



BOY SCOUTS OF AMERICA®

HUDSON VALLEY COUNCIL

Many cyber criminals take advantage of chaotic situations like the one caused by the Covid-19 pandemic. Their goal is to steal valuable personal information from Scouts, adult leaders, parents, businesses—anywhere they can get useable information. The Hudson Valley Council wants to inform you on some step where you can improve your “Cyber Hygiene” and some tips parents can talk to their Scout about, such as the importance of pausing, how phishing and other malware scams work and why shouldn't share information with strangers—not even birthdays!

Here are five tips to help Scouting families establish good cyber hygiene rules for staying safe while learning and playing on the Internet:

1. **THINK BEFORE CLICKING.** Online security threats are changing by the hour and are extremely sophisticated. Ask Scouts to approach every email with caution - the message may sound right, but the messenger may not be. Ask Scouts to pause and check with a parent before they open any email, click on links or open any attachments.
2. **VERIFY DOMAIN NAMES AND EMAIL SENDERS.** If a Scout does have to maintain access to email, talk with them about how to identify proper sources and senders. Check the URL before typing it in a browser or clicking a link. Help them to recognize spelling errors, altered graphics and logos as signs something isn't right. When you spot a phishing email that is obvious, show it to your Scout and point out how you knew it was a fake.
3. **USE BETTER PASSWORDS.** Increasingly, people are turning to password managers to keep their accounts safe, since it can be difficult to remember many long and strong passwords. These managers generate random passwords and allow managing the process with a single master password. If a password manager is not being used, make sure everyone in the house is using sufficiently complex passwords that are unique to the key accounts, and never let Scouts use any passwords associated with parents' online accounts!
4. **MONITOR THEM.** During these unprecedented times, monitoring Scouts online behavior should be a daily task. Don't worry about being a helicopter parent - set restrictions and enable parental controls to limit what kids can access. Look at internet history, app usage and be sure to know what programs and apps school is requiring ensuring Scouts are downloading the correct versions. Establish rules about app shopping. Require Scouts to run any app purchases by a parent or adult.
5. **SECURE MOBILE DEVICES.** Scouts may be using their phone, laptop, tablet and even watch to continue with schoolwork or stay entertained over the next several weeks or months. Secure all mobile devices in the household with frequent and routine firmware and software updates. Back up data frequently on hard drives that are not connected 24/7 to the internet.

For more information and training on the Boy Scouts of America's Cyber Chip and information on cyberbullying, cell phone use, texting, blogging, gaming, and identity theft visit:

<https://www.scouting.org/training/youth-protection/cyber-chip/>

