

// E-SAFETY FACT SHEET

Staying Safe on Social Media

Understanding the Risks –
and Building Smart Online Habits
for Students, Teachers, and Parents

Social media is where young people connect, create, and learn — but it is also where they face some of the most common online risks: oversharing personal information, contact from strangers, cyberbullying, scams, misleading content, and pressure that can affect wellbeing. Most of these risks follow recognizable patterns, and recognizing the pattern is the single best defense.

The goal is not to scare young people off social media — it is to help them use it with the same critical thinking a cybersecurity professional would.

This document outlines the main risk areas, offers practical steps for students, parents, and educators, and lists trusted resources for further help.

In this document:

- 01 Know the risks
- 02 What can you do?
- 03 Resources and where to get help

1 Know the risks

A. Oversharing & Your Digital Footprint

Everything posted online — photos, comments, locations, tagged friends — builds a permanent record. Details that seem harmless on their own (a school logo in a photo, a birthday post, a check-in at a local park) can be combined to reveal where a young person lives, studies, and spends time. Deleted posts are not truly gone: screenshots, reposts, and archives mean content can resurface years later, including in front of college admissions officers and employers.

B. Contact from Strangers & Fake Profiles

Not everyone online is who they claim to be. Adults with harmful intentions sometimes pose as peers, building trust over weeks or months before asking for personal information, images, or offline meetings. Common patterns include excessive flattery, requests to move the conversation to a private or encrypted app, requests for secrecy from parents and friends, and gifts or game currency offered "no strings attached." Any request to keep an online friendship secret from trusted adults is a red flag, full stop.

C. Cyberbullying & Harassment

Social media can amplify bullying: it follows young people home, spreads fast, and can feel inescapable because it happens on the same device they use for everything else. It may take the form of cruel comments, exclusion from group chats, sharing embarrassing content, impersonation accounts, or coordinated pile-ons. Both targets and bystanders play a role — and platforms provide reporting and blocking tools that genuinely work when used.

D. Scams, Phishing & Account Takeovers

Young people are targeted by the same social engineering used against adults: fake giveaways, "free" game currency, too-good-to-be-true marketplace deals, and messages that appear to come from friends whose accounts have been hijacked. A single reused password can turn one compromised account into many. Phishing links sent by DM are one of the most common ways accounts are stolen.

E. Misinformation, AI Content & Algorithmic Pressure

Feeds are ranked by engagement, not accuracy. Viral content is often misleading, and generative AI now makes fake images, videos, and voices cheap to produce and hard to spot. Recommendation algorithms can also pull young users toward increasingly extreme or harmful content, and the constant comparison culture of curated highlight reels can affect self-esteem, sleep, and mental wellbeing.

2 What can **you** do?

For students: lock down, think first.

- ▶ Set accounts to private and review your follower list — if you wouldn't talk to them in person, they don't need access to your life.
- ▶ Turn off location sharing in posts and app permissions. Never post your school, address, or daily routine.
- ▶ Use a unique, strong password for every account and turn on two-factor authentication (2FA). This one habit stops most account takeovers.
- ▶ Apply the "billboard test" before posting: would you be comfortable seeing it on a billboard with your name on it, forever?
- ▶ Don't click links sent by DM — even from friends — without verifying. "Is this you in this video?" is a classic account-stealing lure.
- ▶ If a stranger (or anyone) asks you to keep your chats secret, asks for photos, or pressures you to move to a private app — stop, screenshot, block, and tell a trusted adult. You will not be in trouble for asking for help.

For parents & caregivers: talk early, talk often.

- ▶ Make online life a normal conversation topic, not an interrogation. Kids report problems to adults they don't expect to panic or punish.
- ▶ Set up accounts together. Walk through privacy settings, blocking, and reporting so your child knows how to use them before they need them.
- ▶ Agree family rules on screen time, devices in bedrooms overnight, and which apps are okay — and follow the age minimums platforms set.
- ▶ Watch for changes: secrecy about devices, distress after being online, new "friends" you've never heard of, or withdrawal from offline activities.
- ▶ If something goes wrong, lead with support. A child who fears blame will hide the problem until it grows.

For teachers & schools: build the skills.

- ▶ Teach media literacy as a core skill: how feeds are ranked, how to reverse-check images and claims, and how to spot AI-generated content.
- ▶ Treat e-safety like fire drills — regular, practical, and rehearsed, not a one-off assembly.
- ▶ Make reporting routes visible and low-friction, and respond to cyberbullying reports as seriously as in-person incidents.
- ▶ Frame good security habits (2FA, password hygiene, phishing awareness) as the same skills used in cybersecurity careers — it turns "rules" into capability.

Turn defense into a career skill. The habits above — spotting phishing, verifying sources, protecting accounts — are the exact entry-level skills of the cybersecurity workforce. Explore where they lead at getintocyberjobs.com and practice them with free games at gamingforlearning.com.

3 Resources and where to get help

No one has to handle an online problem alone. These trusted, free resources cover the most common situations:

- ▶ **NCMEC** — the United States's leading non-governmental child protection organization. Sextortion and exploitation information: ncmec.org/sextortion
- ▶ **24-hour hotline** for children and families: 1-800-THE-LOST (1-800-843-5678)
- ▶ **CyberTipline** — report online exploitation of a child; reports are reviewed and routed to the appropriate law enforcement agency: report.cybertip.org
- ▶ **Take It Down** — helps minors anonymously request removal of explicit images of themselves from participating platforms: takeitdown.ncmec.org
- ▶ **StopBullying.gov** — federal guidance on cyberbullying, including how to document, report, and respond: stopbullying.gov
- ▶ **FTC consumer guidance** — recognizing and reporting scams and phishing: consumer.ftc.gov · report at reportfraud.ftc.gov
- ▶ **Common Sense Media** — age ratings, app reviews, and family media agreements: commonsensemedia.org
- ▶ **988 Suicide & Crisis Lifeline** — if online experiences are affecting a young person's mental health, free confidential support is available 24/7: call or text [988](https://988lifeline.org)
- ▶ **In-app tools** — every major platform has block and report functions. Use them early; blocking is not overreacting.

Golden rule for adults: when a young person tells you something went wrong online, the first response that matters most is calm support — not blame, not confiscating the device. Kids who expect punishment stop reporting.

// Warning signs to watch for

- ▶ Sudden secrecy about devices or switching screens when adults approach
- ▶ Distress, anxiety, or anger after being online
- ▶ New online "friends" no one has met, or unexplained gifts and game currency
- ▶ Withdrawal from offline friends, activities, or sleep disruption
- ▶ Unexplained changes in behavior, especially after being online

Changes in teenage behavior can have many causes. Whatever the reason, check in on red flags — and remember to include online activity in the 'check-in' conversations.

getintocyberjobs.com · A free resource for K-12 students and teachers across the US.

This fact sheet is for general educational purposes. If a child is in immediate danger, call 911. For suspected online exploitation of a child, report to the NCMEC CyberTipline at report.cybertip.org.