but as a calculated first step in a larger intrusion chain, reflecting how real-world attackers operate.
- Episode 18 of *StuGo*, "Phishin' Chip" (Disney Channel, 2025), illustrates how children can fall victim to email scams through the lure of something free (in this case, clicking a link for a free gift card). An adult character reminds the young characters to pause: "Hover and think before clicking that link."

Resources for Further Guidance

- Take9, funded by Craig Newmark Philanthropies, is a public service cybersecurity campaign that encourages people to pause and think before they click, download, or share. A 9-second pause allows people to slow down, verify the sender, and look for "phishy" clues that can help them stay safe online and avoid scams.
- Check out this free GDI webinar with experts from Aspen Digital for top insights and tips about phishing: "Take 9 Seconds, Take Control: Practical Guidance for Smarter Cyber Decisions."
- For guidance on portraying best practices for a character who has been scammed, see the Better Business Bureau's "Scam Survival Kit."
- The Cyber Education Alliance is a group of organizations, including GDI, that have come together to provide resources designed to enhance cybersecurity awareness and knowledge for students across K–12 education. Check out their resources here: www.getcybersmart.org/get-started

PonyWang / E+ via Getty Images

Deepfakes

What It Is

A deepfake is an artificial image, video, or voice cloning of a real person generated through machine learning.

Why It Matters to Your Audience

As synthetic audio and video become easier to create and harder to detect, audiences are increasingly vulnerable to misinformation and disinformation, fraud, harassment, and reputational harm. Thoughtful portrayals help viewers understand that deepfakes can affect everyday people, relationships, and institutions, not just celebrities. Accurate storytelling can help build media literacy.

Pitfalls to Avoid

- **"You can always tell":** Obvious visual glitches, robotic voices, or extra fingers and exaggerated facial errors — termed "cheap fakes" in the cybersecurity field — no longer reflect reality, and modern generative AI has made deepfakes harder to identify. While these "cheap fakes" are a small part of the deepfake ecosystem, highlighting them instead of more realistic deepfakes may give audiences false confidence.
- **Portraying experiencing harm from generative AI as inevitable:** Deepfakes are often framed as an unstoppable technology rather than tools, where a bad actor (or company) is responsible for its misuse. De-emphasizing the human element behind the generation and dissemination of deepfakes can disincentivize the need to develop digital media literacy skills.
- **Immediate universal belief:** Not everyone instantly believes or disbelieves a deepfake. Uncertainty, conversation, and debate are more realistic, and they are important habits to promote.

DO THIS INSTEAD:

- **Depicting the myth of competence:** Despite many people being confident they can correctly identify deepfakes, our ability to do so is often a lot worse than we think, especially as generative AI becomes more sophisticated and hyperrealistic. Pointing audiences to this fact may help them be more suspicious of potential deepfake content.
- **Center the human stakes:** Focus on how deepfakes affect trust, relationships, careers, information integrity, and safety. Deepfakes can produce a lasting emotional toll on victims and challenge shared concepts of reality that are foundational to our media environment.
- **Depict realistic motivations:** Deepfakes are commonly used for harassment, financial scams, political manipulation, entertainment, or personal revenge. A common rising scam leverages deepfake voice technology to produce a call from someone pretending to be a child who is kidnapped or otherwise mimicking loved ones. One solution is modeling how families can create a private "code word" to make sure it is actually them in a crisis.

On-screen Examples

- In the film *Thelma* (2024), 93-year-old Thelma (June Squibb) is victim of a deepfake scam that mimics her grandson's voice and asks her to send $10k ransom money to have him released. The movie is based on real events.[4] Thelma confides in her family to tell them what happened, then seeks justice on her own.
- The "Joan Is Awful" episode of *Black Mirror* (Netflix, 2023) explores the dangers of personal data collection and digital likeness. The main character, Joan, discovers that a streaming service is broadcasting a TV show that recreates her life. The show is produced using real-time data collected from her devices and AI-generated versions of real actors, allowing the service to broadcast personal events from her life almost as they happen.

Resources for Storytelling Guidance

- The National Cybersecurity Alliance's resource "How To Protect Yourself Against Deepfakes" provides tips to reduce your risk of becoming a victim of deepfake-related scams and misinformation.
- Read AARP's guide on how AI-powered scams make fraud harder to spot "AI makes it next to impossible to detect scams. Now what?"
- Review the Global Investigative Journalism Network's brief "How to identify and investigate AI audio deepfakes."

