

October Cyber Security Month



Online gaming is a fun and interactive activity for millions of people across the globe, but it's also a space where cyber criminals try to ruin your fun by sending malicious links, stealing credentials and payment card information, and much more.

Tips:

- Use long, unique passwords
- Enable multi- factor authentication
- Secure payment data
- Think before you click
- Share with care- Be cautious about how much personal information you provide on gaming account profiles.
- Use Secure Wi-Fi -Public wireless networks and hotspots are not secure.



Block the bullies If another player is making you feel uncomfortable, tell a trusted adult. Remember that you can always kick a player out of the game if they are making you uncomfortable.

Play in disguise

Playing with people you don't know or who aren't your good friends? Use a safe Game Name. Don't use your first or last name in your usernames. Use an avatar instead your actual photo. If a stranger asks you to share a photo or to turn on your webcam, say no.

Parental controls are a great way to establish parameters around what kids can and can't do in their gaming environments, including limiting communications, limiting time spent, restricting e-commerce, etc.

Privacy Settings Go through accounts with children to configure privacy and security settings to limit over-sharing of information—such as location sharing. Walk the kids through why certain settings need to be changed.

