**VOCABULARY BANK FOR ONLINE DANGERS**

* **Phishing**: A type of online scam where fraudsters impersonate legitimate organizations to steal personal information.
* **Scam**: A dishonest scheme or fraud designed to trick people into giving away money or personal details.
* **Spam**: Unsolicited or irrelevant messages, typically sent in bulk, often for advertising purposes.
* **Encryption**: The process of converting information into a code to prevent unauthorized access.
* **Verification**: The process of confirming the authenticity of something (e.g., verifying someone's identity).
* **Malware**: Malicious software designed to damage or gain unauthorized access to a computer system.
* **Scam Website**: A website designed to trick users into providing personal or financial information through fraudulent means.
* **Fake News**: False or misleading information presented as news.
* **Clickbait**: Headlines or content designed to attract attention and generate clicks, often by misleading or exaggerating the truth.
* **Fact-Checking**: The process of verifying the accuracy of information before accepting it as true.
* **Misinformation**: Incorrect or misleading information, regardless of intent to deceive.
* **Fake news**: false information made to look like real news. It is shared online to trick or confuse people.
* **Social Media Addiction**: Excessive or unhealthy use of social media platforms.
* **Cyberbullying**: The use of digital platforms to harass, threaten, or intimidate others.
* **Privacy Settings**: Controls that allow users to manage who can see their content or information on social media platforms.
* **Online Predator:** Someone who uses the internet to trick or harm people, especially young people. They often pretend to be someone else.