WEBROOT®

#CYBERSMART CHECKLIST

No doubt about it: the internet gives young people remarkable opportunities to learn new skills, have fun, and stay connected with friends and family. But kids and teenagers are just as vulnerable to cybercrime as adults. Use this handy checklist to raise your cyber awareness and teach safe online habits in your household!

- [ ] **STAY UPDATED.**
Criminals can use vulnerabilities in outdated software to attack your devices. Check for and install any updates—especially for your device's operating system and applications. Uninstall any old, unused applications that can be security risks.

- [ ] **STRENGTHEN YOUR PASSWORDS.**
Change your account passwords regularly. We recommend using strong, unique passphrases that are still easy to remember. Consider a password manager tool like LastPass® to easily store your login information. We also recommend adding extra security to your online accounts with two-factor authentication.

- [ ] **TIDY THINGS UP.**
Messy workspaces and desktops can create cybersecurity hazards. Take time clean your physical workspace and organize the files and folders on your devices.

- [ ] **CREATE DATA BACKUPS.**
Whether it's an important homework assignment, family photos, or your favorite video game's save file, back up your data regularly. We recommend a secure cloud storage tool such as iCloud or Dropbox to keep real-time data backups.

- [ ] **GET PROTECTED.**
Keep your devices secure from online threats with reliable internet security software. Whether it's a desktop, laptop, or mobile phone, antivirus protection has never been more important.

- [ ] **REVIEW SOCIAL MEDIA USE.**
Social media can be a great way to stay connected with friends and family, but it can also present privacy and security risks. Make sure your child knows how to control the privacy settings on each of their accounts. Also, teach caution when sharing any personal information on social media. Cybercriminals may use that info to target you and your family with social engineering scams and fraud.

- [ ] **TALK ABOUT COMMON SCAMS.**
Social engineering attacks are designed to trick victims very convincingly, and they're everywhere online. Teach your children how to spot and avoid phishing attacks and other scams in emails and social media messaging. Remember: if something seems too good to be true, question it.

- [ ] **SECURE YOUR CONNECTIONS.**
Did you know hackers can breach your devices and data through WiFi and Bluetooth? Be cautious of connecting in public places. Use a VPN to stay safe on public WiFi, and always turn Bluetooth off when not in use.

JOIN THE **#CYBERSMART** CONVERSATION ON THE WEBROOT COMMUNITY AND SOCIAL MEDIA.

COMMUNITY.WEBROOT.COM

@WEBROOT