Cyber Safety for Families

bb

ITS Information Technology Services | LAUSD UNIFIED

ITS | LAUSD UNIFIED
Information Technology Services

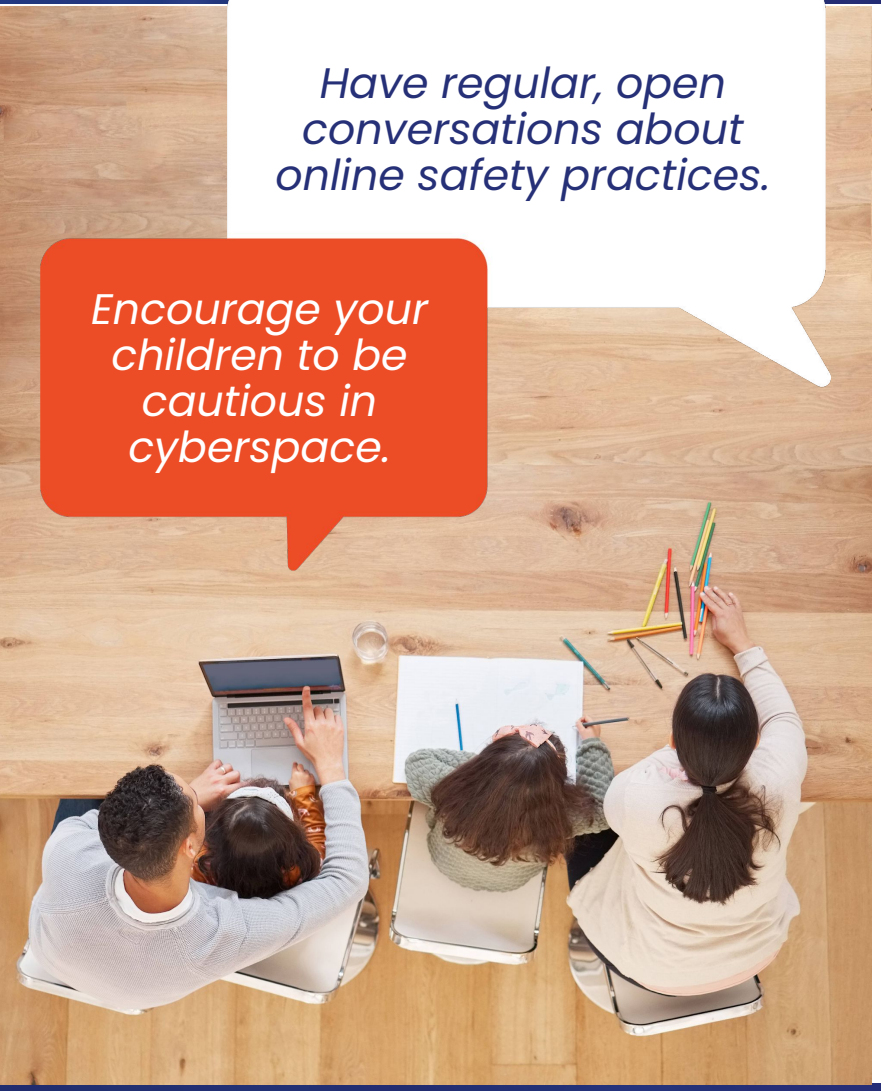
The Importance of Cyber Safety

- **The Internet and cyberspace offer a world of opportunities, such as:**
    - Email, messaging, video chatting, and social media
    - Online research, virtual field trips, and instructional content
    - Videos, gaming, music, and podcasts
    - Online banking and shopping
- **Kids ages 8-12 spend almost 4 hours** and **teens ages 13-18 spend almost 6.5 hours a day online** watching videos, gaming, browsing websites, videochatting, and using social media
- It is therefore essential to learn about and understand **common online dangers to beware of** and **actions you can take to protect your family**

Source: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign; Common Sense Media, "The Common Sense Census: Media Use by Tweens and Teens, 2021".

ITS Information Technology Services | LAUSD UNIFIED

General Tips to Protect Your Children in Cyberspace



- Foster **open, honest communications** to discuss online risks and behaviors
- Have **regular conversations** about online safety practices, **offering guidance** rather than trying to control behavior
- Encourage children to be cautious – remind them **what is on the Internet isn't always true** and **people may not be who they seem to be**
- Talk about the **importance of a positive online identity**
- Watch for **changes in behavior** – sudden avoidance of the computer may be a sign your child is being bullied online
- **Review security settings and privacy policies** for Apps and websites
- **Protect Internet-enabled devices** like smart phones and tablets

Source: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign.

ITS | LAUSD UNIFIED
Information Technology Services

Cyber Predators and Bullies

- **Cyber Predators** look online for children, teens, and sometimes adults to exploit, control, or hurt in some way. They often try to connect through chat rooms, instant messaging, social media, and gaming communities.

- **Cyber Bullies** post mean, hurtful messages or photos about others online or through text messages or email. Common places for cyberbullying are social media, gaming communities, instant/text messaging, and email.

- Nearly **1 of every 2 teens have experienced cyberbullying**

Sources: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign; Pew Research Center, Teens and Cyberbullying 2022.

ITS | LAUSD UNIFIED
Information Technology Services

Cyber Predators and Bullies

Cyber Tips to Share with Your Children

- **Keep your personal information private:** Never share your name, address, phone number, birthday, passwords, or school you attend online.
- **Speak Up:** If you see something inappropriate, tell an adult and let the website know.
- **Don't talk to strangers and never agree to meet in person.** Tell an adult you trust if a stranger contacts you in a chat room or via email or texting.
- **Only communicate online with people you actually know** in person.
- **Think carefully before posting:** Once something is in cyberspace, it's there forever.
- **Practice the Golden Rule:** Treat others the way you want to be treated.

Source: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign.

ITS | LAUSD UNIFIED
Information Technology Services

Phishing and Identity Theft

- **Phishing** is a scam that tries to trick you into providing your personal information or passwords and may also install malware onto your computing system.
- **Identity theft** is when someone steals and uses your personal information to get credit or financial benefits. When this happens, it can damage your credit status and cost time and money to resolve the issues.
- Almost **1 million children were the target of identity theft** (1 in 80) in 2021-2022

Sources: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign; AARP, "Criminals Target Children for Identity Theft and Fraud", 10-31-2022.

ITS | LAUSD UNIFIED
Information Technology Services

Phishing and Identity Theft

Cyber Tips for Families

- **Beware of requests or emails to update or confirm your personal information.** Most organizations (banks, companies, schools, etc.) don't ask for your personal information.
- **Beware of emails offering prizes or things for free**. These are tricks to get your information or get you to click on a link that installs malware or spyware.
- **Use strong passwords** with 8 or more characters including letters, symbols and numbers, and don't share your passwords with anyone.
- **Change your passwords often** and avoid using the same password on multiple sites.
- **Don't open emails from strangers** and don't click on links for unfamiliar sites.
- **Enter web addresses by hand** instead of following links.
- **Use and check your privacy settings** on social media sites.

Source: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign.

ITS | LAUSD UNIFIED
Information Technology Services

Mobile Device Security

- **Mobile device security** is needed for cell phones, tablets, and other portable devices used to play games, video chat, browse the Internet, and more. It helps protect information stored on and transmitted by your device and keeps unauthorized users from accessing your network.
- There are **four main types of threats** to beware of when using a mobile device:
  - **Applications** that steal info from your device after the app is downloaded
  - **Web-based sites** that seem OK but download malicious content when visited
  - **Public Wi-Fi networks** can enable unencrypted data to be stolen while in use
  - **Physical loss or theft of a device** can enable others to access data stored on it

Source: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign.

ITS Information Technology Services | LAUSD UNIFIED

Mobile Device Security

Cyber Tips for Securing Mobile Devices

- **Keep a close watch on your device** and don't leave it unattended.
- **Keep your device locked** when not in use and keep it password protected so others can't access it. Don't share your password.
- **Update your mobile software** including operating system and Apps to improve your device's ability to defend against malware.
- **Know your Apps.** Discuss Apps with your children before they are downloaded and review the settings with them.
- **Only connect to the Internet if needed,** disconnect when done, and make sure devices aren't set to automatically connect to Wi-Fi. Confirm the name of any public Wi-Fi and login procedures to ensure the network is legitimate.
- **Use caution when accessing websites**.

Source: Department of Homeland Security *Stop.Think.Connect.* Cybersecurity Awareness Campaign.