Catherine Falls Commercial / Moment via Getty Images

Nonconsensual Intimate Imagery (NCII)

What It Is

Nonconsensual intimate imagery (also referred to as "revenge porn," though survivors, experts, and advocates discourage using this term) is a form of sexual abuse that disproportionately targets women, LGBTQIA+ people, and young people. It can include nonconsensual sharing of real intimate photos and videos or the creation of sexually explicit deepfake content using AI tools without the consent of the person depicted.

Why It Matters to Your Audience

The impact of nonconsensual intimate imagery can be long-lasting, including emotional trauma, career damage, harassment, and loss of safety. Media portrayals shape how audiences understand consent, blame, and accountability. Like other forms of sexual violence, NCII is vastly underreported but widespread: In the past year alone, an estimated 1 in 10 American women experienced some form of technology-facilitated sexual violence, according to the Centers for Disease Control and Prevention, and more than 2.3 million women have had their intimate images shared without their consent.[5] Responsible storytelling can reduce victim-blaming and help audiences recognize this as a serious cyber threat and crime.

Pitfalls to Avoid

- **Framing it as drama or gossip:** Treating the spread of NCII as a "leak" and a juicy plot twist, rather than an act of sexual exploitation and abuse, minimizes the harm.

- **Victim-blaming narratives:** Avoid portraying victims as naive or reckless — regardless of whether the image or video was initially shared consensually. Victim-blaming narratives say someone shouldn't have taken intimate photos in the first place, which puts the onus on the victim, not the perpetrator. Additionally, apps can take a photo of a real, clothed person and convert the image into a nude one, as well as generate fake nude images by imposing someone's likeness onto a naked body. The apps can also generate deepfake videos depicting people engaging in sexual acts without their consent of a person and are often used to harass women. This means someone could never take an intimate image and still become a victim of these predatory tools. Regardless of whether NCII is real or synthetic, all victims deserve to be treated with dignity and respect, not blame.
- **Oversexualized visuals:** Repeated playback of the nonconsensual images, sexualizing them, or aestheticizing them shifts focus away from the impacts to the victim and instead treats the harm as a spectacle. Showing the explicit imagery on screen sensationalizes the content at the expense of the person it was used to hurt, and it fails to tell a needed story about accountability.

DO THIS INSTEAD:

- **Name the harm clearly and accurately:** In the U.S. and globally, the sharing of nonconsensual intimate images of adults is not only harmful, it is also a crime — and sexual imagery of minors is always illegal.[67] For storytelling involving adults, use the term "nonconsensual intimate imagery," or emphasize language like "shared without consent" or "sexual exploitation," not euphemisms that soften accountability or blame the victim (like "revenge porn"). For storytelling involving sexually explicit content of those under 18 (e.g., sharing nonconsensual content or images that a teenager expected their dating partner to keep private), use the term "image-based sexual abuse" or employ language like "online sexual exploitation."
- **Center the survivor's experience, and avoid storylines that prioritize the perpetrator's intent over the harm caused to victims:** Focus on health, safety, and emotional consequences rather than public shame or embarrassment. Model consent language that illustrates how agreeing to share intimate imagery with one person does not mean the victim consented to public exposure of those images, and such language avoids storylines that focus heavily on motivation or intent of the perpetrator as a general rule. Given the real, devastating consequences of NCII, legal experts, survivors, and advocates advise against legislation that requires an intent to cause harm as the basis for defining the offense.[8] Media that shifts the emphasis away from how NCII impacts victims and survivors by overemphasizing the perpetrator's intent can perpetuate bad policies.
- **Show realistic barriers to justice:** Survivors may face disbelief, jurisdiction issues, slow platform responses, or pressure to stay quiet.
- **Depict positive interventions among peer groups:** Often, nonconsensual images are shared as a form of perverse bonding among men. Show men (or boys) within such peer groups speaking out against these activities when their friends engage in them, to model allyship and responsible behavior.

On-screen Examples

- The series *I May Destroy You* (HBO, 2020), has been praised for its treatment of this issue and others related to sexual abuse online and offline.
- Content creators can look to the true-crime docuseries *The Most Hated Man on the Internet* (Netflix, 2022) for modeling. It centers the victims and practical responses, such as reporting, legal action, and advocacy.
- The 2025 Netflix drama *Adolescence* offers a chilling portrayal of how normalized image-based sexual abuse has become among adolescents. When a 13-year-old girl's intimate photo is widely shared among classmates without her consent, the story reveals how online misogyny often intersects with offline forms of gender-based violence, conveyed without ever showing the image on screen.

Resources for Storytelling Guidance

- Read U.N. Women's article on AI-powered online abuse: "How AI is amplifying violence against women and what can stop it."
- Read the Cyber Civil Rights Initiative's "Guide for Media" on reporting about NCII.
- See the recommendations for responsible NCII-related storytelling in "Model National Framework on Adult Image-Based Sexual Abuse," from StopNCII.org, U.N. Women, and the U.N. Office on Drugs and Crime.
- Ensure that storytelling about NCII and image-based sexual abuse includes clear signposts to resources for people to get help, including:
    - National Image Abuse Helpline and Safety Center, a free and confidential 24/7 service operated by the Cyber Civil Rights Initiative: 1-844-878-2274.
    - StopNCII.org has a free tool that creates a digital fingerprint (hash) of the image so it can be blocked from sharing on participating platforms without sharing the actual image.
    - TakeItDown.NCMEC.org uses the same hash-matching technology as StopNCII.org, and is a service specifically for those under 18.

ATHVisions / E+ via Getty Images

Cybersecurity Careers

Cybersecurity is one of the fastest-growing and most influential fields, yet women and people from racial and ethnic minority groups remain significantly underrepresented in the workforce. Today, only about 1 in 4 members of the global cybersecurity workforce are women, highlighting a persistent gender gap in the field.[9]

Research also shows that representation and awareness can influence career interest. One study found that the more girls learn about cybersecurity and the realities of working in the sector, the more interested they become in pursuing careers in the field.[10] Media portrayals play a powerful role in shaping that awareness by influencing who audiences imagine belongs in technical and cybersecurity roles.

When viewers repeatedly see cybersecurity experts depicted through narrow archetypes — often white, male, socially isolated, or genius stereotypes — it can unintentionally signal that others do not belong in these careers. Authentic and diverse portrayals can expand public understanding of who works in cybersecurity, inspire interest in STEM and digital safety careers, and reflect the collaborative, multidisciplinary reality of the field. It can also support women already working in the field, because seeing people like themselves represented on screen can encourage them to remain in the profession. Representation helps audiences see these roles as accessible, varied, and socially impactful.

Pitfalls to Avoid

- **The "lone hacker genius" stereotype:** Portraying cybersecurity professionals as isolated prodigies working alone misrepresents how the field actually operates, which relies heavily on teamwork, communication, and diverse expertise.

- **Narrow casting patterns:** Repeatedly showing cybersecurity experts as white, male, and young reinforces existing workforce disparities and limits audience perception of who can succeed in the field.
- **Overemphasis on technical jargon:** Presenting cybersecurity as incomprehensible or inaccessible may discourage audiences from imagining themselves in the field. In fact, misconceptions that cybersecurity is "too technical" may deter young girls from cybersecurity careers.[11]

DO THIS INSTEAD:

- **Show cybersecurity as collaborative:** Highlight team dynamics, shared problem-solving, and interdisciplinary perspectives. This reflects reality and creates space for multiple types of expertise and personalities, and may draw in young women interested in STEM.
- **Portray leadership diversity:** Show women and racially diverse professionals as decision-makers, senior analysts, founders, educators, or crisis leaders.
- **Highlight multiple entry paths:** Characters may come from military service, self-teaching, community college programs, career pivots, or policy and communications backgrounds. Many people enter the field because they became interested through middle and high school programs. Depicting girls going to hackathons, doing STEM projects together, etc., can encourage young people to seek these opportunities in the real world.

On-screen Cybersecurity Experts We Love

- Lisbeth Salander in *The Girl with the Dragon Tattoo* (2011) & *The Girl in the Spider's Web* (2018)
- Shuri in *The Black Panther* (2018) & *Black Panther: Wakanda Forever* (2022)
- Penelope Garcia on *Criminal Minds* (2005–present)
- Abby Sciuto on *NCIS* (2003–present)
- Darlene Alderson on *Mr. Robot* (2015–2019)
- Dr. Avery Ryan, Brody Nelson, and Raven Ramirez on *CSI: Cyber* (2015–2016)
- Cindy "Mac" Mackenzie in *Veronica Mars* (2004–2019)
- Root/Samantha Groves in *Person of Interest* (2011–2016)

Resources for Storytelling Guidance

- In "Portray Her 2.0: An Analysis of 15 Years of Women in STEM On-Screen, 2007–2022," GDI discusses the nuanced shifts and enduring barriers in female STEM representation, and provides recommendations to inspire future change.
- To assist in storytelling to address the gender gap in cybersecurity professionals, this research from Girls Who Code offers data-driven insights into girls' awareness of cybersecurity, their attitudes toward the field, and the conditions that could support them in pursuing it as a career: "Breaking Barriers: Girls and the Future of Cybersecurity."
- Visit getcybersmart.org to explore resources that describe a variety of roles in cybersecurity, along with the diverse types of expertise and personality traits that are valuable across different cybersecurity paths. Resources featured:
  - CYBER.ORG Career Exploration
  - WiCyS's Pathways in Cyber
  - WISP Careers in Security & Privacy

ENDNOTES

1. Craig Newmark Philanthropies. (n.d.). *Take9*. https://pausetake9.org/

2. Aspen Digital, Consumer Reports, & Global Cyber Alliance. (2025). *2025 consumer cyber readiness report*. https://www.aspendigital.org/wp-content/uploads/2025/09/Aspen-Digital_2025-Consumer-Cyber-Readiness-Report.pdf

3. Syracuse University. (n.d.). *Inside Mr. Robot: Technical advisor discusses the show's realism and cybersecurity*. https://onlinegrad.syracuse.edu/blog/mr-robot-cybersecurity-expert/

4. Contino, G. (2024, July 5). *The voice scam call portrayed in "Thelma" is real—and a growing threat in the age of AI*. CNBC. https://www.cnbc.com/2024/07/05/ai-voice-scam-call-movie-thelma-growing-threat.html

5. Centers for Disease Control and Prevention. (2024). *The National Intimate Partner and Sexual Violence Survey (NISVS): 2023–2024 sexual violence data brief*. https://www.cdc.gov/nisvs/media/pdfs/sexualviolence-brief.pdf

6. Rape, Abuse & Incest National Network. (n.d.). *Take It Down Act*. https://rainn.org/federal-legislation/take-it-down-act/

7. United Nations Office on Drugs and Crime. (n.d.). *United Nations convention against cybercrime: Full text*. https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html#art16

8. End Violence Against Women Coalition. (2025, January 27). *Government U-turn on deepfakes offence*. https://www.endviolenceagainstwomen.org.uk/government-u-turn-on-deepfakes-offence/

9. ISC2. (2024, April 25). *Women in cybersecurity: Inclusion, advancement and pay equity are keys to attracting and retaining more women*. https://www.isc2.org/insights/2024/04/women-in-cybersecurity-report-inclusion-advancement-pay-equity

10. Girls Who Code. (2025). *Breaking barriers: Girls and the future of cybersecurity*. https://girlswhocode.com/assets/downloads/craft-prod/downloads/GWC_CyberResearchReport_final.pdf

11. Girls Who Code. (2025). *Breaking barriers: Girls and the future of cybersecurity*. https://girlswhocode.com/assets/downloads/craft-prod/downloads/GWC_CyberResearchReport_final.pdf

Would you like us to connect you with an expert to help with these storylines? Get in touch here.

Acknowledgements

The authors would like to thank Sharlene Chiu (marketing consultant at Girls Who Code), Cailin Crockett (independent expert and consultant at StopNCII.org and Cyber Civil Rights Initiative), Amira Dhalla (director of cyber civil defense at Aspen Digital) and Talia Stringfellow (senior associate for Take9 at Aspen Digital) for their thoughtful feedback and insightful comments. We would also like to thank Getty Images for the images featured in this report.

About the Geena Davis Institute

Since 2004, the Geena Davis Institute has worked to mitigate unconscious bias while creating equality, fostering inclusion and reducing negative stereotyping in entertainment and media. As a global research-based organization, the Institute provides research, direct guidance and thought leadership aimed at increasing representation of marginalized groups within six identities: gender, race/ethnicity, LGBTQIA+, disability, age, and body type. Because of its unique history and position, the Institute can help achieve true onscreen equity in a way that few organizations can. Learn more at geenadavisinstitute.org.

How to cite these narrative guides:

Conroy, M., Perez, R., and Urban, D. (2026). “Cyber Narrative Guides.” Geena Davis Institute.