# RAISING DIGITAL CITIZENS

We all know the internet is a fantastic world of learning and entertainment for kids, but, like the real world, there can be dangers, too. With some precautions, you can set your children up to become upstanding digital citizens that will lead the future. On the other hand, giving children uninhibited access to the internet can put your child, computer and personal data at risk.

## Remain positively engaged

Pay attention to the online environments your children use. Surf the web with them. Appreciate your children's participation in their online communities and show interest in their friends. When they encounter inappropriate material, react constructively and make it a teachable moment.

## Keep a clean machine

Cybersecurity starts with protecting all household computers with a security suite, meaning antivirus, antispyware and firewall software. Software companies often send updates that deal with the latest cybersecurity threats, so set your software to update automatically so you don't have to worry about it. Keep your operating system, web browsers and other software current as well. Importantly, back up computer files regularly either on the cloud, on an external hard drive or both.

# Know the protection features of websites, software and apps

All major internet service providers (ISPs) have tools to help you manage your children's online experience. These tools empower you to select approved websites, monitor the amount of time children spend online and limit the people who can contact them. Your ISP might also have other security features, such as pop-up blockers. Third-party tools for limiting children's internet activities are also available. Remember, your home computer isn't the only place they can go online. It is important that your children understand good internet behavior wherever they may access it.

# Review privacy settings

Look at the privacy settings available on social networking platforms, computers, smartphones, apps and other digital tools your children use. Engage your children in these decisions—decide together which settings provide the appropriate amount of protection for each child. Teach critical thinking: help your children identify safe, credible websites and other digital content. Teach them how to be cautious about clicking on, downloading, posting and uploading content.

# Explain the implications

Explain to your children the public nature of the internet and its risks and benefits. Be sure they know that any digital info they share, such as emails, photos or videos, can easily be copied and pasted elsewhere and is almost impossible to take back. Remind your children that some of this digital communication, like social media posts or photos, could damage their reputation, friendship or future job prospects and should not be shared.

## Help them be good digital citizens

Remind your children to be good "digital friends" by respecting personal information of friends and family and not sharing anything online about others that could be embarrassing or hurtful.

## Empower your children to handle issues

Your children may face situations like cyberbullying, unwanted contact or hurtful comments online. Work with them on strategies for when problems arise. These can include talking to a trusted adult right away, refusing to retaliate, calmly talking with the bully, blocking the person or filing a complaint. Agree on steps to take if the strategy fails. It is better to have these strategies in place ahead of time instead of reacting to cyberbullying after it happens.

# Taking these steps helps
# Secure Our World.

**We can all help one another**
stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld