For older children and teenagers (middle school and high school):

* Understanding and preventing phishing and social engineering:
  + Recognizing and handling suspicious emails and texts.
  + Being aware of sophisticated phishing tactics that use deepfake technology.
  + Learning to spot malicious QR codes.
* <https://gatefy.com/blog/real-and-famous-cases-social-engineering-attacks/>
* Deepfake technology:
  + Understanding what deepfakes are and how they can be used for deception.
  + Scrutinizing online content before sharing.
* <https://thehill.com/homenews/education/4760128-pennsylvania-middle-schoolers-create-fake-tik-tok-profiles/>
* Cyberbullying:
  + Recognizing the signs of cyberbullying and knowing how to report incidents.
  + Understanding the negative impact of cyberbullying on mental health.
  + Learning about advanced cyberbullying tactics.
* <https://www.nbcnews.com/news/us-news/new-jersey-family-sue-school-district-after-12-year-old-n788506>
* Data privacy:
  + Understanding privacy settings and app permissions.
  + Being mindful of the personal information shared online.
  + Learning about data breaches and their consequences.
* Safe social media usage:
  + Setting privacy controls on social media accounts.
  + Not sharing excessive personal information online.
* Password security:
  + Creating strong passwords and avoiding reusing them across different accounts.
  + Using multi-factor authentication.
* Ransomware and malware:
  + Understanding the threat of ransomware attacks, particularly on educational institutions.
  + Learning how to prevent malware downloads.
* Responsible AI use:
* Understanding the potential risks of AI-driven tools.
* Focusing on AI ethics and data management.