INTERNET SAFETY & SECURITY TERMS

Chapter 7 Resources

The following list of terms is provided by Mark Wenberg, author of *Cybersecurity Basics*.

clickbait – misleading links or headlines designed to grab attention and trick people into clicking.

cyberbullying – bullying that happens online through messages, social media, gaming platforms, or other digital communication.

digital footprint – the trail of data your child leaves behind when using the internet, including posts, likes, and search history.

encryption – a method of scrambling data so only authorized people can understand it—used in secure messaging.

grooming – when an adult builds a relationship with a child online to gain their trust and exploit them later, often for sexual purposes.

in-app purchases – buying items within apps or games, often with real money, which can happen accidentally if not restricted.

location sharing – a setting that shows where a device is in real time—can be dangerous if shared with strangers.

malware – harmful software that can damage or take control of your device, often installed without your knowledge.

parental controls – features or apps that let you manage what your child can access online and monitor their activity.

phishing – a scam where someone pretends to be a trustworthy source (like a school or company) to trick you into giving personal information.

privacy settings – tools that help control who can see your or your child's information on apps and websites.

reporting/blocking – tools that allow users to report harmful content or people and prevent further contact.

safe browsing mode – a browser setting or tool that helps filter out harmful or inappropriate websites.

screen time – the amount of time someone spends using digital devices like phones, tablets, or computers.

sextortion – a serious crime where someone threatens to share private images of a person unless they send more or meet demands.

social engineering – manipulating someone into giving up confidential information (e.g., tricking kids into revealing passwords or family info).

stranger danger (online) – the risk of children interacting with unknown individuals who may not be who they say they are.

terms of service – the rules you agree to when signing up for apps, games, or websites—often skipped but important.

two-factor authentication (2FA) – an extra layer of login security that requires not just a password, but also a second step (like a code sent by text).

VPN (Virtual Private Network) – a tool that hides your internet activity and location, often used for privacy.